Silencing the Messenger:
Communication Apps under Pressure

November 2016

Freedom House

FREEDOM ON THE NET 2016

Freedom on the Net 2016
Table of Contents

Silencing the Messenger: Communication Apps under Pressure 1

Major Developments 4

Tables, Charts, and Graphs

FOTN Score Declines 3

Tracking Restrictions on Apps 5

Global Internet Population by 2016 FOTN Status 6

Censored Topics by Country 10

Key Internet Controls by Country 15

Countries with Largest Five-Year Declines 17

Distribution of Global Internet Users by Country and FOTN Status 18

Global Internet User Stats 19

FOTN World Map 20

65 Country Score Comparison 22

Score Comparison by Region 24

Internet Freedom vs. Press Freedom 26

Internet Freedom vs. Internet Penetration vs. GDP 27

Overview of Score Changes 28

65 Country Reports 30

Angola 31
Argentina 41
Armenia 57
Australia 68
Azerbaijan 79
Bahrain 93
Bangladesh 113
Belarus 127
Brazil 151
Cambodia 170
Canada 182
China 193
Colombia 221
Cuba 240
Ecuador 256
Egypt 275
Estonia 289
Ethiopia 298
France 314
Gambia, The 327
Georgia 337
Germany 348
Hungary 368
Iceland 384
India 394
Indonesia 423
Iran 440
Italy 455
Japan 467
Jordan 484
Kazakhstan 499
Kenya 517
Kyrgyzstan 530
Lebanon 542
Libya 553
Malawi 565
Malaysia 573
Mexico 589
Morocco 606
Myanmar 620
Nigeria 633
Pakistan 644
Philippines 659
Russia 670
Rwanda 688
Saudi Arabia 698
Singapore 711
South Africa 725
South Korea 736
Sri Lanka 754
Sudan 774
Syria 786
Thailand 800
Tunisia 818
Turkey 830
UAE 850
Uganda 866
Ukraine 877
United Kingdom 890
United States 911
Uzbekistan 937
Venezuela 953
Vietnam 975
Zambia 988
Zimbabwe 999

Methodology 1012

Checklist of Questions 1015

Contributors 1020

This report was made possible by the generous support of the U.S. State Department's Bureau of Democracy, Human Rights and Labor (DRL), Google, the Schloss Family Foundation, the Dutch Ministry of Foreign Affairs, Facebook, the Internet Society, Yahoo, and Twitter. The content of this publication is the sole responsibility of Freedom House and does not necessarily represent the views of its donors.

Cover: A Bahraini woman uses a mobile phone to take photos during clashes with riot police in Sitra, south of the capital Manama, January 2016.
Photo credit: Mohammed al-Shaikh/AFP/Getty Images

Freedom House

Silencing the Messenger: Communication Apps under Pressure

by Sanja Kelly, Mai Truong, Adrian Shahbaz, and Madeline Earp

Internet freedom has declined for the sixth consecutive year, with more governments than ever before targeting social media and communication apps as a means of halting the rapid dissemination of information, particularly during antigovernment protests.

Public-facing social media platforms like Facebook and Twitter have been subject to growing censorship for several years, but in a new trend, governments increasingly target messaging and voice communication apps such as WhatsApp and Telegram. These services are able to spread information and connect users quickly and securely, making it more difficult for authorities to control the information landscape or conduct surveillance.

The increased controls show the importance of social media and online communication for advancing political freedom and social justice. It is no coincidence that the tools at the center of the current crackdown have been widely used to hold governments accountable and facilitate uncensored conversations. Authorities in several countries have even resorted to shutting down all internet access at politically contentious times, solely to prevent users from disseminating information through social media and communication apps, with untold social, commercial, and humanitarian consequences.

Some communication apps face restrictions due to their encryption features, which make it extremely difficult for authorities to obtain user data, even for the legitimate purposes of law enforcement and national security. Online voice and video calling apps like Skype have also come under pressure for more mundane reasons. They are now restricted in several countries to protect the revenue of national telecommunications firms, as users were turning to the new services instead of making calls through fixed-line or mobile telephony.

Other key trends

Social media users face unprecedented penalties: In addition to restricting access to social media and communication apps, state authorities more frequently imprison users for their posts and the content of their messages, creating a chilling effect among others who write on controversial topics. Users in some countries were put behind bars for simply "liking" offending material on Facebook, or for not denouncing critical messages sent to them by others. Offenses that led to arrests ranged from mocking the king's pet dog in Thailand to "spreading atheism" in Saudi Arabia. The number of countries where such arrests occur has increased by over 50 percent since 2013.

In a new trend, governments increasingly target messaging and voice communication apps such as WhatsApp and Telegram.

Governments censor more diverse content: Governments have expanded censorship to cover a growing diversity of topics and online activities. Sites and pages through which people initiate digital petitions

or calls for protests were censored in more countries than before, as were websites and online news outlets that promote the views of political opposition groups. Content and websites dealing with LGBTI (lesbian, gay, bisexual, transgender, and intersex) issues were also increasingly blocked or taken down on moral grounds. Censorship of images—as opposed to the written word—has intensified, likely due to the ease with which users can now share them, and the fact that they often serve as compelling evidence of official wrongdoing.

Security measures threaten free speech and privacy: In an effort to boost their national security and law enforcement powers, a number of governments have passed new laws that limit privacy and authorize broad surveillance. This trend was present in both democratic and nondemocratic countries, and often led to political debates about the extent to which governments should have backdoor access to encrypted communications. The most worrisome examples, however, were observed in authoritarian countries, where governments used antiterrorism laws to prosecute users for simply writing about democracy, religion, or human rights.

The number of countries where arrests for online posts occur has increased by over 50 percent since 2013.

Online activism reaches new heights: The internet remained a key tool in the fight for better governance, human rights, and transparency. In over two-thirds of the countries in this study, internet-based activism has led to some sort of tangible outcome, from the defeat of a restrictive legislative proposal to the exposure of corruption through citizen journalism. During the year, for example, internet freedom activists in Nigeria helped thwart a bill that would have limited social media activity, while a WhatsApp group in Syria helped save innocent lives by warning civilians of impending air raids.

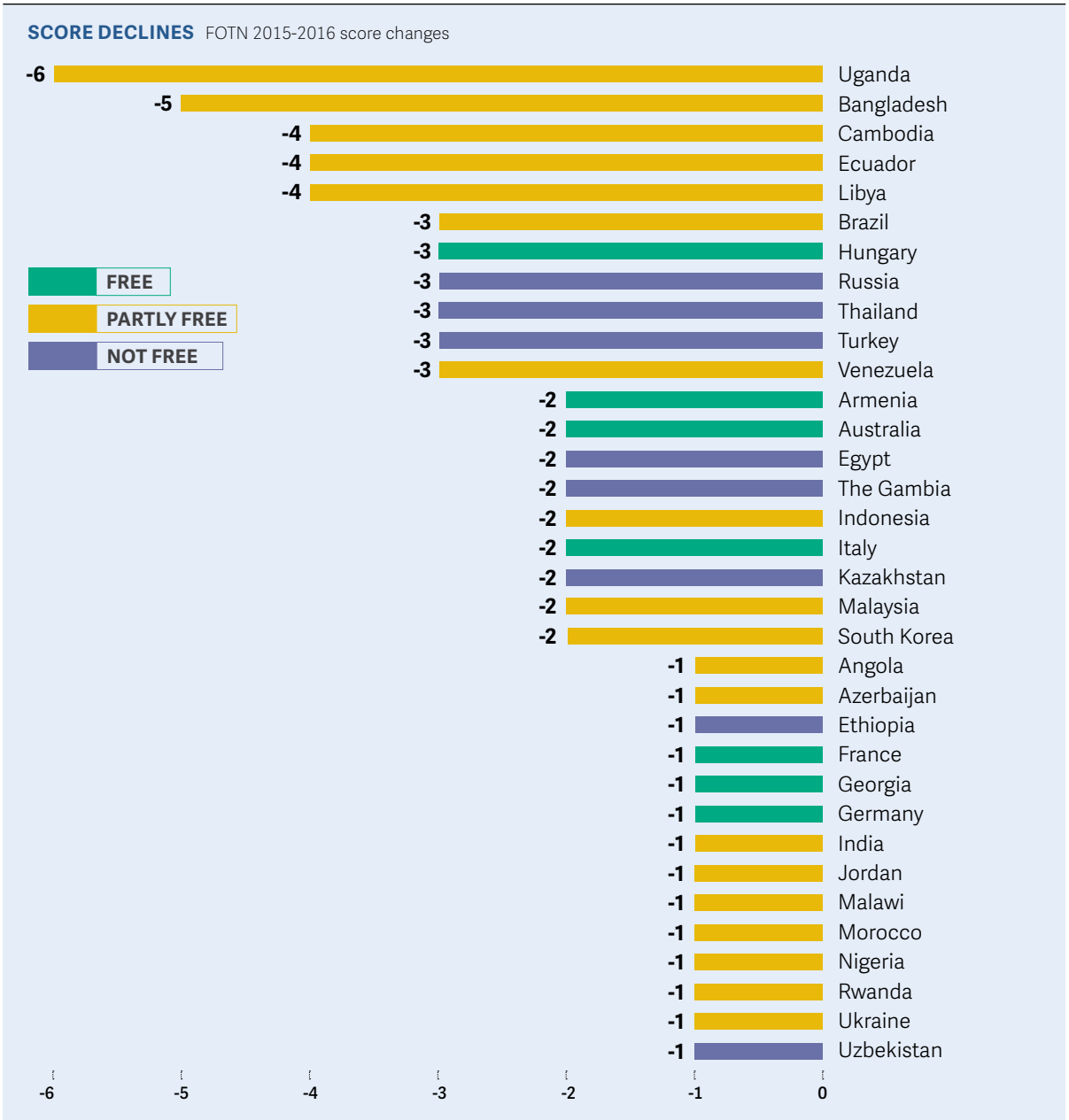
Tracking the global decline

Freedom on the Net is a comprehensive study of internet freedom in 65 countries around the globe, covering 88 percent of the world's internet users. It tracks improvements and declines in governments' policies and practices each year, and the countries included in the study are selected to represent diverse geographical regions and types of polity. This report, the seventh in its series, focuses on developments that occurred between June 2015 and May 2016, although some more recent events are included in individual country narratives. More than 70 researchers, nearly all based in the countries they analyzed, contributed to the project by examining laws and practices relevant to the internet, testing the accessibility of select websites, and interviewing a wide range of sources.

Of the 65 countries assessed, 34 have been on a negative trajectory since June 2015. The steepest declines were in Uganda, Bangladesh, Cambodia, Ecuador, and Libya. In Uganda, the government made a concerted effort to restrict internet freedom in the run-up to the presidential election and inauguration in the first half of 2016, blocking social media platforms and communication services such as Facebook, Twitter, and WhatsApp for several days. In Bangladesh, religious extremists claimed responsibility for the murders of a blogger and the founder of an LGBTI magazine with a community of online supporters. And Cambodia passed an overly broad telecommunications law that put the industry under government control, to the detriment of service providers and user privacy. Separately, Cambodian police arrested several people for their Facebook posts, including one about a border dispute with Vietnam.

China was the year's worst abuser of internet freedom. The Chinese government's crackdown on free expression under President Xi Jinping's "information security" policy is taking its toll on the digital activists who have traditionally fought back against censorship and surveillance. Dozens of prosecutions related to online expression have increased self-censorship, as have legal restrictions introduced in 2015. A criminal law amendment added seven-year prison terms for spreading rumors on social media (a charge often used against those who criticize the authorities), while some users belonging to minority religious groups were imprisoned simply for watching religious videos on their mobile phones. The London-based magazine *Economist* and the Hong Kong–based *South China Morning Post* were newly blocked in mainland China, as were articles and commentaries about sensitive events including a deadly chemical blast in Tianjin in 2015.

Turkey and Brazil were downgraded in their internet freedom status. In Brazil, which slipped from Free to Partly Free, courts imposed temporary blocks on WhatsApp for its failure to turn over user data in criminal investigations, showing little respect for the principles of proportionality and necessity. Moreover,



at least two bloggers were killed after reporting on local corruption. Turkey, whose internet freedom environment has been deteriorating for a number of years, dropped into the Not Free category amid multiple blockings of social media platforms and prosecutions of users, most often for offenses related to criticism of the authorities or religion. These restrictions continued to escalate following the failed coup in July 2016, in spite of the crucial role that social media and communication apps—most notably FaceTime—played in mobilizing citizens against the coup.

Just 14 countries registered overall improvements. In most cases, their gains were quite modest. Users in Zambia faced fewer restrictions on online content compared with the previous few years, when at least two critical news outlets were blocked. South Africa registered an improvement due to the success of online activists in using the internet to promote societal change and diversifying online content, rather than any positive government actions. Digital activism also flourished in Sri Lanka as censorship and rights violations continued to decline under President Maithripala Sirisena's administration. And the United States registered a slight improvement to reflect the passage of the USA Freedom Act, which puts some limits on bulk collection of telecommunications metadata and establishes several other privacy protections.

Major Developments

Social Media and Communication Tools under Assault

In the past year, social media platforms, communication apps, and their users faced greater threats than ever before in an apparent backlash against growing citizen engagement, particularly during politically sensitive times. Of the 65 countries assessed, governments in 24 impeded access to social media and communication tools, up from 15 the previous year. Governments in 15 countries temporarily shut down access to the entire internet or mobile phone networks, sometimes solely to prevent users from disseminating information through social media. Meanwhile, the crackdown on users for their activities on social media or messaging apps reached new heights as arrests and punishments intensified.

Governments in 24 countries impeded access to social media and communication tools, up from 15 the previous year.

New restrictions on messaging apps and internet-based calls

In a new development, the most routinely targeted tools this year were instant messaging and calling platforms, with restrictions often imposed during times of protests or due to national security concerns. Governments singled out these apps for blocking due to two important features: encryption, which protects the content of users' communications from interception, and text or audiovisual calling functions, which have eroded the business model and profit margins of traditional telecommunications companies.

Whatever the justification, restrictions on social media and internet-based communication tools threaten to infringe on users' fundamental right to access the internet. In a landmark resolution passed in July 2016, the UN Human Rights Council condemned state-sponsored disruptions to internet access and the free flow of information online.

WhatsApp faced the most restrictions, with 12 out of 65 countries blocking the entire service or disabling certain features, affecting millions of its one billion users worldwide. Telegram, Viber, Facebook Messenger, LINE, IMO, and Google Hangouts were also regularly blocked. Ten countries restricted access to platforms that enable voice and video calling over the internet, such as Skype and FaceTime.

Nearly ubiquitous among internet and mobile phone users, these communication platforms have become essential to the way we connect with the world. Incidents of blocking have had far-reaching effects, preventing family members from checking in during a crisis, activists from documenting police abuses during a protest, and individuals from communicating affordably with social and professional contacts abroad.

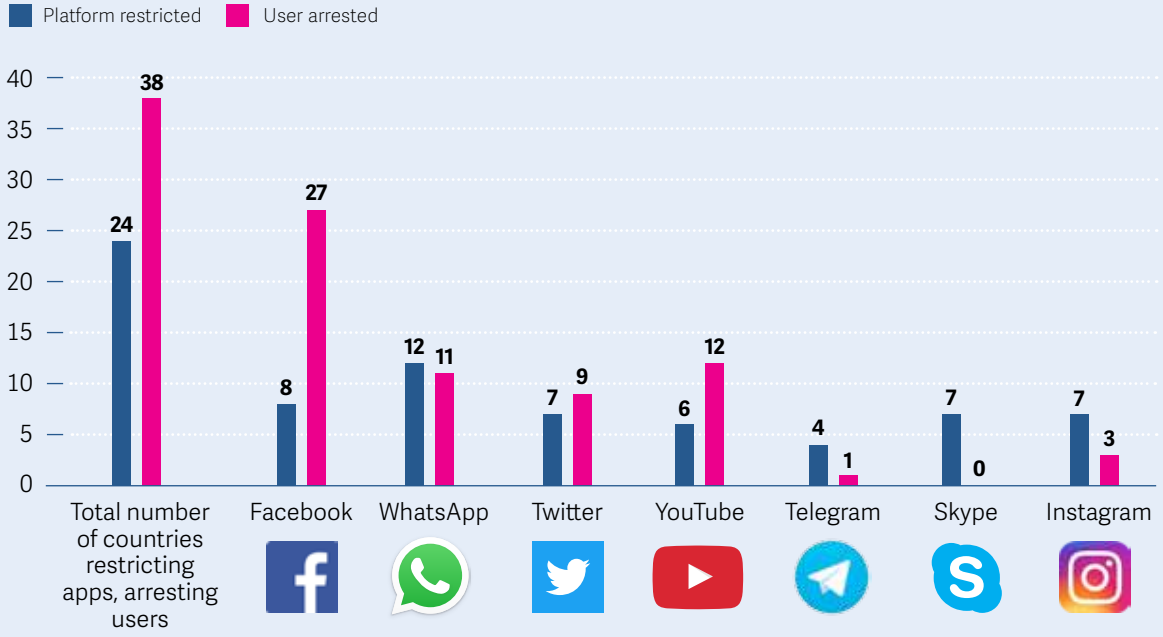
While all users are adversely affected by restrictions, the harm is often disproportionately felt by marginalized communities and minority groups, who are more likely to be cut off from critical information sources and the ability to advocate for their rights. In the United Arab Emirates (UAE), for example, where migrant workers and other noncitizens make up 88 percent of the population, blocks on communication tools have made it difficult for these individuals to organize or seek support from their home countries.

App blocking aimed at protests, expressions of dissent

Authoritarian regimes most frequently restricted communication apps to prevent or quell antigovernment protests, as they have become indispensable for sharing information on demonstrations and organizing participants in real time. In Ethiopia, ongoing protests that began in November 2015 in response to the government's marginalization of the Oromo people have

NUMBER OF COUNTRIES WHERE POPULAR APPS WERE BLOCKED OR USERS ARRESTED

WhatsApp was blocked more than any other tool, while Facebook users were arrested for posting political, social, or religious content in 27 countries.



been met with periodic blocks on services including WhatsApp, Facebook Messenger, and Twitter. In Bahrain, Telegram was blocked for several days around the anniversary of the February 14, 2011, "Day of Rage" protests, likely to quash any plans for renewed demonstrations.

In Bangladesh, the authorities ordered the blocking of platforms including Facebook Messenger, WhatsApp, and Viber to prevent potential protests following a Supreme Court ruling in November that upheld death sentences for two political leaders convicted of war crimes. The longest block lasted 22 days. In Uganda, officials directed internet service providers to block WhatsApp, Facebook, and Twitter for several days during the presidential election period in February 2016 and again in the run-up to the reelected incumbent's inauguration in May. In both instances, the unprecedented blocking worked to silence citizens' discontent with the president's 30-year grip on power and their efforts to report on the ruling party's notorious electoral intimidation tactics.

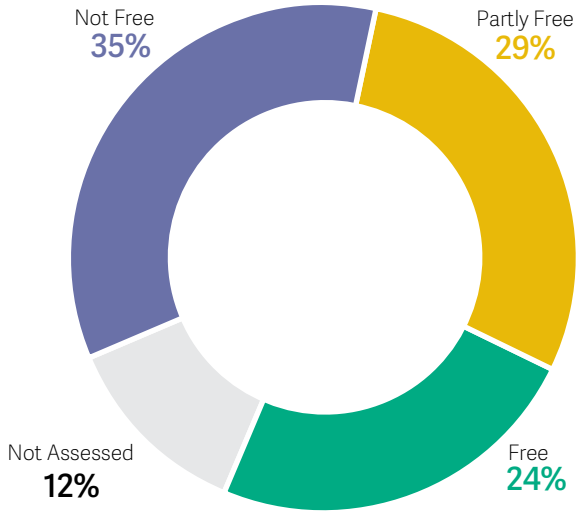
New security and encryption features also trigger blocking

Governments increasingly imposed restrictions on internet-based messaging and calling services due to their strong privacy and security features, which have attracted many users amid growing concerns about surveillance worldwide.

Telegram was blocked in China after the authorities learned of its popularity among human rights lawyers.

GLOBAL INTERNET POPULATION BY 2016 FOTN STATUS

FOTN assesses 88 percent of the world's internet user population.



In many countries, individuals are using messaging apps as private social networks where they can enjoy greater freedom of expression than on more established, public-facing social networks such as Facebook and Twitter. New messaging and calling apps also provide greater anonymity than conventional voice and SMS services that can be tracked due to SIM-card registration requirements, and several offer end-to-end encryption that prevents wiretapping and interception.

Activists and human rights defenders in repressive countries protect their communications by convening on WhatsApp, Viber, and Telegram to share sensitive information, conduct advocacy campaigns, or organize protests. Journalists in Turkey, for example, have established new distribution networks for their reporting via group channels on WhatsApp to avert censorship.

The same security features that appeal to users of the new platforms have brought them into conflict with governments in both democratic and authoritarian countries. In Brazil in 2015 and 2016, regional courts ordered a block on WhatsApp three times after it failed to turn over encrypted communications to local authorities during criminal investigations. On all three occasions, WhatsApp's parent company, Facebook, insisted that it did not have access to the information in question, since WhatsApp does not store the content of users' communications. Nevertheless, the judges chose to penalize not just the company, but also Brazil's 100 million WhatsApp users.

Authoritarian regimes targeted Telegram for its "secret chat" mode, which allows messages to self-delete after a period of time. The platform was blocked in China after the authorities learned of its popularity among human rights lawyers, joining a long list of other international communication apps that are unavailable to Chinese users. State-run news outlets in the country accused Telegram of aiding activists in "attacks on the [Communist] Party and government." Iran also targeted Telegram, blocking it for a week in October 2015 when it refused to aid officials' surveillance and censorship efforts. In May 2016, Iran's Supreme Council on Cyberspace ordered Telegram to host all data on Iranian users inside the country or face blocking.

Market threats to national telecoms lead to backlash

Internet-based messaging and calling platforms faced increasing restrictions from governments seeking to protect their countries' major state-owned or private telecommunications companies. Given the rising popularity of new communication services over the past decade, telecoms in some markets have become concerned about the future economic viability of their traditional text and voice services, particularly when the new competitors are not subject to the same regulatory obligations and fees.

Typically free to download, messaging platforms such as WhatsApp, Telegram, and Facebook Messenger have proliferated in emerging markets, where the advent of low-cost, internet-enabled mobile devices and smartphones have made sending messages, photos, and even videos via online tools much more affordable than traditional SMS, for which telecom carriers charge a variable rate per message. Indeed, app-based mobile messaging has surpassed SMS texting worldwide since at least 2013.

Similarly, Voice over Internet Protocol (VoIP) and internet-based video calling services such as Skype, Google Hangouts, and Apple's FaceTime have signifi-

cantly reduced the cost of real-time audio and visual communication for users, resulting in the decreased use of traditional phone services that charge by the minute. Though telecom companies still profit from the data used by internet-based platforms, continual improvements in network infrastructure have only made data plans cheaper, threatening to leave traditional voice and SMS services further behind.

One of the first market-related restrictions on internet-based communication services was imposed by the American telecommunications company AT&T in 2007, when it partnered with Apple to become the sole mobile provider for the first iPhone and subsequently banned VoIP applications that could make calls using a wireless data connection. Google's Voice app was consequently rejected by the iPhone's app store, and Skype developed a version of its platform that only allowed iPhone users to make calls when connected to a Wi-Fi network. Under pressure from the Federal Communications Commission (FCC), AT&T changed course in 2009, setting a positive precedent and providing users with more freedom to choose from a suite of services based on quality and affordability.

In the past year, restrictions to protect market interests escalated most prominently in the Middle East and North Africa. The UAE had been an early mover, requiring VoIP services to obtain a license to operate as a telecom provider and subsequently blocking both the voice and video calling features of Skype, WhatsApp, and Facebook Messenger in 2014, in an effort to protect the profits of state-owned telecom companies. Most recently, Snapchat's calling function was disabled in April 2016. While circumvention tools such as virtual private networks (VPNs) were widely used to bypass the blocks, the government cracked down in July 2016, adopting amendments to the Cybercrime Law that penalize the "illegal" use of VPNs with temporary imprisonment, fines of between US$136,000 and US$545,000, or both.

Morocco's telecommunications regulator issued a directive in January 2016 that suspended all internet calling services over mobile networks, citing previously unenforced licensing requirements under the 2004 telecommunications law. The order seemed heavily influenced by the UAE's Etisalat, which purchased a majority stake in Maroc Telecom, the country's largest operator, in 2014. In Egypt, where long-distance VoIP calls on Skype have been blocked since 2010, voice calling features on WhatsApp and Viber have reportedly been inaccessible since October 2015. The calling functions of popular platforms were also disabled in Saudi Arabia, while Apple has been forced to sell its iPhone in the kingdom without the built-in FaceTime app.

A Turkish man was handed a one-year suspended sentence for this meme juxtaposing President Reçep Tayyip Erdogan and a character from the Lord of the Rings films. In determining whether or not the image insulted the president, the judge assembled a panel of film experts. Another user is facing up to two years in prison for reposting the same meme.

Pressure to regulate mobile communication services in the past year threatened to impede access to such platforms in other regions, particularly sub-Saharan Africa, where mobile internet use has been growing rapidly. In Kenya, Nigeria, South Africa, and Zimbabwe, private telecommunications companies lobbied governments to regulate internet-based messaging and voice calling platforms such as Skype and WhatsApp, citing concerns over their profits. Meanwhile, Ethiopia's single telecommunications provider, state-owned

Since June 2015, police in 38 countries arrested individuals for their activities on social media.

EthioTelecom, announced plans in April 2016 to introduce a new pricing scheme for mobile users of popular communication applications. Companies in the European Union (EU) pushed EU officials throughout 2016 to regulate new communication services, calling for a "level playing field" that subjects messaging and calling platforms to the same regulatory framework, licensing fees, and law enforcement access requirements as traditional telecoms.

Social media users face unprecedented penalties

While many governments attempted to restrict access to social media and communication platforms, far more turned to traditional law enforcement methods to punish and deter users. Since June 2015, police in a remarkable 38 countries arrested individuals for their activities on social media, compared with 21 countries where people were arrested for content published on news sites or blogs. The rising penetration of social networks in repressive societies has enabled discussion and information sharing on issues that governments deem sensitive, resulting in arrests of journalists, politicians, activists, and ordinary citizens who may not be aware that they are crossing redlines.

A Saudi court sentenced an individual to 10 years in prison and 2,000 lashes for spreading atheism on Twitter.

Dramatic sentences for social media 'crimes'

Social media users were prosecuted for a range of alleged crimes during the coverage period. Some supposed offenses were quite petty, illustrating both the sensitivity of some regimes and the broad discretion given to police and prosecutors under applicable laws. Lebanon's bureau of cybercrimes interrogated a Facebook user for criticizing a Lebanese singer, while soldiers in the UAE were arrested for disrespecting the army after they shared a video of themselves recreating a popular dance craze in their uniforms.

While severe punishments for online speech are not new, their application to social media activities that many people engage in daily was a cause for serious concern. In February 2016, a Saudi court sentenced an individual to 10 years in prison and 2,000 lashes for allegedly spreading atheism in 600 tweets. In the harshest examples of the coverage period, military courts in Thailand issued 60- and 56-year sentences in separate cases involving Facebook posts that were deemed critical of the monarchy in August 2015, though they were reduced to 30 and 28 years after the defendants pleaded guilty. While sentences like these may not cause people to stop using social media entirely, they are likely to encourage self-censorship on sensitive topics, robbing the technology of its potential for galvanizing social and political change.

Many detentions were justified under criminal laws penalizing defamation or insult, but they often aimed to suppress information in the public interest. In Morocco, YouTube footage of a man lifting asphalt barehanded from a local road led to his arrest for allegedly defaming the official responsible for the poor construction.

Users punished for their connections and readership

One goal of social media is to allow users to share content with a wide circle of connections. Police in some countries seem determined to undermine that goal, specifically pursuing individuals whose content goes viral. In Zimbabwe, Pastor Evan Mawarire was arrested in July 2016 after his YouTube videos criticizing the country's leadership sparked the #ThisFlag social media campaign and inspired nationwide protests. Elsewhere, charges often multiplied as content was passed along: in November 2015, 17 people in Hungary were charged with defamation for sharing a Facebook post that questioned the legitimacy of the mayor of Siófok's financial dealings.

In a disturbing development, defendants whose content failed to spread widely were nevertheless punished as a warning to others. In Russia, mechanical engineer Andrey Bubeyev was sentenced to two years in prison in May 2016 for reposting material that identified the Russian-occupied Crimean Peninsula as part of Ukraine on the social network VKontakte. He shared the information with just 12 contacts.

Authorities in other cases scoured social media for a pretext to charge specific individuals, or were so intent on suppressing certain content that identifying the correct defendant was of secondary importance. In Ethiopia, charges against an opposition politician and student protesters principally cited evidence gleaned from social media. Pseudonymous accounts offered limited protection and raised the risk of mistaken identity. A man in Uganda was charged on suspicion of operating the popular Facebook page Tom Voltaire Okwalinga, but he denied being responsible for the page, which frequently accused senior leaders of corruption

and incompetence. Some people were held responsible for posts clearly made by others. At least three criminal charges were filed in India against the administrators of WhatsApp groups based on offensive or antireligious comments shared by other group members.

A number of users were apparently targeted only to punish their associates. In Thailand, Patnaree Chankij, the mother of an activist who opposes Thailand's military government, was charged with insulting the monarchy based on a private, one-word acknowledgement she sent in reply to a Facebook Messenger post from her son's friend; police said she failed to criticize or take action against the antiroyalist sentiment in the post, instead replying "yes" or "I see." Patnaree told journalists that the charge was in reprisal for her son's activities. In China, police detained the local relatives of at least three overseas journalists and bloggers who produce online content that the Chinese government perceives as critical.

Governments Censor More Diverse Content

This year featured new trends in the type of content that attracted official censorship. Posts related to the LGBTI community, political opposition, digital activism, and satire resulted in blocking, takedowns, or arrests for the first time in many settings. Authorities also demonstrated an increasing wariness of the power of images on today's internet.

A longer roster of forbidden topics

Attempts to censor LGBTI content were observed in 18 countries, up from 14 in 2015, as more individuals and groups sought to use digital tools to connect and share resources, sometimes in defiance of local laws or religious beliefs. In July 2016, an LGBTI group reported that Azerbaijan's national domain-name registrar was declining to register website domains like lgbt.az. In Indonesia, the information ministry asked the LINE messaging platform to remove emojis with gay or lesbian themes from its online store. Also in 2016, South Korean regulators told the Naver web portal to exercise "restraint" after it linked to an online gay drama. At least 13 countries blocked content serving the LGBTI community on moral grounds, including Saudi Arabia and Sudan. Turkish authorities systematically blocked the most popular LGBTI websites over several weeks in mid-2015.

Content related to political opposition was subject to censorship in 26 countries, an increase from 23 in 2015. A court in Kazakhstan ordered an opposition-affiliated magazine to shutter its Facebook page along with its print edition in October 2015. In Bahrain, prosecutors questioned Sheikh Ali Salman, leader of the country's largest political organization, for allegedly tweeting about democracy, even though he was already imprisoned; police are now investigating who continues to operate the account.

A 22 year-old student in Egypt was sentenced to three years in prison for posting this photo depicting President Abdel Fattah al-Sisi with Mickey Mouse ears on Facebook.

Digital activism, including petitions, campaigns for social or political action, and protests, were subject to censorship in 20 countries in *Freedom on the Net*, up from 16 in 2015. Campaigns using smartphones or social media can appear dangerous because they are particularly effective at reaching young people. In The Gambia, a Facebook post calling on young people to join peaceful protests disappeared in April 2016 and was replaced with a warning to abide by the law; the protest organizer left the country, citing death threats. Because online mobilization amplifies discontent, authorities in many countries sought to shut it down even when the issues at stake were local. In Kazakhstan, two activists were arrested in May 2016 for planning on social media to attend land-reform protests scheduled to take place the next day.

Authorities in 26 of the 65 countries assessed, up from 23 in 2015, tried to suppress satire, which often skewered public officials. A poet in Myanmar was charged in November 2015 for posting a satirical poem on Facebook that described a newlywed's dismay at discovering a tattoo of the president on her husband's genitals.

CENSORED TOPICS BY COUNTRY

Censorship was reflected if state authorities blocked or ordered the removal of content, or detained or fined users for posting content on the topics considered. The chart does not consider extralegal pressures such as violence, self-censorship, or cyberattacks, even where the state is believed to be responsible.

Other topics that have long been subject to censorship remained in authorities' crosshairs this year:

- **Criticism of the authorities** was censored in 49 out of 65 countries, two more than in the previous year. In Cuba, for example, dissident or independent news sites that are perceived as critical—such as *Cubanet*, *Penúltimos Días*, *Diario de Cuba*, *Cubaencuentro*, *Hablemos Press*, and *14ymedio*—are restricted at most internet access points.

- **Corruption allegations** were subject to censorship in 28 out of 65 countries. Starting in July 2015, the Malaysian government, which had pledged never to censor the internet, blocked prominent blogs and news websites for the first time. The sites had reported on a billion-dollar corruption scandal implicating Prime Minister Najib Razak. The content-sharing platform Medium was blocked completely after one of the previously affected sites used it to repost content.

- News and opinion on **conflict**, terrorism, or outbreaks of violence were subject to censorship in 27 out of 65 countries. Sensitivity about ongoing conflict resulted in legitimate content being censored. In May 2016, British journalist Martyn Williams challenged South Korean regulators for blocking his website, North Korea Tech.

- **Social commentary** on issues including history and natural disasters was censored in 21 out of 65 countries. In August 2015, Ecuador prohibited independent reporting on the newly active volcano Cotopaxi. Citizens turned to social media for news, and as a result the government announced legal actions against users for "unscrupulous" comments on social networks. In China, discussion of the 1989 crackdown on prodemocracy protesters in Tiananmen Square is censored so comprehensively that internet users in mid-2015 reported being unable to make online financial transfers in denominations of 6 or 4, numbers which connote the crackdown's June 4 anniversary.

- Twenty out of 65 countries censored **blasphemy**, or content considered insulting to religion, suppressing legitimate commentary about religious and other issues. In 2016, internet service providers in India were ordered to block jihadology.net, an academic repository of primary sources about Islamist militancy. In Brazil, artist Ana Smiles was ordered to remove images of religious figurines dressed as superheroes or famous artists from social media.

- Information by or about particular **ethnic groups** was subject to censorship in 13 out of 65 countries. In Turkey, where fighting between security forces and the Kurdistan Workers' Party (PKK) has escalated, dozens of websites and Twitter accounts belonging to journalists reporting on the conflict have been censored.

Images draw greater scrutiny

Images, a vivid and immediate way of communicating information online, became a new priority for censors around the world in the past year. Several governments blocked platforms that allow users to exchange images easily in a bid to contain social and political protests. In Vietnam, Instagram was blocked along with Facebook during environmental protests in 2016, after both tools were used to organize and share images of fish killed en masse by industrial pollution.

World leaders proved particularly sensitive to altered images of themselves circulating on social media. In Egypt, a photo depicting President Abdel Fattah al-Sisi with Mickey Mouse ears resulted in a three-year prison term for the 22-year-old student who posted it on Facebook. Three people in Zimbabwe were arrested for photos of President Robert Mugabe that they shared in satirical social media posts.

Journalists were often targeted for disseminating images as part of their work. Police in Kenya arrested journalist Yassin Juma for using Facebook to report on and share photos of casualties in an attack on Kenyan forces stationed in Somalia. Egyptian photojournalist Ali Abdeen was arrested in April 2016 for covering protests against the transfer of Egyptian islands to Saudi Arabia. He was convicted in May of inciting illegal protests, publishing false news, and obstructing traffic, though his employers at the news website El-Fagr confirmed that he was working on assignment.

Security Measures Threaten Free Speech and Privacy

In both democratic and authoritarian countries, counterterrorism measures raised the likelihood of collateral damage to free speech, privacy rights, and business operations. Although in some cases the actions were meant to address legitimate security concerns, 14 of the 65 countries assessed in *Freedom on the Net* approved new national security laws

or policies that could have a disproportionately negative effect on free speech or privacy, with especially threatening consequences for government critics and journalists in countries that lack democratic checks and balances. Meanwhile, high-profile terrorist attacks in Europe and the United States led to increased pressure on technology companies to cooperate more closely with law enforcement regarding access to user data.

14 of the 65 countries approved national security laws or policies that could have a negative effect on free speech or privacy.

Broad antiterrorism laws lead to unjust penalties

In numerous authoritarian countries, officials enforced antiterrorism and national security laws in a manner that produced excessive or entirely inappropriate punishments for online activity. In the gravest cases, such laws were used to crack down on nonviolent activists, prominent journalists, and ordinary citizens who simply questioned government policies or religious doctrine.

In December 2015, a court in Russia handed down the first maximum sentence of five years in prison for extremism to blogger Vadim Tyumentsev, who was charged for posting videos that criticized pro-Kremlin separatists in eastern Ukraine and called for the expulsion of refugees coming to Russia from the Ukrainian regions of Donetsk and Luhansk. In July 2016, a new Russian law increased the maximum prison term for justifying or inciting terrorism to seven years. Penalties are even harsher in Pakistan, where antiterrorism courts sentenced two men in separate cases to 13 years in prison for promoting sectarian hatred on Facebook. A lawyer for one of the men said he had only "liked" the post in question, which was described as "against the belief of Sunni Muslims."

Ethiopian blogger Zelalem Workagenehu was found guilty of terrorism for facilitating a course on digital security.

Overly broad definitions of terrorism often resulted in spurious convictions. In Jordan, activist Ali Malkawi was arrested for criticizing the stance of Arab and Muslim leaders regarding the plight of Myanmar's persecuted Rohingya minority. He was sentenced to three months in jail under the antiterrorism law for "disturbing relations with a friendly state." Ethiopian blogger Zelalem Workagenehu was found guilty of terrorism and sentenced to over five years in prison in May for facilitating a course on digital security.

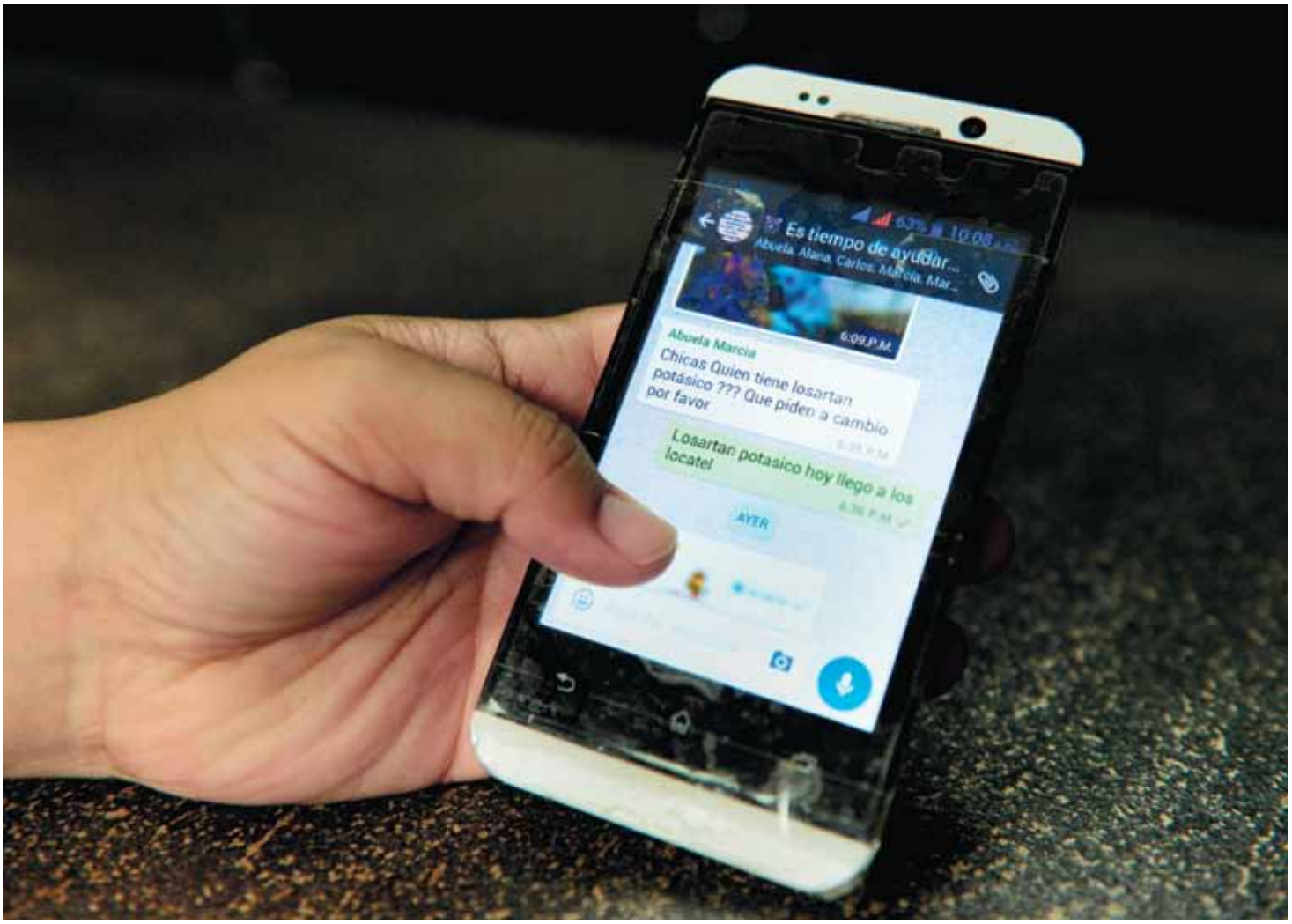
In some cases, journalists were branded as terrorists for independently documenting civil strife and armed conflicts. Sayed Ahmed al-Mousawi, an award-winning Bahraini photojournalist, was sentenced to 10 years in prison under an antiterrorism law in November 2015 due to his role in covering antigovernment protests and providing SIM cards to alleged "terrorists." Hayri Tunç, a Turkish journalist for the news site Jiyan, was sentenced to two years in prison for creating "terrorist propaganda" through his tweets, Facebook posts, and YouTube videos related to the conflict between the state and Kurdish militants.

Pressure to enable backdoor access

In democracies, where the definition of terrorism tends to have a narrower scope, debate has focused on the ability of intelligence and law enforcement agencies to prevent and prosecute terrorist attacks. As technology companies develop stronger privacy safeguards for their users, they have clashed with government entities attempting to gather information on suspected terrorists.

A United States district court ordered Apple to create new software that could bypass its own security measures and access a locked iPhone used by a perpetrator of the December 2015 terrorist attack in San Bernardino, California. Apple chief executive Tim Cook warned in a public letter that doing so would set a dangerous domestic legal precedent, embolden undemocratic governments to make similar requests, and make Apple products more vulnerable to hackers. U.S. authorities eventually dropped the case after experts were able to unlock the iPhone without Apple's help, leaving the broader legal issue unresolved.

Similarly, high-profile terrorist attacks in Europe have increased pressure to bolster the surveillance powers of government agencies tasked with disrupting future plots. France has extended a state of emergency since a major attack struck Paris in November 2015, autho-



Venezuelans rely on secure messaging tools to exchange information about scarce goods. Online content about currency exchange rates is pervasively censored.

rizing security agencies to monitor and detain individuals with little judicial oversight. Germany passed a law mandating the retention of telecommunications data by providers for up to 10 weeks, despite fierce protests from the opposition and a 2014 ruling by the EU's Court of Justice that such blanket requirements contravene fundamental rights. In August 2016, interior ministers from both countries called on the European Commission to draft an EU-level framework for compelling the makers of encrypted chat apps to hand over decrypted data in terrorism cases.

Authoritarian states have also joined the fray, but with far fewer scruples about individual rights. In Russia, for example, a draconian antiterrorism law passed in June 2016 requires all "organizers of information online"—which in theory could include local service providers as well as foreign social media companies—to provide the Federal Security Service (FSB) with tools to decrypt any information they transmit, essentially mandating backdoor access. The law will also require service providers to keep users' metadata for up to three years and the content of users' communications—calls, texts, images, videos, and other data—for up to six months.

Faced with growing pressure to comply with government requests, some tech companies have pushed back. Shortly after the Apple case, Microsoft sued the United States over the right to tell customers when data stored on the company's servers has been handed over to government agencies (Twitter initiated

Russia's new antiterrorism law requires all "organizers of information online" to provide the FSB with tools to decrypt any information they transmit.

a similar lawsuit in 2014). And in March 2016, roughly a billion people received a huge boost in their cybersecurity when Facebook rolled out end-to-end encryption for all WhatsApp users, incorporating technology from the makers of the security app Signal. However, such resistance is nearly impossible in countries that lack free and independent judicial institutions. Companies operating in authoritarian settings have little choice but to leave the market, comply with state demands, or risk blocking, closure, or imprisonment of their local staff.

Exploiting encryption's weakest links

Even when back doors are not installed, state entities and other actors have found ways to overcome cybersecurity and privacy safeguards. This year several governments exploited one of the weakest links in some encrypted apps: SMS authentication. Many platforms currently allow users to confirm their identity through a text message sent to their phone, whether to augment password security, replace forgotten passwords, or activate a new account. German agents reportedly intercepted these messages—which are unencrypted by default—in order to access the Telegram accounts of a neo-Nazi terrorist group suspected of plotting to attack a refugee shelter and assassinate Muslim clerics. The same technique was used in attempts to spy on nonviolent political and social activists in Egypt, Iran, and Russia over the past year. Companies and activists have recommended turning off SMS authentication in favor of code-generator apps.

In two-thirds of the countries under study, internet-based activism led to a tangible outcome.

Another potential weak link can be found in certificates, the small files that allow encrypted web traffic to travel to its destination and be decrypted for access by the intended recipient. Kazakhstan passed a new law requiring users and providers to install a "national security certificate" on all devices. While questions remain about how the requirement will be implemented in practice, observers worry that the measure will undermine cybersecurity for all Kazakh users by allowing security agencies or hackers to intercept and decrypt traffic before it reaches end users. If the law is successful, repressive countries around the world will look to Kazakhstan as a model for circumventing encryption in the name of national security.

New Heights in Digital Activism

As governments around the world impose new restrictions on internet freedom, it is worth remembering what is at stake. The present crackdown comes as digital platforms are being used in new and creative ways to advocate for change and, in many cases, save lives. Internet advocacy had real-world results in both democracies and authoritarian settings over the past year, and its impact was often most pronounced in countries where the information environment was more open online than off. In over two-thirds of the countries examined in this study, there was at least one significant example of individuals producing a tangible outcome by using online tools to fight for internet freedom, demand political accountability, advance women's rights, support victims of unjust prosecution, or provide relief to those affected by natural disasters.

Fighting for internet freedom and digital rights

Social media were used effectively to fight for internet freedom in a variety of countries over the past year. In Thailand, over 150,000 people signed a Change.org petition against a government plan to centralize the country's internet gateways, which would strengthen the authorities' ability to monitor and censor online activity. As a result, the government announced that it had scrapped the plan, though skeptical internet users remain vigilant.

Using the hashtag #NoToSocialMediaBill, Nigerian digital rights organizations launched a multifaceted campaign to defeat a "Frivolous Petitions Prohibition Bill" that threatened to constrain speech on social media. Alongside significant digital media activism, civil society groups organized a march on the National Assembly, gathered signatures for a petition presented during a public hearing on the bill, and filed a lawsuit at the Federal High Court in Lagos, all of which contributed to the bill's withdrawal in May 2016. India's telecommunications regulator banned differential pricing schemes in February after more than a million comments were submitted online to protest companies that charge consumers different prices for select content or applications.

Protesting governments and demanding accountability

Social media were also used to combat corruption, wasteful spending, or government abuse. Movements like Lebanon's #YouStink or #ElectricYerevan in Armenia channeled citizens' anger over bread-

KEY INTERNET CONTROLS BY COUNTRY

Freedom House documented how governments censor and control the digital sphere. Each colored cell represents at least one occurrence of the cited control during the report's coverage period of June 2015 to May 2016; colored cells with an asterisk (*) represent events that occurred between June and September 2016, when the report was sent to press. The Key Internet Controls reflect restrictions on content of political, social, or religious nature. For a full explanation of the methodology, see page 31.

Types of key internet controls

COUNTRY	# KICs employed	Social media or communications apps blocked	Political, social, or religious content blocked	Localized or nationwide ICT shutdown	Progovernment commentators manipualte online discussions	New law or directive increasing censorship or punishment passed	New law or directive increasing surveillance or restricting anonymity passed	Blogger or ICT user arrested, imprisoned, or in prolonged detention for political or social content	Blogger or ICT user physically attacked or killed (including in custody)	Technical attacks against government critics or human rights organizations	FOTN SCORE
Angola	2					*					40
Armenia	3	*									30
Azerbaijan	6										57
Bahrain	8			*							71
Bangladesh	5										56
Belarus	5										62
Brazil	2										32
Cambodia	4										52
Canada	1										16
China	9										88
Cuba	5										79
Ecuador	4										41
Egypt	7										63
Ethiopia	8					*	*				83
France	2										25
The Gambia	7	*									67
Georgia	1										25
Hungary	1						*				27
India	4										41
Indonesia	3										44
Iran	5										87
Jordan	5								*		51
Kazakhstan	9										63
Kenya	2										29
Kyrgyzstan	2										35
Lebanon	3										45
Libya	4										58
Malawi	1										41
Malaysia	4										45
Mexico	4										38
Morocco	4										44
Myanmar	3										61
Nigeria	2										34
Pakistan	7						*				69
Russia	7										65
Rwanda	2										51
Saudi Arabia	5										72
Singapore	1										41
South Korea	4										36
Sri Lanka	1										44
Sudan	4										64
Syria	6										87
Thailand	4										66
Tunisia	4										38
Turkey	6										61
Uganda	4										42
Ukraine	4								*		38
United Arab Emirates	5										68
Uzbekistan	7										79
Venezuela	6										60
Vietnam	8										76
Zambia	2			*							38
Zimbabwe	2	*						*			56
June 2015 – May 2016 coverage period		21	32	13	26	18	11	45	20	25	
June 2016 – September 2016		3	0	2	0	2	3	1	2	0	
Total June 2015 – September 2016		24	32	15	26	20	14	46	22	25	

NO KEY INTERNET CONTROLS OBSERVED

	FOTN Score
Argentina	27
Australia	21
Colombia	32
Estonia	6
Germany	19
Iceland	6
Italy	25
Japan	22
Phillipines	26
South Africa	25
United Kingdom	23
United States	18

and-butter issues—a garbage crisis and energy price hikes, respectively—into sustained protests that brought thousands of people to the streets and extracted responses from the government. Citizens in Kyrgyzstan criticized the parliament's plan to spend some US$40,000 on 120 new chairs to replace those purchased only five years earlier. The campaign, called #120Кресел (120Chairs), received extensive coverage on Twitter and through news outlets, and lawmakers subsequently abandoned the plan.

The Syrian American Medical Society used WhatsApp to guide a veterinarian who delivered twin babies by caesarean section.

Even in some of the world's most closed societies, individuals have used smartphones to record and publicize instances of abuse by state officials. After a video showing abuse at a military academy went viral in Myanmar, public outrage forced the military to launch a high-level investigation, an unprecedented gesture toward accountability from the country's most untouchable institution. In Saudi Arabia, the head of Riyadh's Committee for the Promotion of Virtue and the Prevention of Vice was dismissed in a bid to quell popular unease over a video in which members of the so-called morality police chased a girl outside a mall in the Saudi capital.

Defending women's rights around the globe

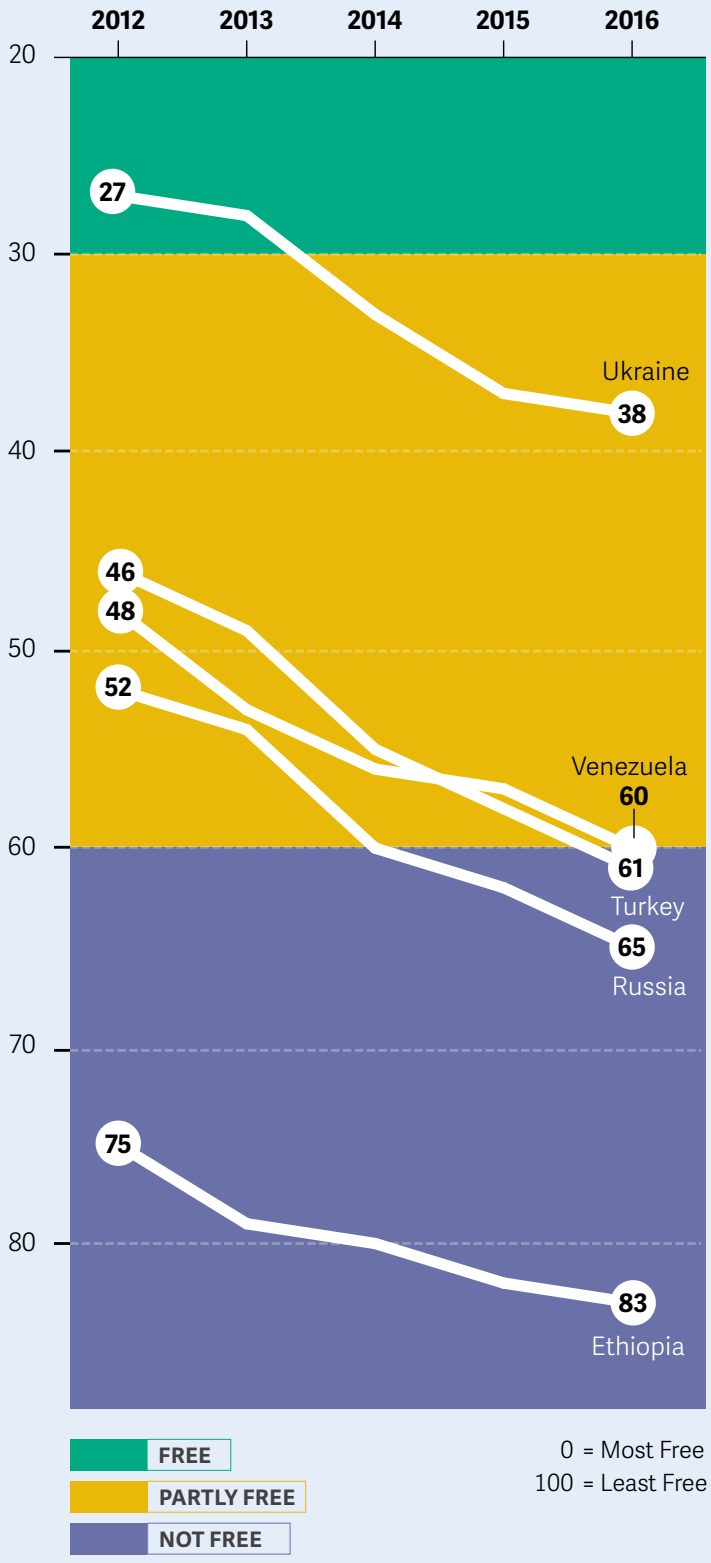
Several countries featured notable internet-based campaigning for women's rights. A Jordanian activist launched a popular online petition asking the parliament to amend Article 123 of the civil law, which requires that a male guardian be present for children to be admitted at hospitals. The National Council for Family Affairs, chaired by Queen Rania, later drafted legislation that created an exception in cases of emergency. In Argentina, the alarming rate of femicide and other gender-based violence led to an ongoing campaign, #NiUnaMenos (Not One Less), that has generated almost 300,000 tweets and inspired hundreds of thousands of people to demonstrate on June 3 of 2015 and 2016.

Disaster relief and saving lives during wartime

There were numerous instances during the year of social media and communication apps enabling crucial information-sharing that was credited with saving lives. Citizens and organizations have used digital tools to organize relief efforts, solicit donations, and disseminate information about rescue operations. In Sri Lanka, taxi apps like PickMe introduced an SOS button that allowed customers trapped in flood-affected areas to mark their location for rescue. And some of the most extraordinary uses of social media took place in Syria, where online applications have long been vital for citizen journalists and civic activists. The Syrian American Medical Society has used WhatsApp for telemedicine, in one instance guiding a veterinarian who delivered twin babies by caesarean section in the besieged town of Madaya.

Such examples of activism indicate that the internet is an indispensable tool for promoting social justice and political liberty, used by citizens worldwide to fight for their rights, demand accountability, and amplify marginalized voices. This is precisely why authoritarian governments are intensifying their efforts to impose control, and why democratic societies must simultaneously defend internet freedom abroad and uphold their own standards at home.

LARGEST FIVE-YEAR DECLINES



Of the 65 countries covered by *Freedom on the Net*, these five countries have experienced the steepest deterioration in internet freedom over the last five years:

Ukraine's decline reflects the country's struggle to regain stability since the 2014 toppling of the Yanukovych regime and ongoing conflict with Russian-backed separatists. Engaged in an information war with the Kremlin, authorities arrested social media users who stray from the government narrative, while cyberattacks originating in Russia have destabilized critical infrastructure around the country.

Venezuela's economic crisis impeded internet access and sharpened discontent with new president Nicolas Maduro. Seeking to prevent the country's vibrant digital sphere from contributing to social unrest, the regime blocks independent reporting and manipulates online discussions. Twitter users and citizen journalists are increasingly detained, and in some cases beaten by state security agents and progovernment thugs.

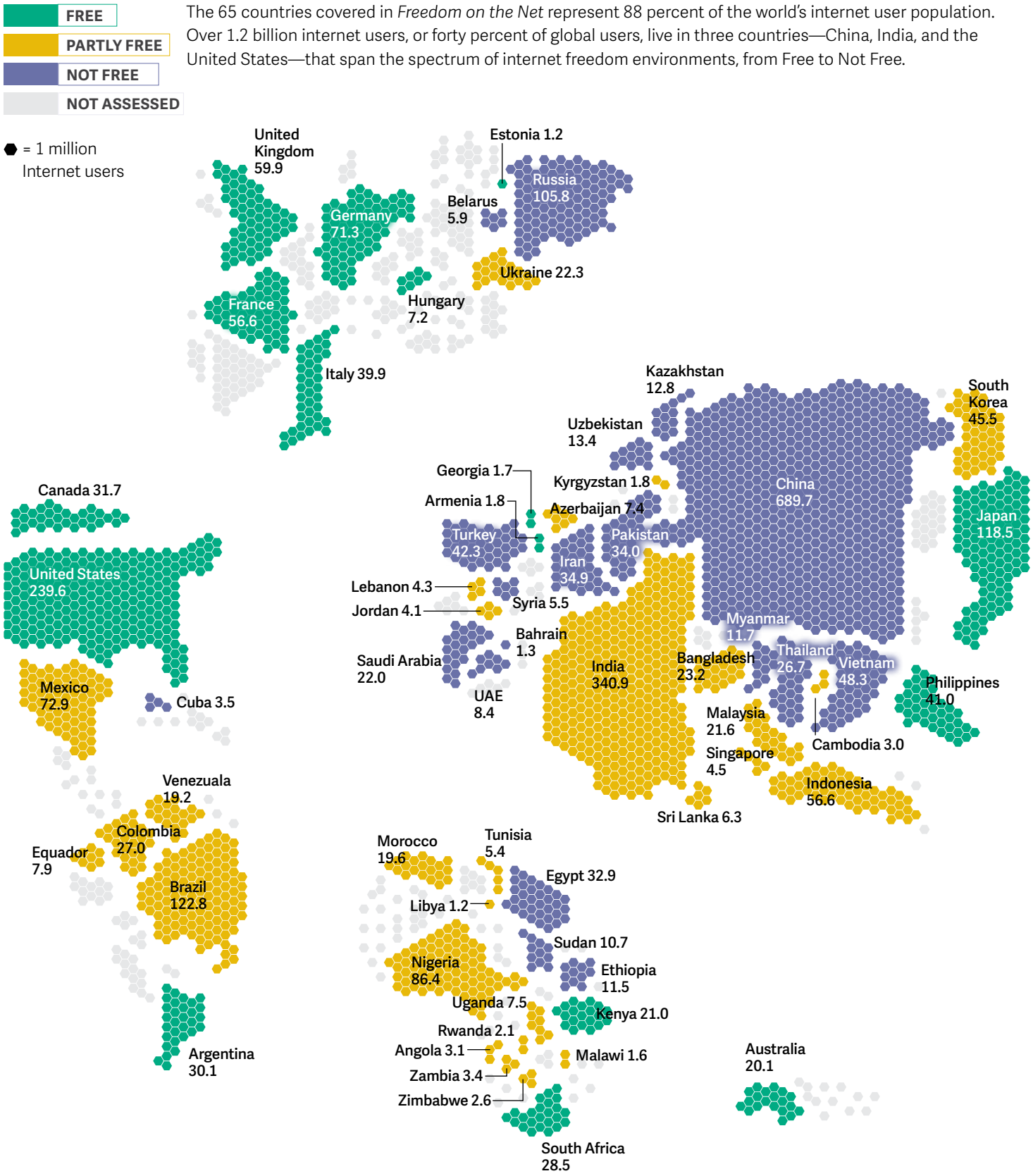
Internet freedom fell by 15 points in **Turkey**, the most drastic five-year decline recorded. President Erdogan oversaw a closing of the digital media sphere, often as a countermeasure to anti-government protests, corruption scandals, or terrorist attacks. Authorities are now more brazen to block social media platforms, demand companies remove "illegal" content, and prosecute individuals for "defaming" public figures.

The **Russian** government's tolerance for dissent diminished following the mass protests accompanying Vladimir Putin's election for a third presidential term in 2012. The regime consolidated power by promoting pro-Russia propaganda, upgrading surveillance technology, and censoring criticism of its Ukraine policy. In addition, new laws on blogger registration, data localization, and decryption requirements have undermined privacy.

Long one of the world's least connected countries, **Ethiopia** intensified its crackdown on bloggers and online journalists over the past five years. The regime has used terrorism laws to imprison individuals for simply calling attention to human rights issues. With ICT growth hindered by a state monopoly, the authorities maintain strict control over the digital sphere through a sophisticated filtering and surveillance apparatus.

DISTRIBUTION OF GLOBAL INTERNET USERS BY COUNTRY AND FOTN STATUS

The 65 countries covered in *Freedom on the Net* represent 88 percent of the world's internet user population. Over 1.2 billion internet users, or forty percent of global users, live in three countries—China, India, and the United States—that span the spectrum of internet freedom environments, from Free to Not Free.



GLOBAL INTERNET USER STATS

Over **3.2 billion people** have access to the internet.

According to Freedom House estimates:

67% live in countries where **criticism of the government, military, or ruling family** has been subject to censorship.

60% live in countries where ICT users were **arrested or imprisoned** for posting content on political, social, and religious issues.

49% live in countries where individuals have been **attacked or killed** for their online activities since June 2015.

47% live in countries where **insulting religion** online can result in censorship or jail time.

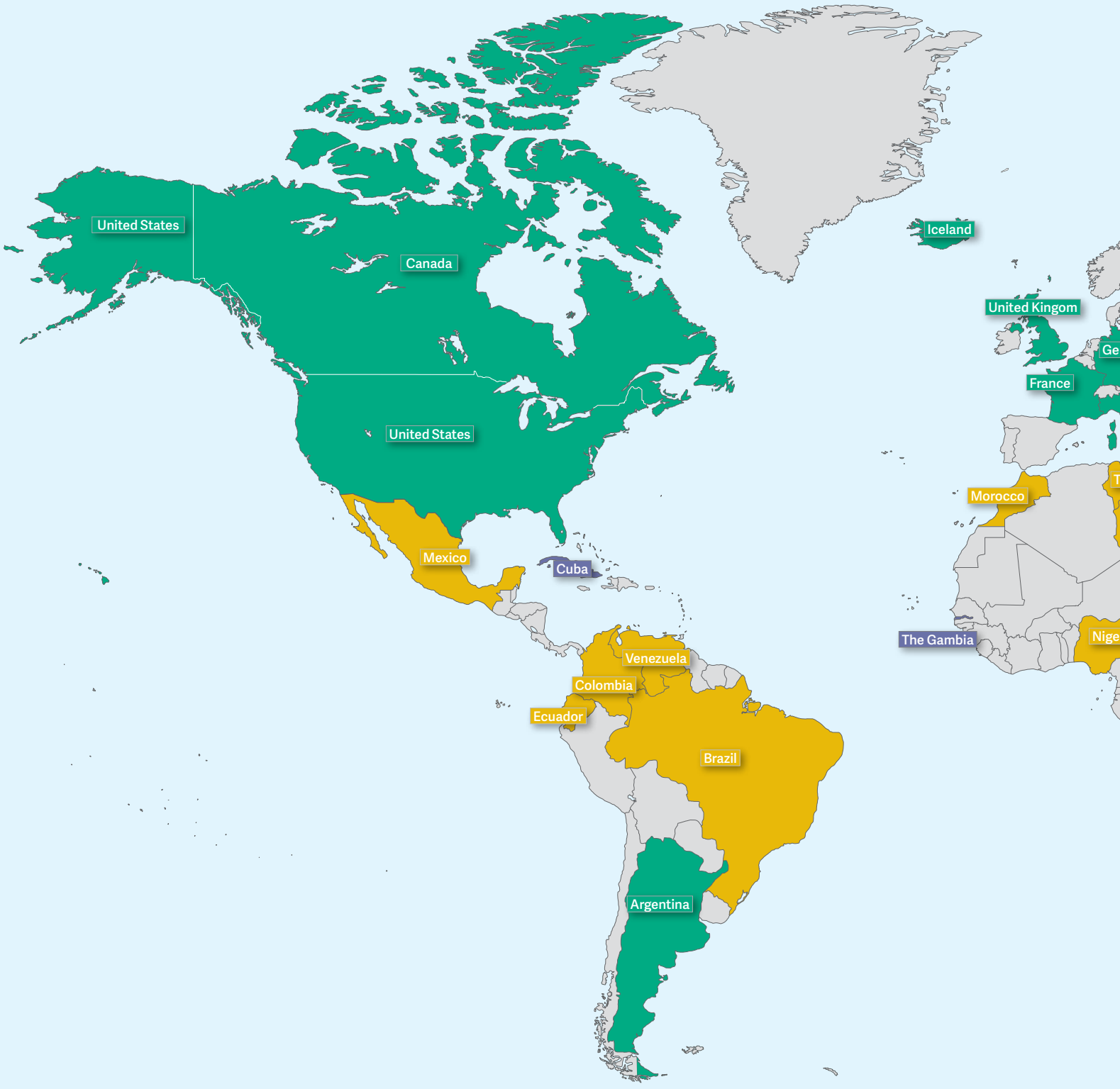
33% live in countries where online discussion of **LGBTI issues** can be repressed or punished.

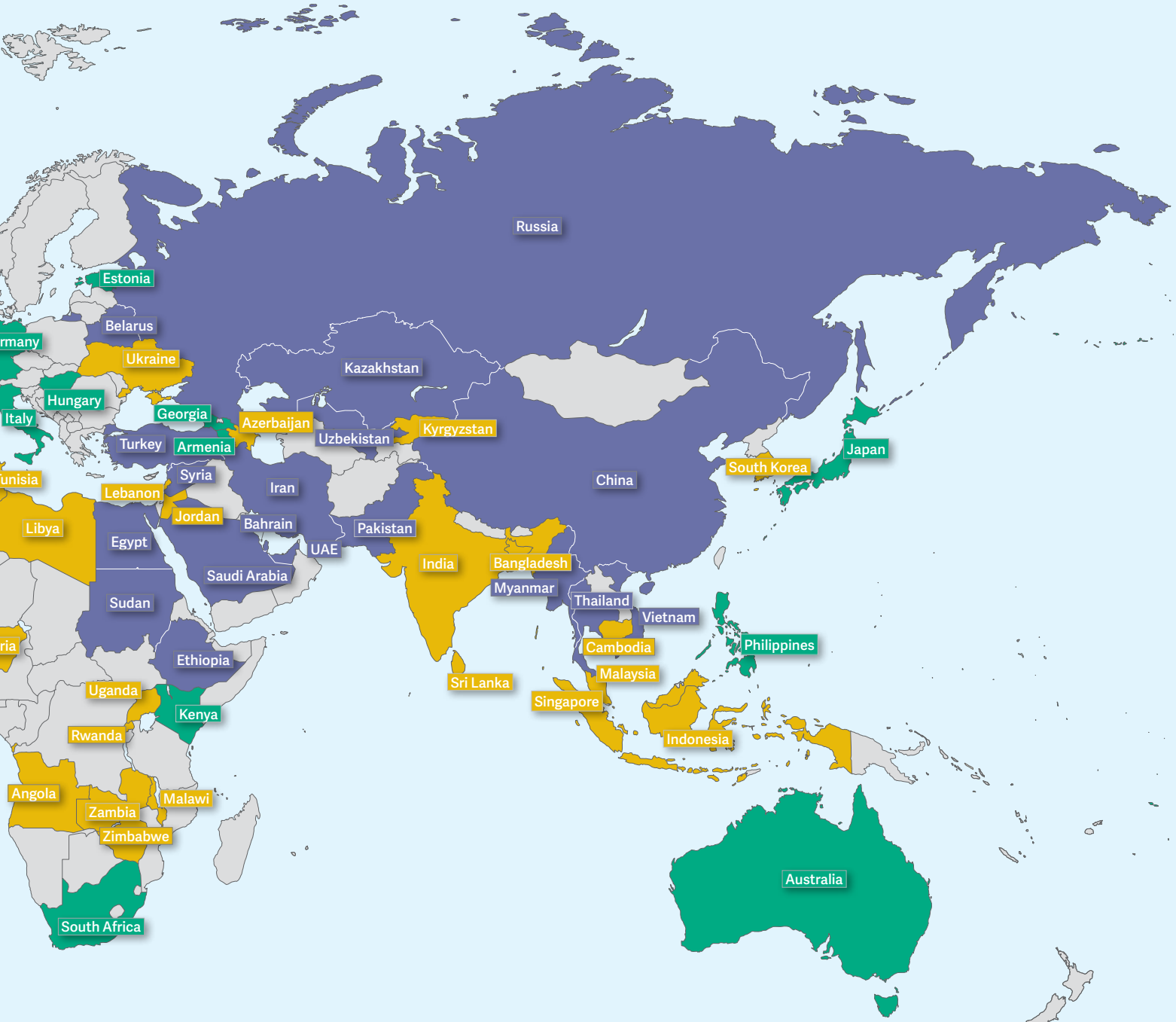
38% live in countries where **social media or messaging apps** were blocked over the past year.

27% live in countries where users have been arrested for **writing, sharing, or even liking Facebook posts**.

38% live under governments that **disconnected internet or mobile phone access**, often for political reasons.

FREEDOM ON THE NET 2016





Status	Countries
FREE	17
PARTLY FREE	28
NOT FREE	20
Total	**65**

Freedom on the Net 2016 assessed 65 countries around the globe. The project is expected to expand to more countries in the future.

65 COUNTRY SCORE COMPARISON

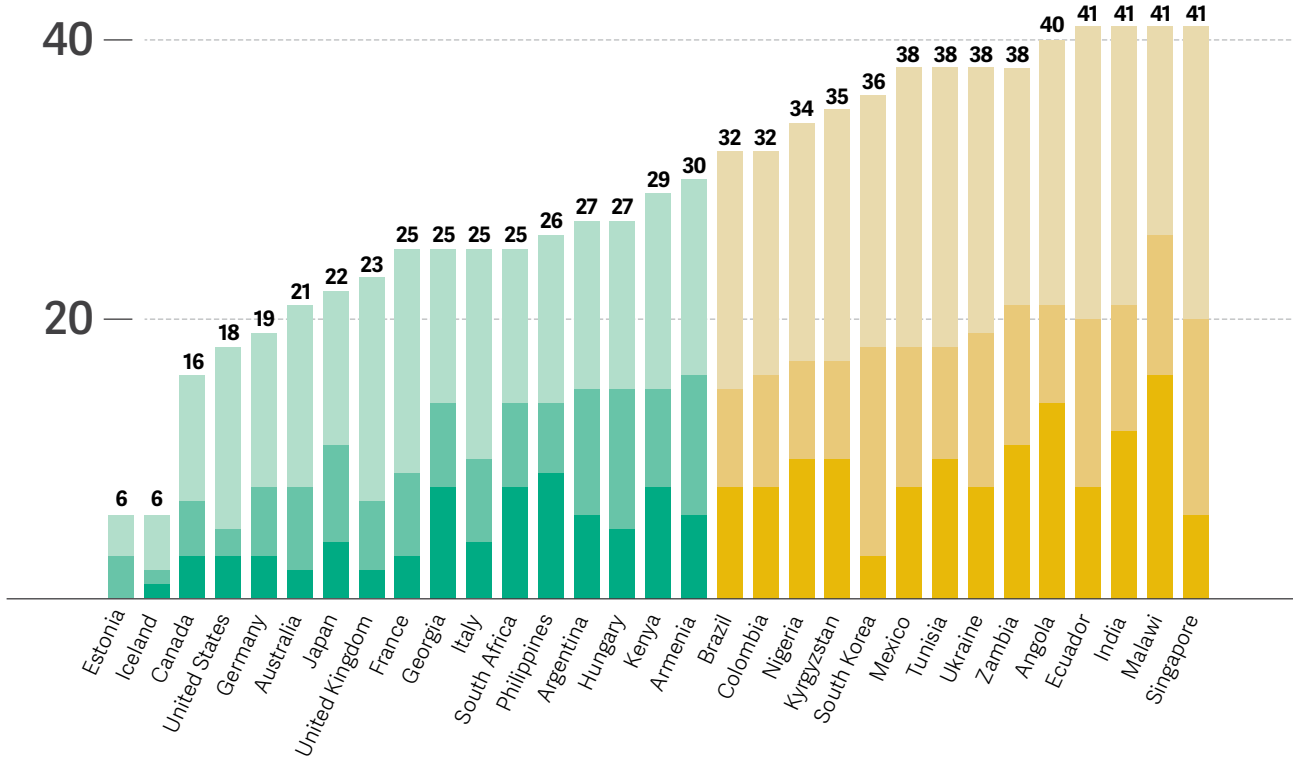
Freedom on the Net measures the level of internet and digital media freedom in 65 countries. Each country receives a numerical score from 0 (the most free) to 100 (the least free), which serves as the basis for an internet freedom status designation of FREE (0-30 points), PARTLY FREE (31-60 points), or NOT FREE (61-100 points).

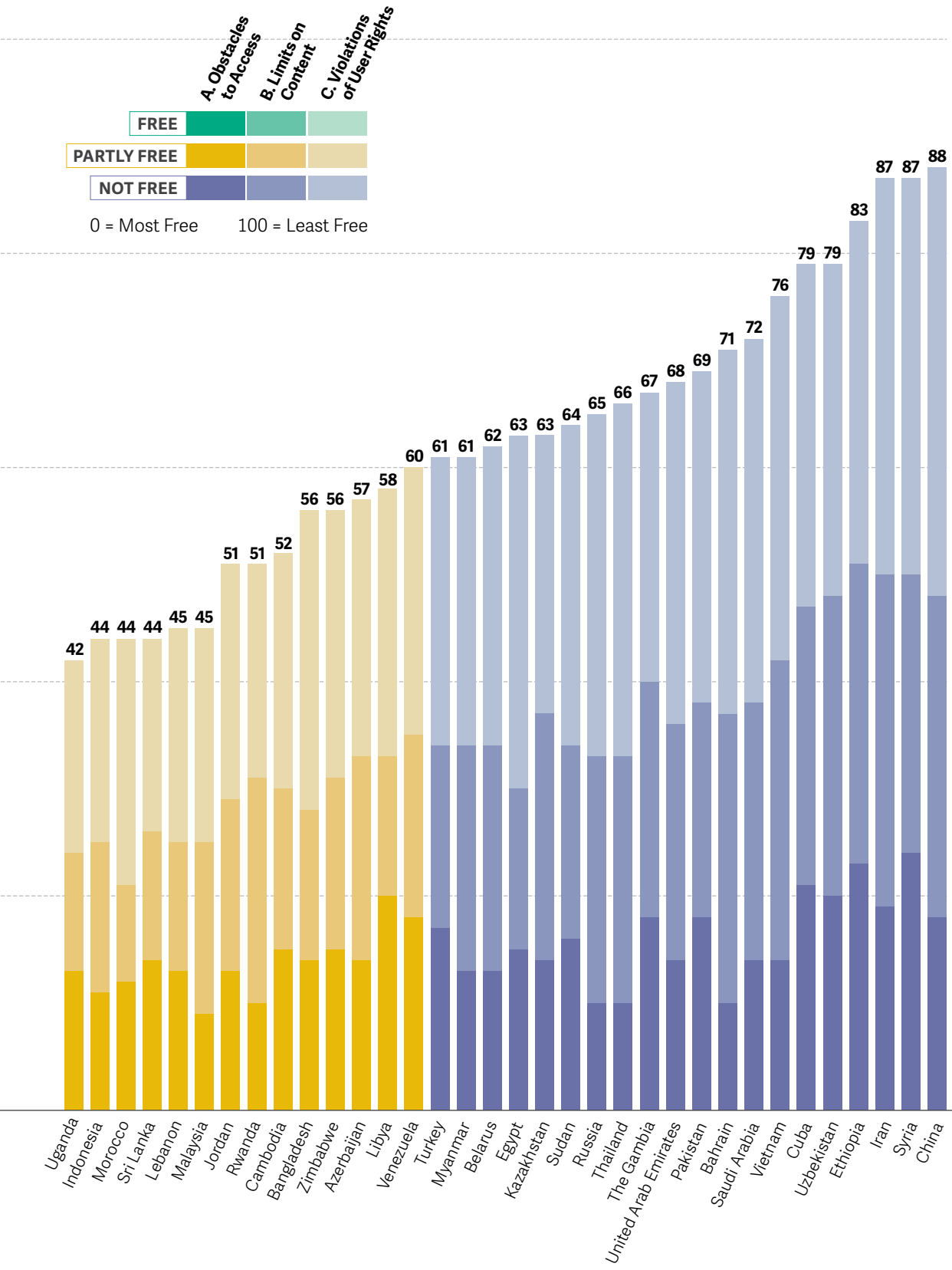
Ratings are determined through an examination of three broad categories:

A. OBSTACLES TO ACCESS: Assesses infrastructural and economic barriers to access; government efforts to block specific applications or technologies; and legal, regulatory, and ownership control over internet and mobile phone access providers.

B. LIMITS ON CONTENT: Examines filtering and blocking of websites; other forms of censorship and self-censorship; manipulation of content; the diversity of online news media; and usage of digital media for social and political activism.

C. VIOLATIONS OF USER RIGHTS: Measures legal protections and restrictions on online activity; surveillance; privacy; and repercussions for online activity, such as legal prosecution, imprisonment, physical attacks, or other forms of harassment.




A. Obstacles to Access
B. Limits on Content
C. Violations of User Rights
FREE
PARTLY FREE
NOT FREE
0 = Most Free
100 = Least Free
42
44
44
44
45
45
51
51
52
56
56
57
58
60
61
61
62
63
63
64
65
66
67
68
69
71
72
76
79
79
83
87
87
88
Uganda
Indonesia
Morocco
Sri Lanka
Lebanon
Malaysia
Jordan
Rwanda
Cambodia
Bangladesh
Zimbabwe
Azerbaijan
Libya
Venezuela
Turkey
Myanmar
Belarus
Egypt
Kazakhstan
Sudan
Russia
Thailand
The Gambia
United Arab Emirates
Pakistan
Bahrain
Saudi Arabia
Vietnam
Cuba
Uzbekistan
Ethiopia
Iran
Syria
China

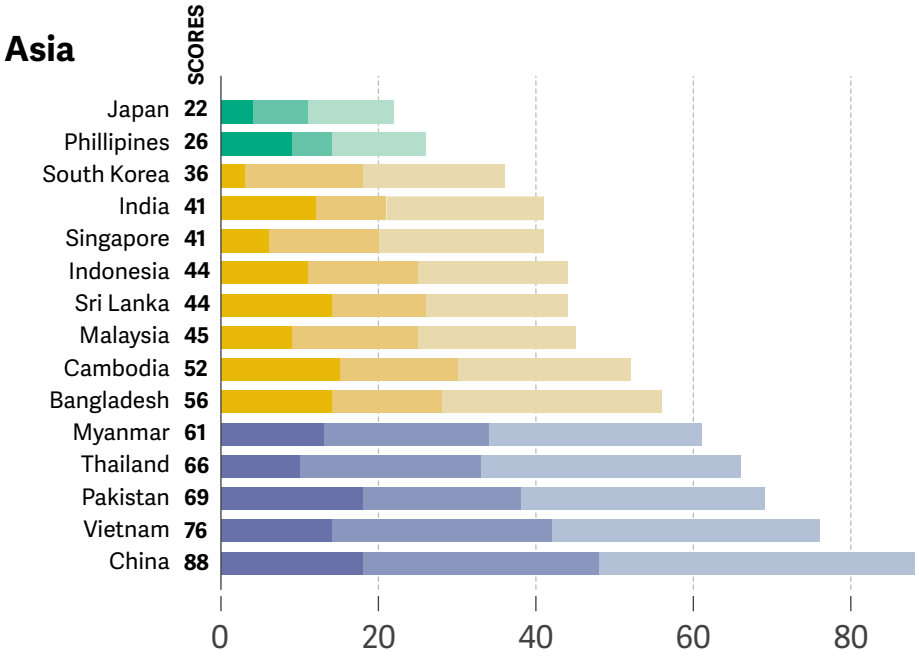
REGIONAL GRAPHS

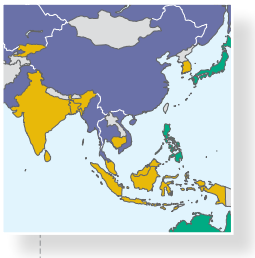
Freedom on the Net 2016 covers 65 countries in 6 regions around the world. The countries were chosen to illustrate internet freedom improvements and declines in a variety of political systems.

A. Obstacles to Access
B. Limits on Content
C. Violations of User Rights

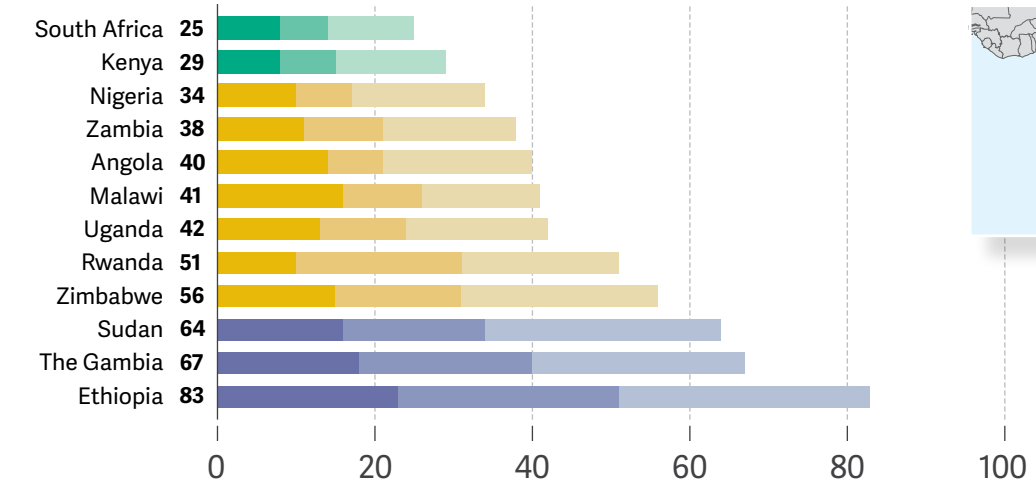
0 = Most Free
100 = Least Free

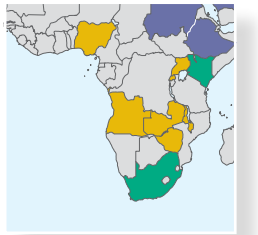
Asia



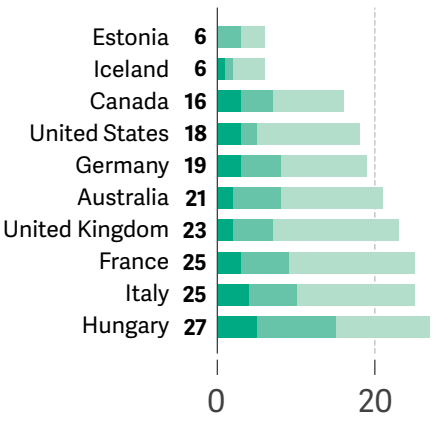


Sub-Saharan Africa

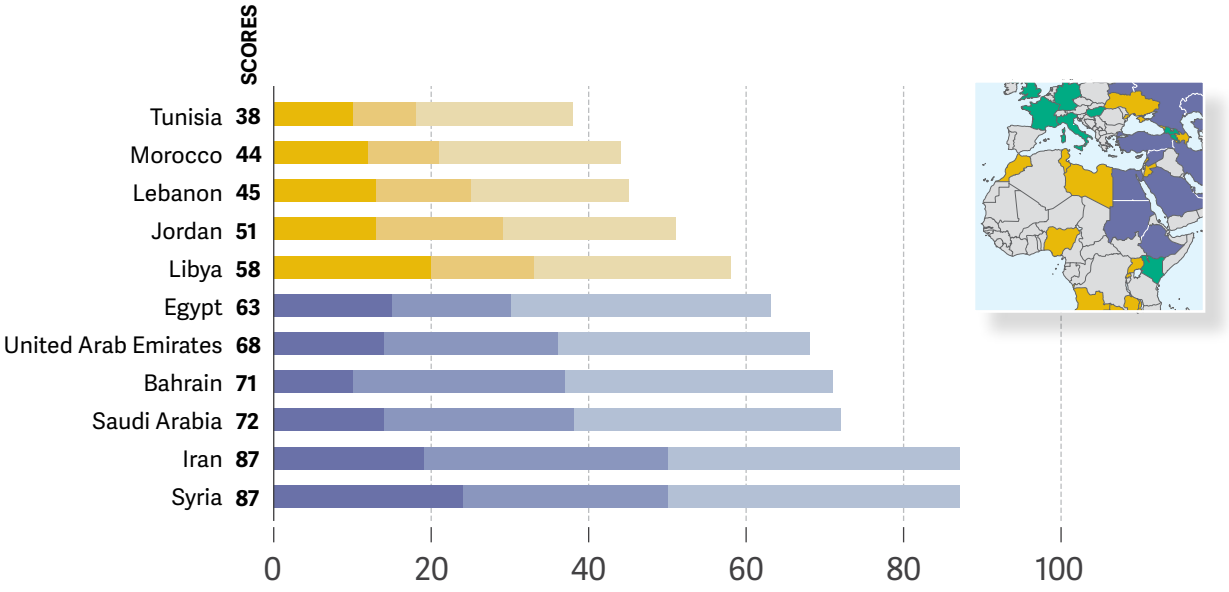




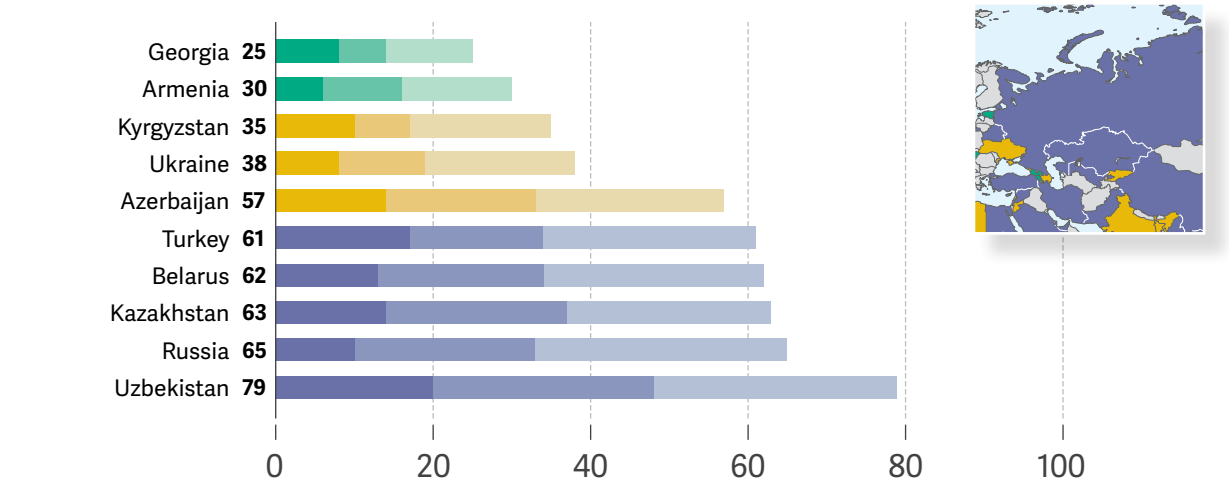
Australia, Canada, European Union, Iceland & United States



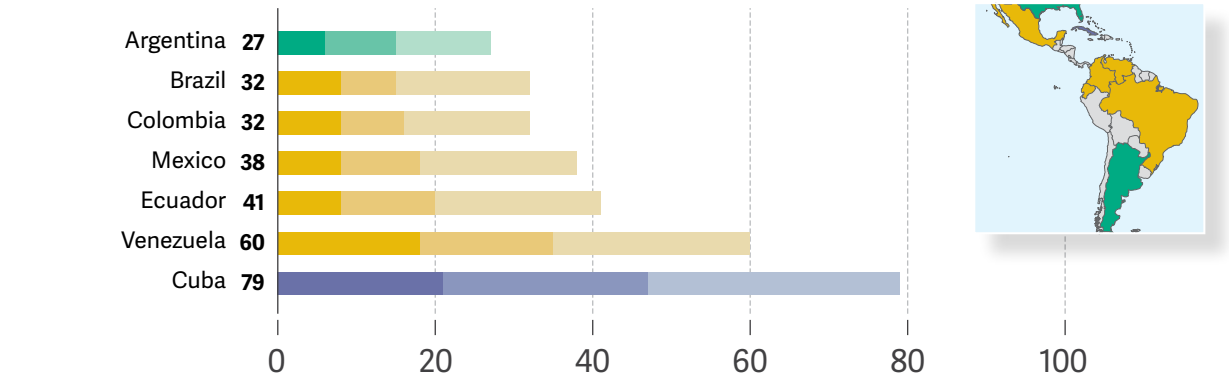
Middle East and North Africa (MENA)



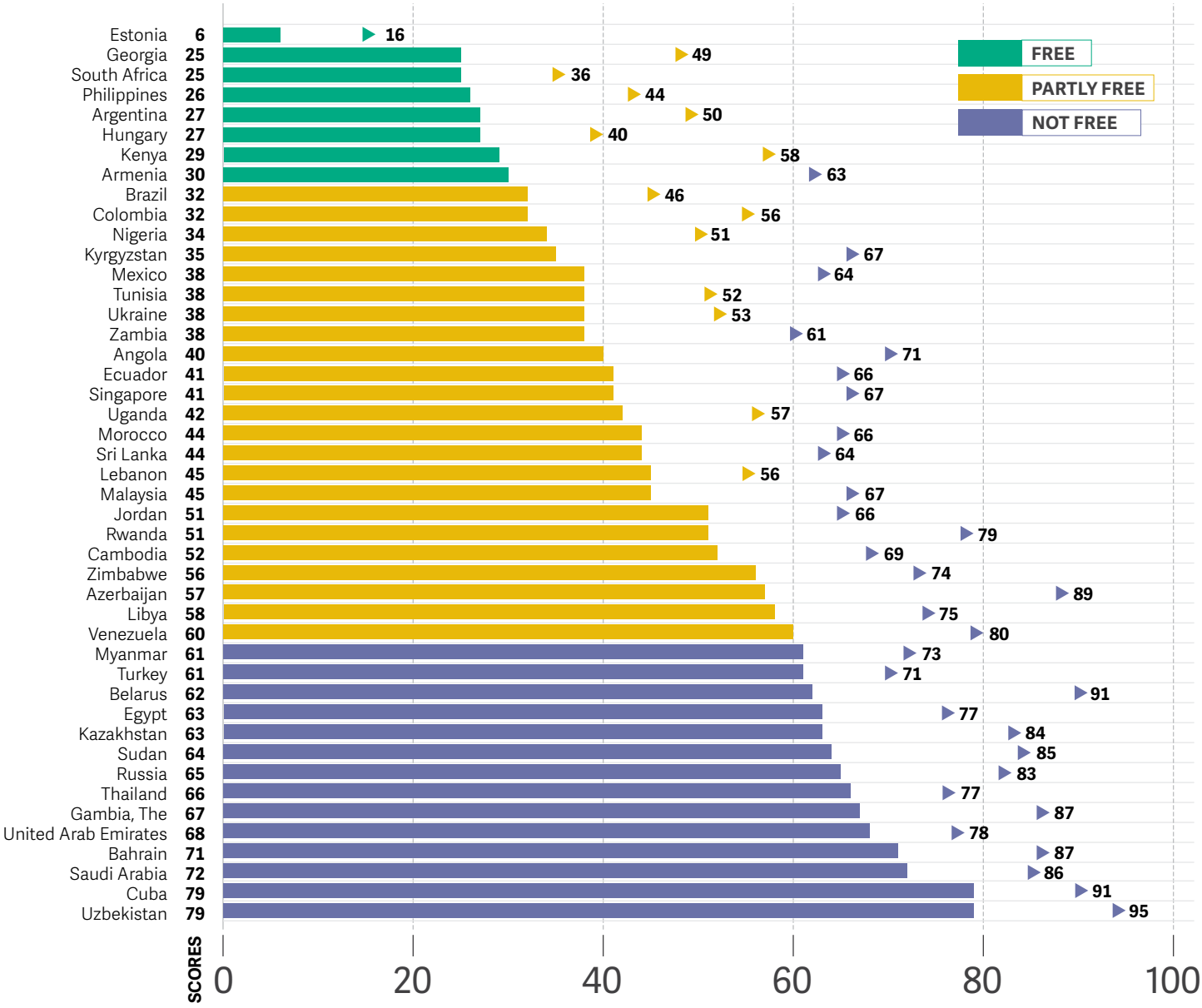
Eurasia



Latin America



INTERNET FREEDOM VS. PRESS FREEDOM

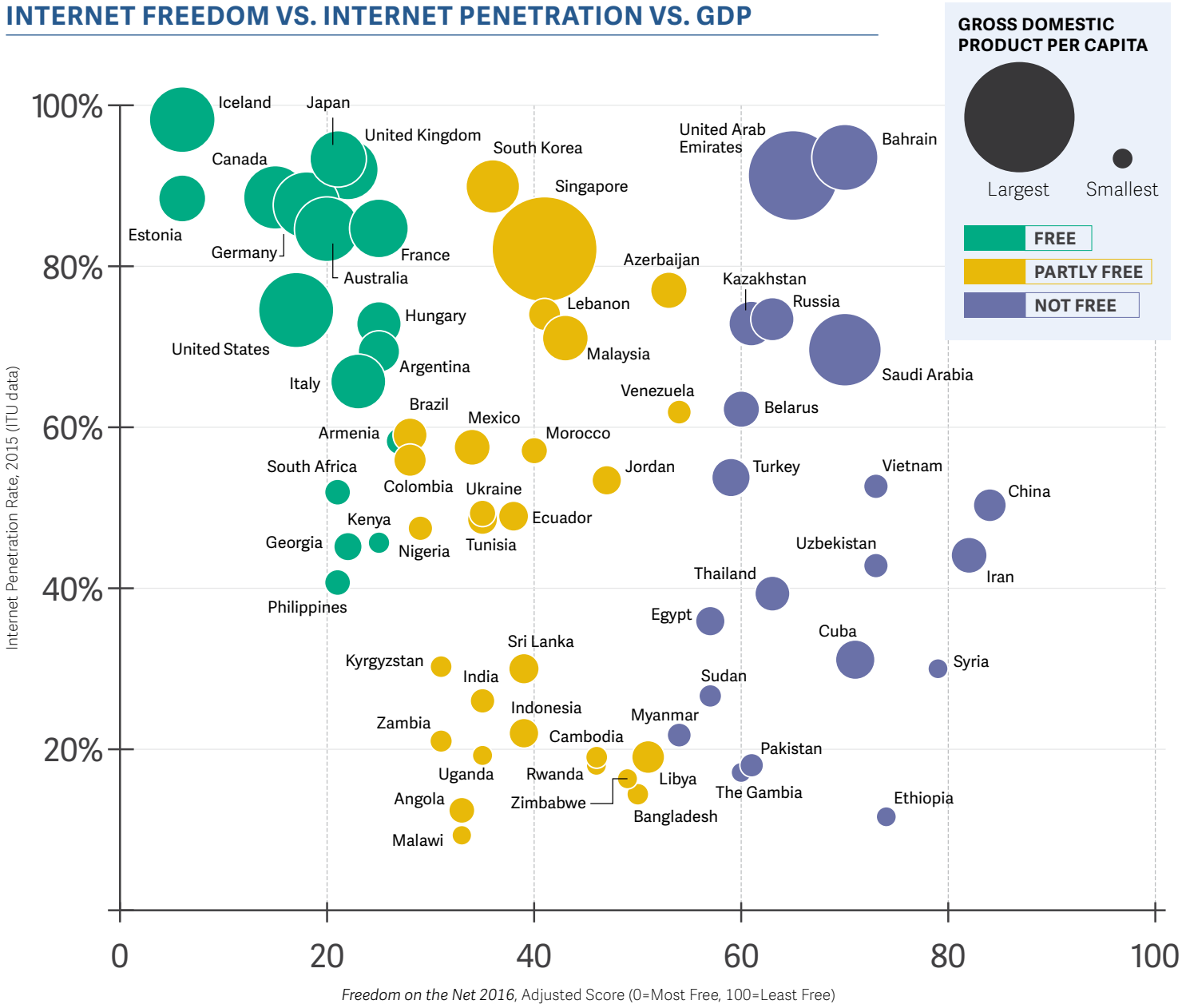


Freedom on the Net 2016 and *Freedom of the Press 2016* scores

In the majority of the 65 countries featured in this report, the internet is significantly more free than news media in general. This difference is evident from the comparison between a country's score on *Freedom on the Net 2016* (represented as the bar graph) and Freedom House's *Freedom of the Press 2016* assessment (represented as the scatterplot, ▶), the latter of which assesses a combination of broadcast, print, and online news media.

The figure above shows the 45 countries with a score difference of 10 points or higher, reflecting how the internet provides citizens with unprecedented access to information, even in the most repressive media environments. Nevertheless, *Freedom on the Net* research has consistently found that government intentions and efforts to control the internet are on the rise, particularly as citizen journalism and traditional media have become more dependent on social media and communications platforms.

INTERNET FREEDOM VS. INTERNET PENETRATION VS. GDP



The figure above depicts the relationship between internet freedom, internet access, and a country's gross domestic product (GDP) per capita. The x-axis considers a country's score in the 2016 edition of *Freedom on the Net*, adjusted to exclude aspects related to internet access. Levels of internet penetration are plotted against the y-axis, using 2015 statistics from the United Nations International Telecommunication Union (ITU). Finally, the size of each plot is indicative of its GDP per capita (at purchasing power parity, PPP), according to the latest figures from the World Bank and International Monetary Fund.

While wealth generally translates to greater access, neither are a decisive indicator of free expression, privacy, or access to information online, as evidenced by the range of internet freedom environments represented at the top of the chart. The Gulf countries lead a cluster of rentier economies investing in high-tech tools to restrict online freedoms. Meanwhile, as "partly free" countries in sub-Saharan Africa and Southeast Asia continue to develop, they would be wise to consider a free and open internet as a mechanism for a prosperous, diversified economy.

OVERVIEW OF SCORE CHANGES

	Overall			Category Scores & Trajectories						Status
Country	FOTN 2015	FOTN 2016	Overall Trajectory	A. Obstacles to Access		B. Limits on Content		C. Violations of User Rights		*Freedom on the Net* 2016
Asia										
Bangladesh	51	56	▼	14	▼	14	▼	28	▼	●
Cambodia	48	52	▼	15	▼	15		22	▼	●
China	88	88		18		30		40		●
India	40	41	▼	12		9	▲	20	▼	●
Indonesia	42	44	▼	11		14	▼	19		●
Japan	22	22		4		7		11		●
Malaysia	43	45	▼	9	▼	16	▼	20	▲	●
Myanmar	63	61	▲	17	▲	17		27	▲	●
Pakistan	69	69		18	▲	20		31	▼	●
Philippines	27	26	▲	9	▲	5		12		●
Singapore	41	41		6		14		21		●
South Korea	34	36	▼	3		15	▼	18	▼	●
Sri Lanka	47	44	▲	14		12	▲	18	▲	●
Thailand	63	66	▼	10	▼	23	▼	33	▼	●
Vietnam	76	76		14	▼	28	▲	34		●
Eurasia										
Armenia	28	30	▼	6		10		14	▼	●
Azerbaijan	56	57	▼	14	▼	19		24		●
Belarus	64	62	▲	13	▲	21		28		●
Georgia	24	25	▼	8	▼	6		11		●
Kazakhstan	61	63	▼	14		23		26	▼	●
Kyrgyzstan	35	35		10	▲	7	▲	18	▼	●
Russia	62	65	▼	10		23		32	▼	●
Turkey	58	61	▼	13		21	▼	27	▼	●
Ukraine	37	38	▼	8		11	▼	19		●
Uzbekistan	78	79	▼	20	▼	28		31		●
Latin America										
Argentina	27	27		6	▲	9	▼	12		●
Brazil	29	32	▼	8	▼	7	▼	17	▼	●
Colombia	32	32		8		8		16		●
Cuba	81	79	▲	21	▲	26	▲	32		●
Ecuador	37	41	▼	8		12	▼	21	▼	●
Mexico	39	38	▲	8	▲	10		20		●
Venezuela	57	60	▼	18	▼	17	▲	25	▼	●

A *Freedom on the Net* score increase represents a negative trajectory (▼) for internet freedom, while a score decrease represents a positive trajectory (▲) for internet freedom.

Country	Overall			Category Scores & Trajectories						Status
	FOTN 2015	FOTN 2016	Overall Trajectory	A. Obstacles to Access		B. Limits on Content		C. Violations of User Rights		*Freedom on the Net* 2016
Middle East & North Africa										
Bahrain	72	71	▲	10	▲	27		34		●
Egypt	61	63	▼	15	▼	15	▼	33	▲	●
Iran	87	87		19	▲	31		37	▼	●
Jordan	50	51	▼	13	▼	16		22		●
Lebanon	45	45		13		12		20		●
Libya	54	58	▼	20		13	▼	25	▼	●
Morocco	43	44	▼	12	▼	9		23		●
Saudi Arabia	73	72	▲	14	▲	24		34		●
Syria	87	87		24		26		37		●
Tunisia	38	38		10		8		20		●
United Arab Emirates	68	68		14		22		32		●
Sub-Saharan Africa										
Angola	39	40	▼	14		7	▲	19	▼	●
Ethiopia	82	83	▼	23		28		32	▼	●
The Gambia	65	67	▼	18		22	▼	27	▼	●
Kenya	29	29		8	▲	7		14	▼	●
Malawi	40	41	▼	16	▼	10	▲	15	▼	●
Nigeria	33	34	▼	10		7	▲	17	▼	●
Rwanda	50	51	▼	10	▲	21	▼	20	▼	●
South Africa	27	25	▲	8		6	▲	11		●
Sudan	65	64	▲	16	▲	18	▲	30	▼	●
Uganda	36	42	▼	13	▼	11	▼	18		●
Zambia	40	38	▲	11		10	▲	17		●
Zimbabwe	56	56		15		16		25		●
Australia, Canada, European Union, Iceland & United States										
Australia	19	21	▼	2		6	▼	13	▼	●
Canada	16	16		3		4		9		●
Estonia	7	6	▲	0	▲	3		3		●
France	24	25	▼	3		6		16	▼	●
Germany	18	19	▼	3	▲	5		11	▼	●
Hungary	24	27	▼	5	▼	10	▼	12	▼	●
Iceland	6	6		1		1		4		●
Italy	23	25	▼	4		6		15	▼	●
United Kingdom	24	23	▲	2		5	▲	16		●
United States	19	18	▲	3		2		13	▲	●

▼ = Decline ▲ = Improvement
Blank = No Change

FREE PARTLY FREE NOT FREE

Freedom House

65 Country Reports

Freedom House

Angola

	2015	2016
Internet Freedom Status	Partly Free	Partly Free
Obstacles to Access (0-25)	14	14
Limits on Content (0-35)	8	7
Violations of User Rights (0-40)	17	19
TOTAL* (0-100)	**39**	**40**

* 0=most free, 100=least free

Population:	**25 million**
Internet Penetration 2015 (ITU):	**12 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- The administrator of a critical Facebook news page was arrested in February 2016, while 17 youth activists were convicted in March on charges of sedition that were substantiated by a single Facebook post (see **Prosecutions and Arrests for Online Activities**).
- SIM card registration requirements were enforced in 2016, threatening mobile phone users' rights to communicate anonymously (see **Surveillance, Privacy, and Anonymity**).
- Leaked Hacking Team emails in July 2015 led to heightened concerns over unlawful surveillance of online and mobile communications (see **Surveillance, Privacy, and Anonymity**).

Introduction

Internet freedom in Angola grew more tenuous during the report's coverage period, as the authoritarian government under President José Eduardo dos Santos took a more aggressive stance towards the internet and its users.

While the government did not employ any technical censorship tactics to limit online content, the president publicly condemned social media during his New Year speech in January 2016, threatening to impose restrictions on platforms for allowing citizens to criticize the government. In August 2016, after this report's coverage period, the National Assembly approved a set of bills to create a new state-controlled regulator called the Angolan Social Communications Regulatory Body. Local analysts said the bills will enable the government to control and censor critical information posted on social media or elsewhere online.

Meanwhile, the government ramped up its crackdown on online activities. In October 2015, police arrested Domingos Magno, who administrates the Facebook page for the citizen news website *Central Angola 7311*. Two days prior to Magno's arrest, he received threats on Facebook, leading observers to believe that he was targeted for his online activism and writings, which have caught the attention of the authorities before. Separately, in March 2016, 17 youth activists were sentenced to between two and eight years in prison on charges of sedition. The prosecution's main piece of evidence was a Facebook post naming a hypothetical new cabinet, though it was not clear that any of the defendants wrote it.

Surveillance became a greater concern, as SIM card registration requirements were enforced, reducing user anonymity and increasing the threat of unchecked government surveillance of users' communications. Internal emails leaked from the surveillance company Hacking Team in July 2015 revealed efforts by Angola's intelligence agency to acquire Hacking Team's notorious Remote Control System (RCS) in 2013, further exacerbating surveillance concerns.

Obstacles to Access

Internet and mobile phone penetration remained low, hindered largely by high costs and poor infrastructure that limit access primarily in urban areas. Senior government officials have direct and indirect shareholder participation in many Angolan ICT companies, providing the government with some level of control over the sector.

Availability and Ease of Access

Access to the internet is low in Angola, with a penetration of 12.4 percent in 2015, according to the latest available data from the International Telecommunications Union (ITU).[1] Mobile phone penetration, while much higher at 61 percent, is below the continent's average of 76 percent.

High costs remain the main hindrance to increasing ICT access for the majority of Angolans whose median annual per capita income was US$720.[2] Unlimited internet subscriptions cost an average of

1 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1cblxxY.

2 Glenn Phelps and Steve Crabtree, "Worldwide, Median Household Income About $10,000," Gallup World, December 16, 2013, http://bit.ly/1j9SsIK.

US$150 per month, while USB dongle devices that provide wireless access cost between US$50 and $60. In urban areas, slightly more affordable subscriptions start at US $50 per month but can still cost as much as US$100 per month for reliable connections. Consequently, few Angolan households have internet access at home. Mobile internet packages come at a monthly cost of about US$45, while internet cafes charge approximately US$1 for 30 minutes. Those who are able go online at their workplaces, especially in the capital, Luanda.

In rural areas, voice and data services can be twice as expensive and of much poorer quality, subject to frequent cuts and extremely slow connection speeds as a result of poor infrastructure. According to the latest data from Akamai's "State of the Internet" report, average broadband connection speed in Angola is 2.7 Mbps (compared to a global average of 6.2 Mbps).[3] ICT access is further hindered by the country's fractured electricity system that serves less than 40 percent of the population, mostly in urban areas.[4]

Restrictions on Connectivity

There were no restrictions on connectivity to internet or mobile phone networks reported during the coverage period.

Angola's domestic backbone is currently comprised of microwave, VSAT, and fibe -optic cables. Connection to the international internet goes through the West Africa Cable System (WACS) and South Atlantic 3 (SAT-3) cable, the latter of which is operated by the state-owned Angola Telecom, which may enable the government to partially control internet connectivity if desired.[5]

In 2014, Angola began construction on the South Atlantic Cable System (SACS), a submarine fibe - optic cable connecting Brazil and Angola that aims to reduce the bandwidth costs associated with the distance that internet traffic cur ently has to travel from Europe and the United States.[6] Construction of SACS is expected to be completed by late 2016.

ICT Market

Senior government officials ha e direct and indirect shareholder participation in many Angolan companies, including ISPs and mobile phone providers, providing the government with some level of control over the ICT sector. The state oil company, Sonangol, owns three of the country's eighteen ISPs (MSTelcom, Nexus, and ACS) and is a major shareholder in two others, UNITEL and Angola Cables, the former of which is the largest ISP.[7] The national telecom company, Angola Telecom, in addition to providing its own internet services, is also a major shareholder in Angola Cables, with 51 percent.[8]

3 Akamai, "State of the Internet, Q1 2016 Report," https://goo.gl/TQH7L7, accessed August 1, 2016.

4 World Bank, "Access to electricity (% of population)," accessed July 31, 2014, http://data.worldbank.org/indicator/EG.ELC.ACCS.ZS.

5 "Sistema de Cabos da África Ocidental entra na fase final" [Cable sys em in Western Africa in final phase] *Portalangop*, October 27, 2012, http://bit.ly/1ZdV7BZ.

6 NEC, "Angola cables to build the world's fi st submarine cable across the South Atlantic," press release, November 4, 2014, http://bit.ly/1MfbXqw.

7 Sonangol's telecom subsidiary, MSTelcom, discloses its full ownership of Nexus and ACS in: *Sonangol Notícias,* "9º Aniversário da Mstelcom: Ligando o País e o Mundo," August 2008, nº 17, Sonangol.

8 "Telecommunications in Angola," *Moses Malone*, http://mosesmalone.ga/Telecommunications_in_Angola.

Mobile phone services are provided by two private operators, UNITEL and Movicel, both of which have indirect ownership ties to the government. For example, 75 percent of UNITEL, the larger mobile phone operator with 80 percent of the market,[9] is held by three entities: Sonangol; a business venture run by Leopoldino do Nascimento, the president's lieutenant general;[10] and the president's billionaire daughter, Isabel dos Santos, according to news reports. Both Leopoldino do Nascimento and Isabel dos Santos sit on the board of UNITEL.[11]

Meanwhile, 80 percent of Movicel is split between fi e ostensibly private Angolan companies—Portmill Investimentos e Telecomunicações with 40 percent, Modus Comunicare with 19 percent, Ipang-Indústria de Papel e Derivados with 10 percent, Lambda with 6 percent, and Novatel with 5 percent—that have majority shareholders who are senior officials within the p esident's office. For example, the majority shareholders of the Angolan investment company Lambda include Minister of Telecommunications and Information Technologies José Carvalho da Rocha, his deputy, and members of both their families.[12] Movicel's remaining capital is held by two state enterprises, Angola Telecom and Empresa Nacional de Correios e Telégrafos de Angola, with 18 percent and 2 percent, respectively.[13]

The 2011 Law on Electronic Communications and Information Company Services further enhances the government's ability to control the country's ICT sector.[14] On paper, the law aims to ensure that ICTs in Angola are developed to play a fundamental role in ensuring citizens' universal access to information, transparency in the public sector, and participatory democracy. It also sets broader goals of poverty alleviation, competitiveness, productivity, employment, and consumer rights.[15]

Nevertheless, this legislation includes several provisions that, if implemented with bad intentions, can threaten online freedom.[16] In particular, the law's provision for universal access to information is dependent upon the state's "creation and promotion of conditions that enable all citizens to access ICT."[17] Accordingly, the law enables the head of government to "intervene when internet service providers jeopardize their social functions or there are situations that gravely compromise the rights of subscribers or users."[18] Because the law does not define "the social functions" or situations" that could be compromised or the scope of intervention allowed, analysts believe that the law empowers the country's authoritarian president to control the ICT sector at will.

Regulatory Bodies

The Ministry of Post and Telecommunications (MCT) is responsible for oversight of the ICT sector, while the Angolan Institute for Communications (INACOM), established in 1999, serves as the

9 Instituto Angolana dos Comunicoçoes, "Estatísticas," http://bit.ly/1R0kxgq.

10 The investment company: Portmill, Investimentos e Telecomunicações.

11 Kerry A. Dolan, "Isabel Dos Santos, Daughter of Angola's President, Is Africa's First Woman Billionaire," *Forbes*, January 23, 2013, http://onforb.es/1s19TrQ.

12 Rafael Marques de Morais, "The Angolan Presidency: The Epicentre of Corruption," *Maka Angola* (blog), accessed October 20, 2015, http://bit.ly/1R0kDod.

13 Rafael Marques de Morais, "The Angolan Presidency: The Epicentre of Corruption," *Maka Angola* (blog).

14 Assembleia Nacional, *Lei das Comunicações Electrónicas e dos Serviços da Sociedade da Informação* (Lei nº 23/11), art. 5.

15 Ministéro Das Telecomunicaçoes e Tecnologias de Informação, "The commitment of Angola in Communications and IT sector according to the Recommendations of the World Summit on the Information Society," (presentation, Geneva, Switzerland, June 2013), http://bit.ly/1jemlbh.

16 Miranda Law Firm, "Angola: Legal News," April-July 2011, http://bit.ly/1GxSrn7.

17 Assembleia Nacional, *Lei das Comunicações Electrónicas e dos Serviços da Sociedade da Informação* (Lei nº 23/11), art. 5.

18 Assembleia Nacional, *Lei das Comunicações Electrónicas e dos Serviços da Sociedade da Informação* (Lei nº 23/11), art. 26, 2.

sector's regulatory body. Reporting to the MCT, INACOM determines the sector's regulations and policies, sets prices for telecommunications services, and issues licenses. On paper, the regulatory body was set up as an independent public institution with both financial and administrati e autonomy from the ministry,[19] though in practice, its autonomy is fairly limited. According to reports by the ITU and World Bank, INACOM is not autonomous in its decision making process,[20] in part due to the ministerial appointment of the director general who can be dismissed for any reason. In addition, the MCT has been known to influence staff appointments, while other ministries a e often involved in sector policy, leading to politically influenced egulatory decisions.

Laws to establish a new Angolan Social Communications Regulatory Body with a remit to control online content were approved in August 2016 (see Legal Environment).

Limits on Content

Online content remained uncensored and unrestricted during the coverage period, though the government may be seeking assistance on censorship strategies from other authoritarian regimes. Legislation passed in August 2016 may give the government more censorship powers.

Blocking and Filtering

To date, there have been no known incidents of the government blocking or fil ering ICT content in Angola, and there are no restrictions on the type of information that can be exchanged through digital media technologies. Social media and communications apps such as YouTube, Facebook, Twitter, and international blog-hosting services are freely available.

Nevertheless, censorship of news and information in the traditional media sphere is common, and the president publicly stated intentions to regulate social media speech during his New Year speech in January 2016. The government subsequently followed through with the passage of bills in August that reportedly empower a new regulatory body with the ability to control online speech (see Legal Environment). In another concerning development, the independent online news outlet *Club-K* reported in July 2015 that the Angolan authorities had been seeking technical assistance from North Korea to restrict access to critical websites.[21]

Content Removal

There were no reports of forced content removal during the coverage period, though informal government demands on users to remove content from the internet have been documented periodically. In one case, a Facebook user arrested in April 2015 for a critical post about a military general was forced to remove the post and apologize in exchange for his release.[22]

In May 2015, a court found journalist and blogger Rafael Marques de Morais guilty of criminal defamation for his 2011 book implicating the Angolan military in alleged torture and corruption

19 Russell Southwood, "The Case for 'Open Access' Communications Infrastructure in Africa: The SAT-3/WASC cable – Angola case study," Association for Progressive Communications, accessed August 30, 2013, 5, http://bit.ly/1N1sn8O.

20 International Telecommunication Union, "Angola Profile (la est data available: 2013)."

21 "Regime ensaia sistema para banir sites críticos," *Club-K*, July 27, 2015, http://bit.ly/1JUHyfl.

22 Interview by Freedom House consultant in May 2015.

in the country's diamond industry. In addition to a six-month suspended prison sentence, the court ordered all online copies and references to de Morais's book to be removed.[23] Given the impossibility of the task, observers believe the court intended the demand to serve as a threat, leaving open the possibility of holding de Morais responsible if the content remained accessible. However, there were no reports of restrictions on the book's accessibility online since the May 2015 ruling, and it remains available outside Angola.

Media, Diversity, and Content Manipulation

As a result of low rates of ICT access, radio, television, and print outlets—which are subject to high levels of government interference—remain the primary sources of information for the majority of Angolans. The president and members of the ruling People's Movement for the Liberation of Angola (MPLA) party own and tightly control a majority of the country's media outlets, including those that are the most widely disseminated and accessed. Of the dozen or so privately owned newspapers, most are held by individuals connected to the government.

Independent news outlets critical of the government do exist, with *Folha8* being the most prominent, though its audience is reached primarily through its print publication. *Rede Angola,* an independent news blog based in Portugal, is one of the main sources of alternative and independent online news on Angola,[24] alongside the news blogs *Club-K* and *Maka Angola*, which is run by journalist Rafael Marques de Morais. Nonetheless, the online information landscape lacks diversity and is unable to represent a variety of groups and viewpoints throughout the country due to both the concentration of internet access in urban areas and the limited space for critical voices in Angola's general media sphere.

In addition, independent outlets, both online and in print, are constrained economically by the lack of advertising revenue from both state and private sources, since it is often denied to news outlets that publish critical stories about the government. According to an Angolan media observer, *Rede Angola* struggled to receive advertising revenue from both private and public sources in 2015 due to the critical cartoons it often publishes. It has only managed to stay afl at through financing f om its wealthy owner, a Brazilian political communications mogul.

Government efforts to manipulate online content are periodically reported. Some independent online news outlets report receiving regular calls from government officials di ecting them to tone down or refrain from reporting on certain issues. For example, in 2015, editors at *Rede Angola*, reportedly received instructions from the authorities not to publish any news about the ongoing defamation case against journalist and blogger Rafael Marques de Morais (see Content Removal).[25]

Self-censorship is pervasive and commonly practiced by journalists in both state-run and private print outlets, though bloggers and social media users are less reluctant to express criticism of the president and ruling party. In the past few years, the internet and social media have become the last frontier for independent voices, with journalists, activists and opposition parties increasingly turning to digital platforms as a means to sidestep the country's longstanding restrictions on traditional media. Nevertheless, there have been anecdotal reports of online self-censorship becoming more

23 Paul Gallagher, "Celebrities join signatories calling on Angolan president to drop prosecution of blood diamonds author Rafael Marques de Morais," *Independent*, June 2, 2015, http://ind.pn/1hsfGbM.

24 *Rede Angola* website: http://www.redeangola.info/.

25 Based on interviews with anonymous online journalists and editors.

prevalent, reinforced by the recent arrests of social media users and bloggers.[26] Taboo topics related to corruption, abuse of power, land grabs, police brutality, and demolitions are often avoided.

Digital Activism

Social media is the leading platform for citizens to criticize the government and react to alleged wrongdoings. Youth groups in particular have increasingly floc ed to Facebook to call out government corruption, reflecting a gradual eakening of the culture of fear within civil society.[27]

Digital activism was significant following the ar est of 17 youth activists in June 2015 and helped mobilize protests against their extended pre-trial detention and ill-treatment in prison. Nonetheless, subsequent arrests of protesters and the Facebook page administrator for the news website *Central Angola 7311* have led to a more muted use of digital media to organize and provide critical commentary in the past year (see Prosecutions and Arrests for Online Activities).

Violations of User Rights

New legislation passed in August 2016 empowers the government with the ability to control social media and penalize online speech. The administrator of a critical Facebook news page was arrested in February 2016, while 17 youth activists were convicted in March on charges of sedition based on a Facebook post. Leaked Hacking Team emails in July 2015 led to heightened concerns over unlawful surveillance of online and mobile communications.

Legal Environment

The Angolan constitution provides for freedom of expression and the press, though in practice, the authorities routinely flout these rights. tringent laws regarding state security and defamation run counter to constitutional guarantees, such as Article 26 of the 2010 state security law that penalizes individuals who insult the country or president in "public meetings or by disseminating words, images, writings, or sound" with prison sentences of up to three years.[28] The 2006 press law holds authors, editors, or directors of a publication criminally liable for libelous content.[29] If the author does not reside in the country or the text is not signed, the law establishes the circumstances in which the editor, director, or both may be held criminally responsible for grievous content.[30] Defamation is a crime punishable by imprisonment, while politicians enjoy immunity from all prosecution. Meanwhile, the judiciary is subject to considerable political influence, with Sup eme Court justices appointed to life terms by the president and without legislative approval.

The Law on Electronic Communications and Information Company Services, enacted in August 2011, provides for citizens' rights to privacy and security online, among other provisions regulating

26 Based on interviews with internet users and bloggers.

27 Central Angola 7311, website, http://centralangola7311.net/; Central Angola 7311, Facebook page, http://on.fb.me/1VGCP7Y.

28 Human Rights Watch, "Angola: Revise New Security Law, Free Prisoners in Cabinda," December 9, 2010, http://bit.ly/1RvD6tN.

29 Art. 71, 2, Assembleia Nacional, *Lei de Imprensa* (Lei 7/06), 2006, http://www.wipo.int/wipolex/en/text.jsp?file_id=17955 .

30 Art. 71, 2, Assembleia Nacional, *Lei de Imprensa* (Lei 7/06), 2006.

telecommunications. Nevertheless, the law also includes problematic aspects that may infringe on internet access (see ICT Market).[31]

In August 2016, after this report's coverage period, the National Assembly approved a set of bills that creates a new state-controlled regulator called the Angolan Social Communications Regulatory Body.[32] Local analysts said the bills will enable the government to control and censor critical information posted on social media or elsewhere online.[33] The legislation came after President dos Santos called for stricter regulation of social media in January 2016.[34]

Prosecutions and Detentions for Online Activities

Arrests and prosecutions for online activities have become more frequent in the past few years. In October 2015, one of the main reporters for the "Central Angola 7311" citizen news site and an administrator of the group's Facebook page, Domingos Magno, was arrested en route to hear the State of the Nation address. Charged with "false pretenses" for allegedly possessing a false press pass, he spent one month in prison, during which time he was interrogated in relation to his online activities. He also received threats on Facebook prior to his arrest (see Intimidation and Violence).[35] The charges were still pending in mid-2016.

In a high profile case, 17 activists ere convicted of sedition in March 2016 and sentenced to between two and eight years in prison. The charges stemmed from their participation in a book club at which they were discussing a book about civil disobedience to authoritarian rule. As the sole piece of evidence of the group's alleged plot to overthrow the government, the prosecution introduced a Facebook post that proposed a hypothetical alternative government, with prominent activists named in key government positions.[36] On appeal, the Supreme Court granted the activists conditional release under house arrest in June 2016.

Surveillance, Privacy, and Anonymity

The government's ability to monitor and intercept the data and communications of Angolan citizens without adequate oversight is a major concern, particularly among human rights activists and journalists, though the full extent of the government's surveillance capabilities and practices is unknown. Sophisticated spyware discovered logging activities on an investigative journalist's laptop in 2013 suggests that, at a minimum, the government engages in the targeted surveillance of select individuals (see Technical Attacks).[37] Investigative reporting over the past few years has unearthed

31 Art. 71, 2, Assembleia Nacional, *Lei de Imprensa* (Lei 7/06), 2006, art. 26º, 2.

32 D Quaresma Dos Santos, "Angola passes laws to crack down on press and social media," *The Guardian*, August 19, 2016, https://www.theguardian.com/world/2016/aug/19/angola-passes-laws-to-crack-down-on-press-and-social-media

33 D Quaresma Dos Santos, "Angola's latest ply to silence critics: A regulatory body to censor social media," Maka Angola (blog), August 16, 2016, http://www.makaangola.org/2016/08/angolas-latest-ploy-to-silence-critics-a-regulatory-body-to-censor-social-media/

34 Divya Kishore, "Media outlets in Angola face tighter restrictions after legal crackdown," *International Business Times*, August 20, 2016, http://www.ibtimes.co.uk/media-outlets-angola-face-tighter-restrictions-after-legal-crackdown-1576942

35 Rafael Marques de Morais, "President's speech nabs another political prisoner," Maka Angola (blog), October 20, 2015, http://www.makaangola.org/2015/10/presidents-speech-nabs-another-political-prisoner/

36 Zenaida Machado, "Dispatches: Basic Rights Still a Pipe Dream in Angola," Human Rights Watch, March 31, 2016, https://www.hrw.org/news/2016/03/31/dispatches-basic-rights-still-pipe-dream-angola

37 Janet Gunter, "Digital Surveillance in Angola and Other "Less Important" African Countries," *Global Voices Advocacy*, February 26, 2014, http://bit.ly/1LjKxn4.

different government plans to implement electronic monitoring systems that could track email and other digital communications.[38] Recent investigations have revealed increased engagement with the Chinese government on surveillance methods.[39]

In June 2015, Wikileaks published leaked internal emails from the Italian surveillance equipment company Hacking Team, which revealed efforts by Angola's intelligence agency, SINSE, to acquire Hacking Team's notorious Remote Control System (RCS) in 2013.[40] Sold to numerous repressive regimes around the world, RCS spyware has the ability to steal files and passwords and intercept Skype communications, among other features. The documents did not reveal whether the Angolan government eventually purchased or installed the spyware.

Meanwhile, SIM card registration requirements enacted in 2014 were enforced in 2016, threatening mobile phone users' rights to communicate anonymously. Users were given until the end of February 2016 to register existing SIM cards or be disconnected. SIM cards must be registered directly with INACOM, the ICT regulator that operates under government oversight (see Regulatory Bodies). The process requires an identity card or driving license and tax card for national citizens, or a passport with a valid visa for visitors.[41]

Strong state influence in the ownership structure of Angola's telecoms, particularly mobile phone operators, suggests that the authorities are likely able to wield their influence over service providers and require them to assist in the monitoring of communications, if desired.[42] Such interweaving of political and business interests through family connections is compounded by the lack of rule of law.

Intimidation and Violence

Violence and harassment against journalists in the traditional media sphere is common in Angola, and online activists have been increasingly targeted. Two days before Domingos Magno was detained in October 2015 (see Prosecutions and Detentions for Online Activities), he received warnings through his Facebook page advising him to distance himself from his friends who were known political activists and opposition figures, or face serious consequences.

While covering a peaceful protest against the detention of the 17 youth activists in August 2015, Rafael Marques de Morais, who runs the *Maka Angola* blog, was repeatedly detained and released, and his camera equipment was repeatedly seized and returned. Marques was later held at the airport in September 2015 when returning from a trip to South Africa, supposedly due to a computer error involving outdated orders banning his movement out of the country.[43]

38 See, *Freedom on the Net 2015*, "Angola" country report, https://freedomhouse.org/report/freedom-net/2015/angola.

39 Freedom House consultant interviews, May 2016.

40 Daniel Finnan, "Kenyan government asked Hacking Team to attack dissident website," *Radio France Internationale*, July 17, 2015, http://rfi.my/1jc5C_p.

41 See, INACOME's website, http://www.inacom.gov.ao/registo/index.html

42 For instance, the top adviser to the head of the Intelligence Bureau at the Presidency, General Leopoldino do Nascimento, is also the chairman and shareholder of Unitel. Meanwhile, the head of the Intelligence Bureau, General Manuel Hélder Vieira Dias "Kopelipa," holds a majority share (about 59 percent) in Movicel. The deputy CEO and Chief Technology Officer of Unitel, Amílcar Safeca, is the brother of Aristides Safeca, the secretary of ICTs who in turn is a shareholder of Movicel.

43 Rafael Marques de Morais, "There is no place like home unless you are banned," Maka Angola (blog), September 10, 2015, http://www.makaangola.org/2015/09/there-is-no-place-like-home-unless-you-are-banned/.

Technical Attacks

Independent and diaspora news websites have been taken down by technical attacks in the past, though there were no reported incidents during the coverage period. In early 2015, the critical news blog *Maka Angola* was attacked and taken down for several days at a time in the lead-up to the criminal defamation case against the outlet's owner, Rafael Marques de Morais (see Content Removal). A frequent target of technical violence, de Morais was previously attacked with customized malware on his personal laptop,[44] which international experts linked to a multinational with strong ties to Angolan military officials [45] Marques now receives technical assistance from Jigsaw's Project Shield, which protects websites from powerful technical attacks.[46]

The hacking collective Anonymous claimed responsibility for taking down more than 20 Angolan government websites in response to the convictions of 17 youth activists in March 2016.[47]

44 There is a detailed account of how the malware was discovered during an international conference. See: Michael Moynihan, "Hackers are Spying On You: Inside the World of Digital Espionage," *Newsweek*, May 29, 2013, http://bit.ly/1s29LJY.

45 Gunter, "Digital Surveillance in Angola and Other 'Less Important' African Countries."

46 Alfred Ng, "Google's Project Shield defends free speech from botnet scourge," CNET, September 29, 2016, https://www.cnet.com/news/google-project-shield-botnet-distributed-denial-of-service-attack-ddos-brian-krebs/

47 "'Anonymous' hackers cyber-attack Angolan government," March 30, 2016, http://www.bbc.com/news/world-africa-35927474

Freedom House

Argentina

	2015	2016
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	7	6
Limits on Content (0-35)	8	9
Violations of User Rights (0-40)	12	12
TOTAL* (0-100)	**27**	**27**

* 0=most free, 100=least free

Population:	**43.4 million**
Internet Penetration 2015 (ITU):	**69 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2016 Status:	**Partly Free**

Key Developments: June 2015 – May 2016

- An emergency decree issued in December 2015 under newly-elected President Mauricio Macri has brought swift changes to Argentina's regulatory framework with the creation of the National Communications Authority (ENACOM). A special commission under the Ministry of Communications will be in charge of drafting a new law to unify digital and broadcast media legislation (See **Regulatory Bodies**).
- On the grounds that certain state-run media served partisan interests under the former government, thousands of news items disappeared from the website of news agency *Infojus Noticias* in February 2016. The articles, which covered issues such as institutional violence, gender-based violence, crimes against humanity and money laundering, were republished on a new website in May 2016 (See **Content Removal**).
- In the lead-up to President Macri's inauguration in early December 2015, *Página 12* denounced a cyberattack on its website which lasted nearly a week. News outlet *Diario Registrado* also reportedly suffered a similar attack on December 11, and a few days later *Clarín* reported a two-hour long attack (See **Technical Attacks**).

Introduction

Marked by the presidential handover and a series of regulatory changes affecting the digital and broadcast media sectors, Argentina's internet freedom environment remained strong as internet penetration continued to increase during this period.

After 12 years of governments led by Cristina Fernández de Kirchner and her late husband, Néstor Kirchner, the election of a center-right government headed by President Mauricio Macri in November 2015 has significantly shi ted public policy priorities.

On December 29, 2015, President Macri issued a Necessity and Urgency Decree (DNU 267/2015), merging the Federal Authority of Audiovisual Communication Services (AFSCA) and the Federal Authority for Information Technology and Communications (AFTIC) into a new regulatory body: the National Communications Authority (ENACOM). The move sparked criticism among opponents, notably due to the possibility of unwarranted executive influence in the composition f the new regulatory body, comprised of four directors chosen by the executive branch and three proposed by the parliament. The use of emergency decrees to significantly amend the egulatory framework also came under fi e. Aiming to promote convergence and more homogenous norms, a special commission will be in charge of drafting a new law to unify digital and broadcast media legislation introduced under the previous administration.

The government does not regularly block or fil er the internet, and lower courts have further clarified takedown criteria following the landmark decision by the Argentine Supreme Court on intermediary liability in October 2014, which established a judicial notice and takedown system. During the coverage period, one case of blocking due to a court order was reported, as part of a criminal case against software developer Joaquín Sorianello, who had detected a security deficiency in the e- oting system developed for mayoral elections in the city of Buenos Aires.

However, several bills introduced in Congress in 2015 and 2016 would regulate the removal or blocking of content. Some of them seek to implement the so-called "right to be forgotten," giving individuals the power to request search engines to delist certain information. Others bills aim to regulate intermediary liability in general, establishing either a judicial notice and takedown system for all cases, or a judicial notice and takedown system for some cases and an administrative, or private notice and takedown system for others. All of these bills remained at early stages in the legislative process.

Obstacles to Access

Access to the internet has increased consistently in Argentina over the past decade. However, there are still infrastructural weaknesses that contribute to a digital divide, especially between urban and rural areas. Barely a year after Congress approved the Argentina Digital Law, newly elected President Mauricio Macri issued a decree changing several provisions, including modifications to the regulatory entity. It also created a commission to reform and unify legislation to promote convergence between the telecommunications and audiovisual sectors.

Availability and Ease of Access

Internet access has consistently been on the rise in Argentina. Statistics published by the Interna-

tional Telecommunications Union (ITU) showed a 69 percent internet penetration rate in the country by the end of 2015, up from 65 percent in 2014, and 34 percent in 2009.[1] Some 33 million people representing 80 percent of the population actively use the internet, according to a report published by We Are Social in January 2016.[2]

An emergency decree issued by newly-elected President Macri in December 2015 introduced reforms to the Argentina Digital Law, which was approved by Congress in December 2014 with the aim of guaranteeing socially and geographically equitable telecommunications services to all citizens. Under the emergency decree, a special commission will be in charge of drafting a new law to promote convergence between the telecommunications and audiovisual sectors, by unifying the Broadcast Media Law and the Argentina Digital Law. According to the decree, such changes would: "allow better decision-making by the national government and would provide legal certainty and predictability."[3]

The National Institute of Statistics and Census (INDEC) recorded some 15.4 million residential internet access points in September 2015—up from 13.3 million in September 2014.[4] Mobile access points represented 60 percent, an increase of nearly 16 percent from 2014, while fi ed internet access points represented 40 percent, up by 5 percent from 2014. According to INDEC's national survey in October 2015, 67 percent of homes in the country had access to computers and 61.8 percent had access to the internet.[5]

The majority of ISP subscriptions are broadband, while dial-up connections account for less than one percent of the total.[6] In another report from June 2015, INDEC stated that there were 2.9 million internet subscriptions belonging to organizations, which represents a 20 percent increase over the previous year.[7] Some 390 of these institutions, which include schools, libraries, and nongovernmental organizations, benefi ed from free internet access, according to INDEC's September 2014 report.[8] The Buenos Aires open government website lists more than 400 public access Wi-Fi spots in the capital city.[9]

Measurements of internet speed in Argentina vary, but a range of sources show that the country lags behind global averages in broadband speed. Akamai reported an average broadband speed of 5.3 Mbps in Argentina in the fi st quarter of 2016, compared to a global average of 6.3 Mbps.[10] According to the United Nations Economic Commission for Latin America and the Caribbean (CEPAL)

1 International Telecommunication Union (ITU), "Percentage of Individuals using the internet, 2000-2015," accessed September 1, 2015, http://bit.ly/2bw4qL4.

2 We are Social, "Digital in 2016" [Sources: ITU, Internet World Stats, CIA, national governments ministries and industry bodies, UN, U.S. Census Bureau for population data], http://bit.ly/1T462wk.

3 Decree 267/2015, December 29, 2015, http://bit.ly/1UycLzB; See also: José Crettaz, "El resumen del DNU que reforma las leyes de medios y de telecomunicaciones" [Summary of the DNU that reforms the media and telecommunications laws], *La Nación,* December 30, 2015, http://bit.ly/1YPd0JP.

4 National Institute of Statistics and Censuses (INDEC), "Informe sobre los accesos a Internet" [Report on Internet Access], March 4, 2016, http://bit.ly/1RBIRqU.

5 INDEC, "Encuesta Nacional sobre Acceso y Uso de Tecnologías de la Información y la Comunicación" [National Survey on Access and Use of Information and Communication Technologies], Results for May-July 2015, October 5, 2015, http://bit.ly/1UL3hQq.

6 INDEC, "Accesos a Internet" [Internet Access], December 16, 2014, http://bit.ly/1G6JS1H.

7 INDEC, "Accesos a Internet" [Internet Access], September 15, 2015, http://bit.ly/1VvFNzr.

8 INDEC, "Accesos a Internet" [Internet Access], September 15, 2015, http://bit.ly/1VvFNzr.

9 Buenos Aires Data, "List of Public Wi-Fi spots," accessed September 2016, http://bit.ly/1Fp42mz.

10 Akamai, "Internet Broadband adoption," State of Internet Report 2016, http://akamai.me/1OcG9aE.

and the Organization for Economic Co-operation and Development (OECD), Argentina registered broadband download speeds of 6.34 Mbps in 2015, below the regional average of 7.26 Mbps.[11]

Mobile phone penetration continues to grow in Argentina, as INDEC's national survey noted a penetration rate of 89.6 percent in 2016, considerably higher than fi ed phone lines at 62.4 percent.[12] ITU estimated 144 mobile phone subscriptions per 100 inhabitants in 2015.[13] Not only did mobile subscriptions increase, but telephone services registered a 15.2 percent decrease in urban calls, according to INDEC.[14]

Mobile phone penetration could increase even further with the announcement of fare increases for fi ed phone lines in March 2016.[15] Prices for mobile phone subscriptions are relatively high in Argentina, and it was labeled as one of the most expensive countries in Latin America for mobile services in 2014.[16] In August 2014, the government launched a prepaid mobile phone plan with affordable prices,[17] which was extended under President Macri's government.[18] In February 2016 the National Modernization Ministry also announced an agreement with mobile phone companies operating in the country to swap 2G mobile technology for devices with 4G.[19] Despite the launch of 4G networks, the Cisco Visual Networking Index 2014-2019 estimated that only 10 percent of users in Argentina will be using 4G networks by 2019.[20]

An average fi ed-broadband plan costs US$40 per month according to the ITU,[21] or U$S32 according to the Regional Dialogue on Information Society (DIRSI),[22] whereas the minimum monthly salary in the country is around US$404.[23] Given changes introduced in the Argentina Digital Law, there is a chance the prices are going to increase even further in 2016.[24] According to a policy brief by DIRSI,

11 CEPAL, "Estado de la banda ancha en América Latina y el Caribe 2015," [State of Broadband in Latin America and the Caribbean 2015], July 2015, http://bit.ly/1SPjYeJ; "Las conexiones de internet más rápidas y más lentas de América Latina" [The quickest and slowest internet connections in Latin America], *BBC Mundo,* August 16, 2015, http://bbc.in/1UTlHNB.

12 INDEC, "Encuesta Nacional sobre Acceso y Uso de Tecnologías de la Información y la Comunicación" [National Survey on Access and Use of Information and Communication Technologies], Results for May-July 2015, October 5, 2015, http://bit.ly/1UL3hQq.

13 ITU, "Mobile-cellular subscriptions," 2000-2015, http://bit.ly/2bfvlcE.

14 INDEC, "Informe de prensa de servicios públicos" [Press Release on Public Services], November 2015, http://bit.ly/1REZ0vG.

15 The recent decree allowed companies to establish prices for fi ed telephone services, which had not been modified for 15 years due to previous government regulations. See: "Acuerdan un aumento de 185% en el abono para la telefonía fija" [Agreement to increase fi ed telephone rates by 185 percent], *Clarín*, March 27, 2016, http://clar.in/25ujOx5.

16 Laura Zommer, "Nuestros precios de celulares, al tope del mundo" [Our mobile phone prices, the highest in the world], *La Nación,* November 10, 2014, http://bit.ly/1tThzAr; Diario BAE, "Argentina y Brasil, los países más caros de la región para hablar por celular" [Argentina and Brazil, the most expensive countries in the region to talk on mobile phones], *Media Telecom,* March 4, 2015, http://bit.ly/1Pp1Va6.

17 "Todo lo que hay que saber del Plan Prepago Nacional" [All there is to know about the National Prepaid Plan], *Télam*, August 8, 2014, http://bit.ly/1mlM3F6.

18 "El Gobierno prorrogó el plan prepago nacional con descuentos de hasta el 50%" [Government extended national prepaid plan with discounts of up to 50 percent], *Télam,* August 30, 2016, http://bit.ly/2db3bkz.

19 "El Gobierno prevé lanzar un plan canje de celulares para mejorar las comunicaciones móviles" [Government plans to launch a swap plan for cellphones to improve mobile communications], *La Nación* , February 22, 2016 http://bit.ly/20RkRlP; "Cómo es el plan canje de celulares que el Gobierno lanzará en 30 días" [The cell phone swap plan that the government will launch in 30 days], *La Nación*, February 23, 2016, http://bit.ly/1oFgoqI.

20 José Crettaz, "Movilidad 4G: en 2019, sólo el 10% de los dispositivos usará la nueva red"[4G mobility: in 2019, only 10 percent of devices will use the new network], *La Nación*, February 6, 2015, http://bit.ly/1C1MpIk.

21 ITU, Measuring the Information Society Report, 2014, http://bit.ly/1NUbnkf.

22 Guillermo Tomoyose, "Un mapa interactivo muestra el nivel de acceso a Internet en la Argentina," [An interactive map shows the level of access to Internet in Argentina], accessed March2016, http://bit.ly/1TgNfxY.

23 Resolution 4/2015, *Infoleg*, http://bit.ly/1WURePJte.

24 Decree 267/2015, *Infoleg,* http://bit.ly/1UzLvkT.

broadband plans have gotten more expensive, with an estimated price variation of 40 percent between 2014 and 2015.[25]

In May 2016, President Macri announced heavy infrastructure investments through the "Federal Internet Plan," promising to bring quality broadband to 29 million people within the space of two years.[26] The initiative would use and expand the fibe -optic network developed under the previous government's "Argentina Connected" plan launched in 2010. Contracted to the state-owned company ARSAT, this project sought to extend approximately 58,000 kilometers of fibe -optic cable across the country,[27] with the ultimate goal of reaching more than fi e million people.[28] Also as part of the Argentina Connected initiative, Argentina's fi st telecommunications satellites, Arsat-1 and Arsat-2, were launched in October 2014 and September 2015, respectively.[29] The planned construction of Arsat-3 was suspended in March 2016, as authorities worked on making Arsat-2 financially indepe - dent.[30] This announcement has been criticized by the previous administration, as well as news about layoffs at ARSAT.[31]

Under the Argentina Connected Plan, the National Ministry of Planning, Public Investments and Services also reported the establishment of more than 280 Access to Knowledge Centers, public spaces that provide free access to ICTs.[32] The "Digital Country Plan" (Plan País Digital) launched in June 2016 will also seek to provide free public Wi-Fi in more than 1,000 municipalities across the country.[33]

Under the previous government, the Connect Equality initiative launched in 2010 sought to foster basic digital education across the country.[34] As of March 2016, more than 5.3 million netbooks had been delivered to public high school students. In March 2016, members of the program reported

25 María Fernanda Viecens, "Precio, calidad y asequibilidad de la banda ancha: las disparidades entre los países de la región son muy importantes" [Price, quality and affordability of broadband: disparities between countries in the region are very important], DIRSI Policy Brief 2016, http://bit.ly/1TAPpcm.

26 "En qué consiste el Plan Federal de Internet que presentó hoy Mauricio Macri" [The Federal Internet Plan presented today by Mauricio Macri], *La Nación,* May 17, 2016, http://bit.ly/1NxeQu8.

27 Ministerio de Planificación, *Plan Nacional de Telecomunicaciones "Argentina Conectada"* [National Telecommunications Plan of Argentina Connected], 2010-2015, 51-55, http://bit.ly/1rW9rMr.

28 "ARSAT presta servicios al 30% de la población del país" [ARSAT services 30 percent of the population in the country], *Revista Fibra*, December 9, 2015, http://bit.ly/1SdSBHL.

29 "Lanzan el Arsat 1, el primer satélite geoestacionario" [Arsat 1, the fi st geostationary satellite, is launched], *Infobae,* October 16, 2014, http://bit.ly/1zd1Otw; "El Arsat-1 llegó a la órbita geoestacionaria" [Arsat-1 reached the geostationary orbit], *La Nación*, October 27, 2014, http://bit.ly/1wv256C; "Lanzaron con éxito el Arsat-2 y ya está en órbita" [Successful launch of Arsat-2, now in orbit], *Clarín*, October 30, 2015,http://clar.in/1KTyt8h; "Lanzaron el satélite argentino Arsat-2 desde la Guyana Francesa" [Argentine satellite Arsat-2 launched from French Guyana], *Perfil,* October 30, 2015, http://bit.ly/21H3N2g.

30 "Arsat suspendió la construcción del tercer satélite argentino" [Arsat suspended the construction of the third Argentinian satellite], March 29, 2016, *La Nación,* http://bit.ly/1pYQBun ; "Por el congelamiento del proyecto Arsat-3, peligran 600 puestos de trabajo" [Freeze on Arsat-3 project puts 600 jobs at risk], *Clarín*, March 29, 2016, http://clar.in/1RFHyaj.

31 "Denuncian despidos por "cuestiones políticas" en Arsat" [Dismissals for "political reasons" are denounced in Arsat], *La Nación*, January 12, 2016, http://bit.ly/1VwO5qW; "Arsat admite que despidió a 22 empleados:," [Arsat admits that 22 employees were fi ed], *La Nación*, January 13, 2016, http://bit.ly/1pGctKR.

32 Ministry of Planning, "Logros del Programa NAC, del Plan Nacional Argentina Conectada" [Accomplishments of National Argentina Connected Program], News release, September 18, 2014, http://bit.ly/1ROnMww; See also: "Access to Knowledge Centers," NAC Official ebsite, accessed August 23, 2016 http://bit.ly/1B0CDrw.

33 Casa Rosada, "El presidente Macri lanzó en Salta el Plan País Digital" [President Macri launched the Digital Country Plan in Salta], June 15, 2016, http://bit.ly/2cg5rL6; See also: País Digital Official ebsite, http://bit.ly/2bVljA0.

34 Decree 459/10, http://bit.ly/1biJ9C5; See also: Government of Argentina, "Conectar Igualdad" [Connect Equality], http://bit.ly/1Ebzusv

layoffs,[35] although the incoming government defended their plan to continue developing the project.[36] According to information published on the official ebsite, more than 120,000 networks were delivered so far in 2016.[37]

Restrictions on Connectivity

The Argentine government does not place limits on bandwidth, nor does it impose control over telecommunications infrastructure. There have been no reported instances of the government cutting off internet connectivity during protests or social unrest. There are currently 18 functioning Network Access Points (NAPs), which help manage internet traffic efficient .[38] NAPs are strategically distributed in the biggest cities all over the country.[39]

ICT Market

There are approximately 816 licensed providers offering internet services in Argentina, which indicates a diverse digital technology spectrum.[40] For a company to offer Internet services, it must fi st obtain a license from the national communications entity, which became ENACOM in December 2015.[41] In May 2016, Resolution 2483/2016 announced a simplified license egistration process for ISPs.[42] The application fee increased from ARS 5,000 (US$333) to ARS 20,000 (US$1,330).[43]

Although generally speaking there are no onerous obstacles to entering the ISP market, around 90 percent of the broadband market is concentrated in three companies: Telefónica, Telecom Argentina, and Cablevisión (Grupo Clarín).[44] The mobile market is also concentrated in the hands of a few companies, namely Movistar (Telefónica), Claro (América Móvil) and Personal (Telecom Argentina).[45]

While Decree 267/2015 ostensibly aims to promote convergence, competition and investment, it is still unclear what effect these reforms will have on the ISP market. Some critics, including telecommunications expert Martin Becerra, have argued that the reforms favor the needs of certain com-

35 "Desde Conectar Igualdad denuncian más de 1000 despidos" [More than 1,000 dismissals denounced from Connect Equality], *La Nación*, March 4, 2016, http://bit.ly/1RvN8PQ; "Denuncian 1000 despidos en el programa Conectar Igualdad" [1,000 dismissals denounced in the Connect Equality Program], *Perfil,* March 4, 2016, http://bit.ly/1o6FzBf; "Conectar igualdad: entre la inclusión pedagógica y la inclusión ciudadana" [Connect Equality: between pedagogical inclusion and citizen inclusion], *ADC Digital*, March 10, 2016, http://bit.ly/22vSXBN; "Denuncian despidos en el programa Conectar Igualdad" [Dismissals denounced in the program Connect Equality], Infobae, March 4, 2016, http://bit.ly/1UkLUYs.

36 **"**El Gobierno confi mó la continuidad de "Conectar Igualdad" y negó despidos" [Government confi med continuation of Connect Equality and denied dismissals], *Télam*, March 4, 2016, http://bit.ly/1MlZd7U.

37 "Conectar Igualdad superó la entrega de 120.000 netbooks en 2016" [Connect Equality exceeds delivery of 120,000 netbooks in 2016], Conectar Igualdad website, September 2, 2016, http://bit.ly/2cYIewV.

38 CABASE – Cámara Argentina de Internet, "NAPS en funcionamiento," http://bit.ly/1JtNxJI.

39 Map of Network Access Points (NAPs) 2015, Argentine Chamber of Internet (CABASE), http://bit.ly/1LH9yK9.

40 ENACOM, "Información de las prestadores" [Information Regarding Providers], http://bit.ly/22w0uAF.

41 National Communications Commission, Decree 764/2000, September 5, 1998, http://bit.ly/1Ry8Mws; ENACOM "Licencia Única de Servicios de Telecomunicaciones," [Licence for Telecommunications Services], http://bit.ly/1LH4ln9.

42 "Government adopts the "multistakeholder" model for the development of Internet" *Convergencia Latina*, May 18, 2016, http://bit.ly/20XqAYj; "ENACOM publicó el nuevo Reglamento de Registro de Servicios TIC" [ENACOM published the new Regulation for the Registration of ICT Services], *Revista Fibra*, May 18, 2016, http://bit.ly/1V9mxrY.

43 Resolution 2483/2016, Official Bulletin, May 16, 2016, http://bit.ly/1X2OTFy.

44 Martín Becerra, *De la concentración a la convergencia*, [From concentration to convergence], Buenos Aires: Paidós, 2015, 64; See also: Leticia Pautasio, "Estadísticas: mercado de telecomunicaciones de Argentina" [Statistics: telecommunications market in Argentina], *Telesemana,* August 4, 2015, http://bit.ly/1T6Jjf8.

45 Leticia Pautasio, "Estadísticas: mercado de telecomunicaciones de Argentina" [Statistics: telecommunications market in Argentina], *Telesemana,* August 4, 2015, http://bit.ly/1T6Jjf8.

panies, and suggest that the new government is encouraging greater concentration.[46] The decree notably categorizes cable TV providers as ICT services, thereby releasing them from obligations in the Broadcasting Law. Some experts have contended that this decision could have a negative impact on standards such as pluralism, diversity, and local content production.[47]

In March 2016, ENACOM approved the sale of Telecom Argentina to Fintech, and Nextel to Grupo Clarín's internet and cable TV provider, Cablevisión.[48] Also in June 2016, Nextel announced the purchase of fi e wireless broadband companies with radio spectrum in the 900 MHz and 2.5 GHz bands, which will enable the deployment of 4G LTE cellular network in the metropolitan area and several towns. According to Nextel, this was a necessary step to preserve competitiveness in the mobile sector.[49]

Regulatory Bodies

Through the Necessity and Urgency Decree (DNU 267/15) issued on December 29, 2015, President Mauricio Macri created the National Authority for Communications (ENACOM), thereby dissolving the Federal Authority of Audiovisual Communication Services (AFSCA), the Federal Authority for Information Technologies and Communications (AFTIC).[50] A previous decree on December 23 had already placed AFSCA and AFTIC under trusteeship for 180 days, replacing their heads with new appointees.[51] While Decree 267/15 received final app oval in Congress on April 6, 2016,[52] these changes prompted heated debate within the country.

Seeking to promote convergence and more homogenous norms, the decree establishes a single entity to regulate the whole system. ENACOM operates within the Ministry of Communications and has a directorate comprised of four directors chosen by the president and three proposed by Congress. ENACOM decisions can be approved by a simple majority and its members may be removed by the president.[53] One concern raised was the possibility of undue executive influence in the composition of the new regulatory body. While the justice minister justified the dec ees as "emergency measures,"[54] the use of emergency decrees to significantly amend the egulatory framework also came under fi e.[55]

46 "Restauración," *Martín Becerra's blog,* January 14, 2016, http://bit.ly/1RG65fw; "Los especialistas opinaron sobre el decreto 267" [Expert opinions on decree 267] *Revista Fibra*, January 4, 2016, http://bit.ly/2cdjStz; "Diversas perspectivas sobre la convergencia" [Diverse persepectives on convergence], *Revista Fibra*, http://bit.ly/2cPOGq3.

47 "El decreto 267 y el fin de los de ates" [Decree 267 and the end of debates], *Revista Fibra,* January 8, 2016, http://bit.ly/2cM3yV6

48 "Aprobaron las ventas de Telecom a Fintech y Nextel a Cablevisión" [Sales of Telecom to Fintech, and Nextel to Cablevisión, are approved], *La Nación,* March 4, 2016, http://bit.ly/1WC6Yqw.

49 "Nextel compró espectro y da otro paso para ser el cuarto operador móvil" [Nextel acquired spectrum and takes another step towards being the fourth mobile operator], *La Nación,* June 24, 2016, http://bit.ly/28VmUH0; See also: "Pelea por el control de las redes" [Fight for the control of the networks], *Página12,* August 2, 2016, http://bit.ly/2cCPSdN.

50 DNU 267/ 15, http://bit.ly/1UycLzB.

51 "Ofi ial: el decreto de Mauricio Macri para intervenir la Afsca y la Aftic por 180 días" [Official: Macri's decree to intervene in Afsca and Aftic for 180 days], *La Nación,* December 23, 2015, http://bit.ly/2eGCA2m.

52 "El Congreso puso punto final a la ley de medios del ki chnerismo" [Congress puts final s op on Kirchner media law], Infobae, April 6, 2016, http://bit.ly/2cLKxQA.

53 ENACOM, "¿Qué es Enacom?" [What is Enacom?], http://bit.ly/1LHw47b.

54 "Garavano: "Vamos a sacar muchas medidas por decreto"" [Garavano: "we are going to issue many measures by decree"], *La Nación,* December 20, 2015, http://bit.ly/22i1w0C.

55 "Audiencia en la CIDH sobre los DNU's de Macri" [Hearing in IACHR on Macri's DNU], *Martín Becerra's blog,* April 8, 2016, http://bit.ly/2cLcgCA.

The executive body that regulates and registers domain names is NIC.ar. All websites with the ".ar" country code Top-Level Domain must be registered with that entity. As of December 2015, registration of any domain ending in ".com.ar" requires an annual fee between ARS 220 and ARS 650 (US$15 and US$43) per year.[56] While these prices are quite affordable, they could deter some users. NIC will also require users to provide a tax ID number to register domains, which must be requested from the Federal Administration of Public Revenue (AFIP) by providing biometric data.[57]

Limits on Content

The groundbreaking ruling on intermediary liability issued by the Supreme Court of Justice in October 2014 has set a precedent for lower court judgments. One case of blocking due to a court order was reported, as part of a criminal case against a software developer who reported a security deficiency in the e-voting system for local elections in Buenos Aires. On the other hand, the current government reportedly removed thousands of online materials from a state-run legal news site, before republishing them on a different site. Finally, several bills that establish mechanisms for removal of content were submitted to the Congress in 2015 and 2016, and may still be debated before the end of the legislative year.

Blocking and Filtering

Internet users in Argentina have access to a wide array of online content, including international and local news outlets, as well as the websites of political parties and civil society initiatives. YouTube, Facebook, Twitter, and international blog-hosting services are freely available. There is no automatic fil ering of internet sites, web pages, platforms, social media sites, or blogs. Law 25.690, however, requires ISPs to provide software that can allow users to choose to limit their own access to "specific websites."[58]

In the past few years, there have been cases of blocking or content removal on grounds of copyright infringement on content sharing platforms. In 2014, a civil court ordered ISPs to block access to IP addresses associated with The Pirate Bay, a website that facilitates peer-to-peer (P2P) file sharing u - ing the BitTorrent protocol, on the grounds that The Pirate Bay included links to copyright protected content.[59] However, users in Argentina can currently access The Pirate Bay through its many mirror sites.[60]

One reported case of blocking by judicial order took place in July 2015 as part of a criminal case against software developer Joaquín Sorianello, who had detected a security deficiency in the e- oting system developed for mayoral elections in the city of Buenos Aires (see "Prosecutions and Detentions for Online Activities"). The judge ordered the telecommunications regulator to request ISPs

56 NIC Argentina, Registration Fees, https://nic.ar/nic-argentina/aranceles.

57 "Exigirán CUIT, CUIL y clave fiscal ara registrar dominios .com.ar" [They will require CUIT, CUIL and tax ID to register .com.ar domains], Télam, May 31, 2016 http://bit.ly/29iWE8w; "¿Qué necesito para operar? [Guide provided by NIC.AR to register a domain], http://bit.ly/29tV425; AFIP, "Trámite para obtener la "Clave Fiscal" para Personas Físicas" [Process to obtain the "tax ID"], http://bit.ly/2d6wM2T.

58 Law 25.690, http://bit.ly/1UqLHCO.

59 National Judicial Branch, Civil Court 64, Argentine Chamber of Phonograms and Videograms Producers (CAPIF), and others with The Pirate Bay, on precautionary measures, March 2014, http://bit.ly/1UqOdsG.

60 "Pese al bloqueo, varios sitios permiten ingresar a the Pirate Bay en la Argentina" [Despite blocking, various sites enable access to the Pirate Bay in Argentina], *Infotechnology,* July 3, 2014, http://bit.ly/1qTe7E2.

to immediately block access to part of the site Justpaste.it, where information obtained from the e-voting system's software source code was published. The judicial order was issued to prevent the spread of sensitive information, but it was still available in other parts of the same site and on other sites.

Several controversial bills introduced in Congress were still up for debate by the end of the coverage period (see "Content Removal" for more information on bills related to the removal of personal data or discriminatory content). Outside the period of coverage of this report, in August 2016, a municipal internet blocking bill in Buenos Aires was introduced in the legislative chamber.[61] The proposal enabled municipal prosecutors to block applications or domain names with the purpose of preventing "unlawful conduct." The bill was widely criticized because the blocking order did not need to be issued by a judge and the wording concerning what might be deemed as "unlawful" was very broad and vague.[62] Also, the bill did not fit national rules on jurisdiction, which confe s powers to regulate internet to the federal government, not a municipal one. Finally, it was withdrawn before it was debated by the Buenos Aires City Legislature.[63]

Content Removal

Under the argument that certain state-run media coverage favored partisan interests, a case of temporary removal of content attracted attention during this coverage period. In February 2016, employees of Infojus Noticias, a news agency created under Fernández de Kirchner and affilia ed to the Justice and Human Rights Ministry, reported that thousands of news items had been removed from its website.[64] The employees denounced that all but 1,200 out of 15,000 articles had been removed from the site, covering judicial issues linked to human rights, crimes against humanity and financial crimes. In response, Justice Minister Germán Garavano argued that "no article had been erased," and subsequently explained that the site was facing a process of transformation to move away from what he called a "political propaganda site," and that the removed items would be made available in a different format.[65] The dispute escalated with the presentation of two judicial claims, one by the Prosecutor of Institutional Violence (PROCUVIN),[66] and the other by the Buenos Aires Press Union (SiPreBa).[67] Both claims requested the judiciary to order the national government to immediately republish the removed articles, to uphold freedom of expression and the right to access public information. Finally, the judicial claims were withdrawn when in May 2016 the articles were reposted on a new website.[68]

61 "Polémica en Argentina por un proyecto de ley que habilita el bloqueo de Internet en Buenos Aires" [Controversy in Argentina on Internet blocking bill], Telesemana.com, August 31, 2016, http://bit.ly/2ciMBOt.

62 ADC Digital, "Un proyecto de ley que pone en riesgo la libertad de expresión en Internet" [A bill that could jeopardize freedom of expression on the Internet], August 29, 2016, http://bit.ly/2cQZxfL; Access Now, "Sociedad civil y organizaciones académicas preocupadas por proyecto de ley para bloquear sitios web y aplicaciones en Argentina," [Civil society and academic organizations concerned about internet blocking bill in Argentina], August 29, 2016, http://bit.ly/2bPGYLX.

63 "Frenan el proyecto de ley para bloquear sitios web" [Internet-blocking bill was stopped], *Minutouno.com* September 1, 2016, http://bit.ly/2cDwqNL.

64 "Denuncian la eliminación del 90 por ciento de las notas del sitio Infojus Noticias" [Deletion of 90 percent of items on the Infojus Noticias site denounced], *Cronista.com,* February 4, 2016,http://bit.ly/1RkHYRc.

65 "Garavano justificó haber eliminado los a tículos de Infojus" [Garavano justified elimination f Infojus articles], *Cronista.com*, February 24, 2016, http://bit.ly/1o6HhT2.

66 "Amparo por Infojus" [Protection for Infojus], *Página 12*, February 27, 2016, http://bit.ly/1UMxChC.

67 SiPreBa, "El SiPreBa reclama al gobierno que reponga las notas de Infojus Noticias" [Press Sindicate of Buenos Aires requests the government to repost the items of Infojus Noticias], March 2, 2016, http://bit.ly/1VEok8a.

68 See website: http://archivoinfojus.gob.ar/; See also: "Una buena para Infojus Noticias" [Good news for Infojus Noticias], *Diarios de Buenos Aires,* May 6, 2016, http://bit.ly/1r5NKPT.

During this coverage period, lower courts clarified certain takedown criteria following the landmark decision by the Argentine Supreme Court regarding intermediary liability. After celebrity Belén Rodríguez sued Yahoo and Google for search results that linked her name to sexual and erotic content, the Supreme Court confirmed in October 2014 that intermediaries should not be liable for third-party content if they did not have knowledge of alleged third-party violations.[69] The ruling established that intermediaries must remove unlawful content only if they are notified by a judicial order, thus favoring a judicial takedown regime over a "notice and takedown" system. The court also stated that if the content involves "manifest illegality," there is no need for a judicial order and it only requires a private communication to the intermediary.

More recent decisions have established criteria to avoid generic injunctions on matters of freedom of expression online. In June 2015, the Tribunal II of the Federal Court of Appeals of the City of Buenos Aires ruled that precautionary measures are able to determine "prima facie" if content is unlawful.[70] However, this measure must not be dictated in general terms and infringing sites have to be individualized in order to be removed. This resolution was supported by another ruling from the same court,[71] confirming that a generic order is not sufficient to generate liability.

Several bills submitted to Congress have sought to implement mechanisms for content removal. Some of them regarded the "right to be forgotten," including a proposal to introduce an online form through which people will be able to request removal of information directly to the search engines, without judicial review.[72] Digital rights activists have raised concerns that such a system could leave the door open to abuses by government and private parties, and encourage search engines to implement self-censorship mechanisms. Others sought to regulate all the activities of intermediaries and included "notice and takedown" systems for cases of "manifest illegality," such as content that facilitates crimes; put an individual's human life at risk; advocacy of national or racial hate; child pornography; or content that produces serious danger to the individual's honor, image or intimacy.[73] Lastly, a new bill on intermediaries was introduced in 2016; unlike the others, it rejects private or administrative notice and takedown systems and establishes that in all cases a judicial order is necessary to remove online content.[74] These bills are still at the early stages of the legislative process and remain in different commissions. Many of the bills will expire if they are not discussed by the end of 2016.[75]

Another controversial bill approved by the Commission of Human Rights of the Chamber of Representatives in July 2015 would have expanded the current meaning of "discriminatory act" to include comments in social networks, blogs, forums and other online media.[76] Criticized for restricting free-

69 Supreme Court of Justice, "Rodriguez, Maria Belén c/ Google Inc. s/ daños y perjuicios," October 28, 2014, http://bit.ly/1UGGjrD.

70 Argentine Federal Court of Appeals on Civil and Commercial Matters, II, "Giovanetti, Laura c.Yahoo Argentina y otro," June 2, 2015, http://bit.ly/2bXF72p.

71 Argentine Federal Court of Appeals on Civil and Commercial Matters, II, "Albertario, Claudia c. Yahoo Argentina y otro s/ daños y perjuicios," June 2, 2015 (link not available).

72 Bill 0444-S-2015, http://bit.ly/1JcOVA4; Bill 1906-D-2015,http://bit.ly/1q26VKn; Bill 4388-D-2015,http://bit.ly/22vQ1Ft.

73 Bill 1865/15, http://bit.ly/1EtTeKs; Bill 3842-D-2015, http://bit.ly/21H3rIY.

74 Bill 942/16, http://bit.ly/2cfPULJ.

75 See Law 13.640 for information governing the legislative process: http://bit.ly/1KA2uJm.

76 National Bill Against Discrimination (9064-D-15), http://bit.ly/1MKrmAW.

dom of expression and violating the constitution and international human rights treaties,[77] the bill ordered online media to take preventive measures to tackle discriminatory content, by monitoring comments published on their sites. It established a new criminal offence for those posting discriminatory comments, as well as shifting the burden of proof on the person who comments. While an amended version of the bill removed provisions addressing online media and social networks, it maintained broad and ambiguous language to define discriminatory acts."[78] The National Institute against Discrimination, Xenophobia and Racism (INADI) held public meetings with civil society organizations to reach consensus for new legislation on anti-discrimination, based on the bills already submitted.[79]

Media, Diversity, and Content Manipulation

Argentina has a relatively open and diverse online media environment, as well as high rates of social media use. According to a map developed by the National Data Protection Authority, there are seven social networks with more than a million users in the country.[80] Self-censorship among bloggers and online users is not widespread in Argentina, although some isolated instances of harassment may elicit self-censorship in particular cases (see Intimidation and Violence).

The government of President Macri has announced a significant eduction in the budget for official advertising, a decision which may affect the current media landscape, including digital media.[81] The discriminatory allocation of official ad ertising, both at the federal and local levels, has played a major role in shaping media content in Argentina. Despite multiple court rulings ordering the government to comply with equitable allocation of official ad ertising,[82] the government has repeatedly come under fi e for providing substantial funding through advertising to media outlets that are favorable to the government, while cutting off advertising for critical organizations.[83] According to recent research, half of total funds allocated to official ad ertising from 2009 to 2015 were distributed among 15 media organizations, 12 of them allegedly close to the Fernández de Kirchner government.[84] In June 2016, the Public Communication Secretary issued an administrative resolution regulating the allocation of official ad ertising to media outlets, including digital media.[85] The resolution states that funding must be allocated according to objective criteria, such as media reach, relevance of the message, geographic zone and promotion of the federalism and plurality of voices.

77 Association for Civil Rights (ADC), "Regular comentarios en Internet: el proyecto de ley antidiscriminación es inconstitucional" [Regulating comments in the internet: the anti-discrimination bill is unconstitutional], July 22, 2015, http://bit.ly/1HS2aVJ; Beatriz Busaniche, "Proyecto de ley antidiscriminación: una supuesta solución que amplía los problemas" [Anti-discrimination bill: a supposed solution that expands the problems], Via Libre Foundation, July 17, 2015, http://bit.ly/21G9Sfi; Center of Legal and Social Studies (CELS), "Proyecto de ley antidiscriminación" [Anti-discrimination bill], August 20, 2015, http://bit.ly/22uOmQv.

78 Bill 9064-D-2014, http://bit.ly/1RG5mYz.

79 National Institute Against Discrimination, Xenophobia, and Racism (INADI), "Diálogo por la nueva ley antidiscriminatoria" [Dialogue for a new anti-discrimination law], June 2, 2016, http://bit.ly/1VCbw2s.

80 National Directorate for the Protection of Personal Data, "Primer mapa argentino de las redes sociales," [First Argentine map of social networks], August, 2015, http://bit.ly/1Y0fekF.

81 José Crettaz, "El fin de la auta oficial está cambiando drásticamen e el mapa de medios" [The end of the oficial attern is dramatically changing the media map], *La Nación*, March, 2016, http://bit.ly/1R68Zqt.

82 Judicial Information Center, "La Corte Suprema declaró la constitucionalidad de la Ley de Medios," [The Supreme Court upheld the constitutionality of the Media Law], October, 2013, http://bit.ly/1Kdidjj.

83 Martín Becerra, "La pauta que los parió," *Martín Becerra's blog*, March, 2016, http://bit.ly/1V3naCp.

84 José Crettaz, "Pauta oficial 2009-2015: odos los nombres y los montos cobrados" [Official guidelines 2009-2015: all names and the amounts charged], *La Nación*, November, 2015, http://bit.ly/1RllekQ.

85 Resolution 247-E/2016, http://bit.ly/2d6Ge4Z.

Digital Activism

Argentinians continue to use social media as a tool for political mobilization. In June 2015, after several women were murdered, a group of journalists and activists called for a demonstration to advocate for concrete action to reduce violence against women. Digital activism played a crucial role in more than 200,000 people gathering in front of Congress on June 3, 2015.[86] The march went viral on social media with the hashtag #NiUnaMenos (Not One Less) and generated more than 270,000 tweets during the mobilization.[87]A second #NiUnaMenos march took place the following year, on June 3, 2016, once again rallying thousands of people around the country and encouraging significant social media engagement.[88]

Violations of User Rights

Argentina has relatively strong privacy protections and authorities must obtain a judicial warrant before conducting surveillance. Argentina does not suffer from high levels of violence against journalists, but during the period of coverage three cases of cyberattacks against news outlets were reported. A judicial order was issued to raid the house of Joaquín Sorianello, a software developer who had discovered a security vulnerability in the electronic voting system used in local elections in Buenos Aires.

Legal Environment

Freedom of expression is guaranteed by the National Constitution.[89] Argentina explicitly established online freedom of expression protections through a presidential decree issued in 1997,[90] which were expanded by the Congress in 2005 to include "the search, reception and dissemination of ideas and information of all kinds via internet services."[91] Defamatory statements regarding matters of public interest were decriminalized in 2009,[92] following the Inter-American Court of Human Rights' ruling in "Kimel vs. Argentina."[93]

Some laws impose criminal and civil liability for online activities. Law 11.723 holds liable those who, by any means, reproduce content that violates intellectual property, and establishes sanctions ranging from fines o six years in prison. In November 2013, Congress approved a law amending the penal code and establishing penalties of up to four years imprisonment for online contact with a minor

86 "Argentine marches condemns domestic violence", BBC, June, 2015, http://bbc.in/1SXuUoa; See also : "Argentina protesta contra la violencia machista: 'Ni una menos'" [Argentina protests against gender violence: 'Not One Less'], *Univisión*, June, 2015, http://bit.ly/21SFfDv; "Histórica marcha contra la violencia machista" [Historic march against gender violence], *Clarín*, June, 2015, http://clar.in/1KB2azu.

87 Guillermo Tomoyose, "Del mundo online a la marcha: el mapa con las repercusiones de #NiUnaMenos en Twitter" [From the online world to the march: the map with the impact of #NiUnaMenoson Twitter], *La Nación*, June, 2015, http://bit.ly/1Jayd8P.

88 "Una multitud en otro grito contra la violencia machista" [A crowd in another cry against male violence], *Clarín*, June 4, 2016, http://clar.in/29qR9AZ.

89 National Constitution, Article 14, http://bit.ly/1K2LdgL. The constitution was amended in 1994, and Article 75 (22) now recognizes numerous international human rights treaties with constitutional status and precedence over national laws.

90 Decree 1279/97, December 1, 1997, http://bit.ly/1JCs3dP.

91 Law 26032, http://bit.ly/1EzDJA5.

92 Law 26551, http://bit.ly/1ZH7UvP.

93 "Kimel vs Argentina," Inter-American Court of Human Rights, 2008, http://bit.ly/1SrPsUN.

carried out "with the purpose of committing a crime against [the minor's] sexual integrity."[94] The law generated concern among academics and civil society organizations because of its vague wording.[95]

In 2008, the government passed a law on cybercrime,[96] which amended the Argentine Criminal Code to prohibit distribution and possession of child pornography, interception of communications and informatics systems, hacking, and electronic fraud. Some of the terms used in the legislation have been criticized as too ambiguous, which could lead to overly broad interpretation. In November 2015, the General Prosecutor's Office c eated the Specialized Prosecutor's Unit on Cybercrime for the investigation of computer-related crimes (see Technical attacks).[97]

The government has further committed to promoting the values of democracy and human rights online. In June 2016, Argentina joined the inter-governmental Freedom Online Coalition, which supports internet freedom and the protection of fundamental human rights.[98] Argentina is the third Latin American country, and the fi st from South America, to join the coalition.

Prosecutions and Detentions for Online Activities

In June 2015, ten days before municipal elections in the Autonomous City of Buenos Aires, Joaquín Sorianello, a software developer, discovered a security vulnerability in the electronic voting system that leaked SSL certifica es used in the machines that transmitted data from voting locations to the vote counting center, and proceeded to report the vulnerability to the company in charge of the voting system, Magic Software Argentina (MSA).[99]

On July 4, just two days before the elections, the Cybercrime Division of the Metropolitan Police of the City of Buenos Aires raided the house of Sorianello, by orders of the Judge María Luisa Escrich, and proceeded to confisca e his electronic devices,[100] on the grounds of violation of Article 183 of the Penal Code,[101] by which Sorianello was accused of causing damage to IT systems. In an interview on March 15, 2016, Sorianello stated that his case was not moving forward and that MSA never appeared at any hearing nor presented any document regarding the case.[102] At the end of July 2016, Sorianello was dismissed from the case on the grounds that, although it was established that Sorianello entered the computer system of the company MSA Group, he did not do so in an unlawful manner nor did he cause any harm; on the contrary, it was to give notice to the company that the security system was vague and could be easily breached.[103]

94 Law 26904, http://bit.ly/1JCto4j.

95 "Nuevas críticas a la ley de grooming reavivan debates irresueltos" [New criticism on grooming law revives unresolved debates], *Infotechnology*, March 22, 2014, http://bit.ly/PYofy8.

96 Law 26388, http://bit.ly/U6ZyAE.

97 Resolution 3743/15, http://bit.ly/1WVqvm2.

98 "Freedom Online Coalition welcomes Argentina as its 30th member," Freedom Online Coalition, June 2016, http://bit.ly/29skEVl.

99 "A diez días de los comicios porteños, descubren filtraciones de seguridad en el sis ema de voto electrónico" [Ten days before elections, security leaks in the electronic voting system are discovered], *Télam*, June 26, 2015, http://bit.ly/1GXzkCa.

100 "La Policía Metropolitana allanó el domicilio del especialista que denunció fallas en el sistema de voto electrónico" [The Metropolitan Police raided the house of the expert who reported vulnerabilities in the electronic voting system], *Télam*, July 4, 2015, http://bit.ly/1KEE98N.

101 Law 11.179, art. 183, http://bit.ly/1gbsj6k.

102 Camila Selva Cabral, "Privatizar el voto no es una buena idea" [Privatizing the vote is not a good idea], News Agency – Communications Science, University of Buenos Aires, March, 2016, http://bit.ly/1USSZ24.

103 "Sobreseyeron al programador que reveló fallas en el sistema de voto por Boleta Única Electrónica" [They dismissed the programmer who revealed flaws in the elect onic voting system], *La Nación,* August 2, 2016, http://bit.ly/2b5n37y.

Surveillance, Privacy, and Anonymity

The Argentine government does not impose restrictions on anonymity or encryption for internet users. Bloggers and other online users are not required to register with the government and can post anonymous comments freely in online forums.

Law 25.891 determines that telecom operators must register users' identification info mation when purchasing a mobile phone or prepaid SIM card.[104] This law was introduced in 2004 as part of an effort to tackle the resale of stolen mobile phones and SIM cards, but it has not yet been regulated, even after multiple attempts to explicitly enforce the creation of a database for the registration of users' identification info mation when buying mobile phones and SIM cards.[105]

In general, Argentina has strong privacy standards rooted in the constitution, as well as data protection laws with standards that compare to those in Europe. In addition to legal conditions for the collection of video surveillance images[106] and guidelines to protect privacy in the development of applications,[107] the National Directorate for Protection of Personal Data has issued legal requirements and privacy recommendations relating to the use of unmanned aerial vehicles (UAVs) or drones.[108]

According to the National Intelligence Law, a court order is necessary to conduct surveillance of private communications.[109] Until December 2015, the only state body that was legally allowed to conduct surveillance was the Department for Interception and Captation of Communications (DICOM), dependent on the Public Ministry.[110] However, Decree 256/15 transferred DICOM to the Supreme Court,[111] which later replaced DICOM with the Directorate of Captation of Communications (DCC).[112] The DCC is presided by a judge, appointed by lottery, for the duration of one year.

Argentina does not systematically collect metadata, although a 2013 resolution by the Secretariat of Communications raised some privacy concerns. Resolution 5/2013 regulating the quality of telecommunications services states that providers should "guarantee the free access of the CNC [the regulatory body in 2013, now ENACOM] to installations… and [should] give them all the information that is required in the set manner and timeframe." It also establishes a period of three years for service providers to keep all collected data.[113] However, the article in question states clearly that the data will be used to calculate quality indicators, and the resolution mentions the obligation to respect personal data. Since its passage in 2013, there has been no evidence to suggest that this provision was implemented in an unlawful or abusive way.

104 Law N° 25.891, http://bit.ly/1ojOlMi.

105 See bills: 6538-D-2010 http://bit.ly/1XZWodz, 0212-D-2012 http://bit.ly/1Sk1gWN, 8141-D-2012 http://bit.ly/1RNTo5w, 2986-D-2014 http://bit.ly/1ojOI9K, 2583-D-2014 http://bit.ly/1WUVeQd, 9439-D-2014 http://bit.ly/1UzQUbI, 1076-D-2015 http://bit.ly/1RxfYd8

106 Ministry of Justice and Human Rights, Disposition 10/2015, http://bit.ly/25EGjlI.

107 Ministry of Justice and Human Rights, Disposition 18/2015, http://bit.ly/1RjhmQb.

108 Ministry of Justice and Human Rights, Disposition 20/2015, http://bit.ly/1fDgI4M.

109 Law 25.520, Art. 5, http://bit.ly/1bp2vWp.

110 Law 27.126, Art. 17, http://bit.ly/1CLiBGU.

111 Decree 256/15, http://bit.ly/1RI8wLr.

112 Judicial Information Center, "La Corte Suprema creó la Dirección de Captación de Comunicaciones del Poder Judicial" [The Supreme Court created the Directorate of Captation of Communications of the Judiciary], February 15, 2016, http://bit.ly/1Urvf5d; See also: ADC, "Reflexiones sob e la creación de la Dirección de Captación de Comunicaciones" [Initial reflections on the creation of the DCC], February 19, 2016, http://bit.ly/2dtGQkc.

113 Ministry of Federal Planning, Public Investment and Services, Communications Secretariat, Resolution 5/2013, http://bit.ly/1VaT2BX.

Although there is little to no information available regarding covert or unlawful surveillance, and although these practices do not seem to be widespread, two main cases can be highlighted in 2015. First, emails leaked from Hacking Team in July 2015 revealed exhanges between the Italian spyware company and Argentine companies that claimed to have ties with state actors (such as the Federal Intelligence Agency, the Army and the Federal Police). The companies appeared to have been interested in acquiring Hacking Team's products, but it was not possible to confi m the completion of a transaction or direct contact between the government and Hacking Team from the emails.[114]

Second, in December 2015, Citizen Lab published research showcasing an extensive malware, phishing, and disinformation campaign active in several Latin American countries, including Ecuador, Argentina, Venezuela, and Brazil.[115] Regarding Argentina, Citizen Lab noted the targeting of political figu es in the malware campaign, such as the deceased prosecutor Alberto Nisman and the journalist Jorge Lanata. Moreover, on October 20, 2015, former deputies Laura Alonso and Patricia Bullrich filed a complaint for alleged illegal spying on jou nalists, politicians, public prosecutors and judges carried out by the Federal Intelligence Agency.[116] However, the day after the complaint was filed, one of the judges stated that it was submitted without documents to support it.[117]

The government requested data on a number of users in 2015, mostly for criminal investigations. Between July and December 2015, Google received a total of 436 requests for data disclosures of 569 Google accounts, and disclosed information in 59 percent of cases.[118] During that same period, Yahoo received a total of 184 data requests related to 220 Yahoo specified accounts:

- 33 percent of requests were rejected,
- 46 percent resulted in the disclosure of non-content data (basic subscriber information, such as name, login details, location and IP address at the time of registration),
- 14 percent resulted in content being disclosed,
- And in 7 percent of cases, no data was found.[119]

Microsoft received a total of 789 law enforcement requests related to 919 specified user accounts, f which 71 percent resulted in the disclosure of non-content data, 19 percent resulted in no customer data being found, 10 percent were rejected for not meeting the legal requirements.[120] Facebook received a total of 892 data requests regarding 1,047 specified user accounts, out f which 71 percent resulted in the disclosure of some data.[121] Between January and December 2015, Twitter received a

114 Leandro Ucciferri, "Hacking Team y sus planes para hackearen Argentina" [Hacking Team and their plans to hack in Argentina], *Tecnovortex,* July, 2015, http://bit.ly/1PDwEgS.

115 John Scott-Railton, Morgan Marquis-Boire, Claudio Guarnieri, and Marion Marschalek, "Packrat: Seven Years of a South American Threat Actor," Citizen Lab, December 2015, http://bit.ly/1U3dFkI.

116 "Denuncian espionaje de la Secretaría de Inteligencia a jueces, políticos y periodistas" [Denounced: spying by the Intelligence Agency against judges, politicians and journalists], *La Nación*, October 20, 2015, http://bit.ly/1OGTcm2; "Denuncian que el Gobierno hizo espionaje ilegal sobre políticos, jueces y periodistas," [They claim that the government carried out illegal spying on politicians, judges and journalists], *Clarín*, October 20, 2015, http://clar.in/21RuOzZ.

117 "Casanello afi mó que la denuncia de Alonso y Bullrich se presentó "sin documentación ni listados"" [Casanello declared that the complaint by Alonso and Bullrich was presented "without documentation nor listings"], *Télam,* October 21, 2015, http://bit.ly/1OIvSEC.

118 Google, *Transparency Report*, July – December 2015, http://bit.ly/1qezDI9.

119 Yahoo, *Transparency Report*, July – December 2015, http://bit.ly/1RIaRGm.

120 Microsoft, *Transparency Report*, July – December 2015, http://bit.ly/1WUWhj1.

121 Facebook, *Government Requests Report*, July – December 2015, http://bit.ly/2ejRQhw.

total of 7 account information requests regarding 17 specified accounts (including witter, Periscope, and Vine accounts); none of them resulted in the production of data.[122]

Intimidation and Violence

Although there were no known cases of bloggers or ICT users being subject of extralegal intimidation or physical violence by state authorities or other actors, the Argentine Forum of Journalism (FOPEA) reported 94 cases of harassment against journalists throughout the country in its 2015 report of attacks on press freedom, of which 12 percent were against digital news media. The report shows a decrease in the overall number of reported attacks, compared to 178 cases recorded in 2014.

Technical Attacks

Cybercrime remains an increasingly important issue in Argentina. In November 2015, the Public Ministry created the Specialized Prosecutor's Unit on Cybercrime (UFECI), which can take part in any legal process where it would be necessary to conduct research into digital environments.[123]

Although there are no known public statistics or reports from the official p ogram that was in charge of cybersecurity activities in the public sector, the National Program of Critical Infrastructure of Information and Cybersecurity (ICIC), there were three reported cases of cyberattacks against news websites: *Página 12, Diario Registrado* and *Clarín*. News outlet *Página 12* claimed to have suffered a Distributed Denial of Service (DDoS) attack on its website lasting from December 3 to 8, during which time users were not able to access the website. On December 9, 2015, the Attorney General's Office launched an in estigation through UFECI,[124] but there have been no official sta ements about the status of the case since. This case led the Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights, Edison Lanza, to state that the attack was a direct violation of freedom of expression.[125] Shortly after this incident, news outlet *Diario Registrado* denounced a similar attack on December 11 that impeded certain users from accessing the website.[126] Another news outlet, *Clarín,* also reported a DDoS attack for a period of two hours on December 13, but the attack did not result in a complete shutdown of the website.[127]

Decree 13/16 created the post of Undersecretary of Technology and Cyber Security under the Ministry of Modernization, in charge of developing the strategy for technological infrastructure, as well as a national cybersecurity agenda, thus absorbing the functions of the National Program of Critical Infrastructure of Information and Cybersecurity (ICIC), which was created in 2011.[128]

122 Twitter, *Transparency Report*, 2015, http://bit.ly/21Rvfu7.

123 Public Prosecutor's Office, "Gils Carbó c eó la Unidad Fiscal Especializada en Ciber-delincuencia" [Gils Carbó created the Specialized Prosecutor's Unit on Cybercrime], November 18, 2015, http://bit.ly/1RFfaFe.

124 "Bloqueo digital a la libertad de expresión" [Digital block against freedom of expression], *Página 12*, December, 2015, http://bit.ly/1QeDhMC.

125 "El ataque es una violación directa de la libertad de expression" [The attack is a direct violation of freedom of expression], *Página 12*, December 9, 2015, http://bit.ly/1lYkoR0.

126 "Hackearon el sitio Diario Registrado.com" [The website DiarioRegistrado.com was hacked], *La Nación*, December 15, 2015, http://bit.ly/2bZRznr.

127 "El sitio de Clarín recibió un ciberataque durante dos horas" [Clarín's website received a cyberattack for two hours], *Clarín*, December 14, 2015, http://clar.in/1jYP0Rg.

128 Decree 13/2016, http://bit.ly/1pHX4J7.

Freedom House

Armenia

	2015	2016
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	6	6
Limits on Content (0-35)	10	10
Violations of User Rights (0-40)	12	14
TOTAL* (0-100)	**27**	**30**

* 0=most free, 100=least free

Population:	**3 million**
Internet Penetration 2015 (ITU):	**58 percent**
Social Media/ICT Apps Blocked:	**Yes^**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2016 Status:	**Not Free**

^Occurred after coverage period until September 2016

Key Developments: June 2015 – May 2016

- In July 2016, amid clashes between an armed militant group and authorities, Facebook was briefly una ailable for users in Armenia across several ISPs (see **Blocking and Filtering**).
- In April 2016, hostilities broke out between Armenian and Azerbaijani forces over the disputed Nagorno-Karabakh territory. Throughout the conflict, online commenta ors were encouraged to practice self-censorship (see **Media, Diversity, and Content Manipulation**).
- In June 2015, police targeted journalists livestreaming the Electric Yerevan protests in the capital, beating them and confiscating their equipment (see **Intimidation and Violence**).
- In July 2015, a trial commenced against the creators of satirical YouTube Channel "SOS TV", with police seeking an apology and payment of a fine for a video which they claim insults the Armenian police force (see **Prosecutions and Detentions for Online Activity**).

Introduction

Internet freedom remained largely uninhibited in the past year, though Armenia's overall score declined somewhat after police physically attacked journalists livestreaming protests in Yerevan.

The past year in Armenia has been marked by periods of civil unrest and regional conflict. In la e 2015, a constitutional referendum changed the country from a semi-presidential system to a parliamentary republic, a change which critics say would allow President Sargsyan to serve beyond his second term in office. The eferendum was marred by suspicions of ballot stuffing and p essure. In April 2016, hostilities broke out between Armenian and Azerbaijani forces over the Nagorno-Karabakh territory, resulting in casualties on both sides. Later, in July 2016, armed anti-regime militants clashed with police in the capital.

While Armenians are generally free to express themselves online without restriction or fear of sanction, some incidents of censorship occurred during and after the coverage period, coinciding with the periods of violence and unrest. Facebook was briefly estricted in July 2016 while armed militants were challenging the authorities, and netizens were pressured to self-censor as violent clashes briefly resumed on the Nagorno-Karabakh frontline.

However, historically the internet has remained relatively free in Armenia, with gradual improvements in infrastructure and accessibility connecting more of the population. Activists regularly use social media as a tool to promote their causes, and opposition and independent media flourish online.

Obstacles to Access

Internet access in Armenia continues to grow, though growth slowed somewhat in 2015, possibly due to market saturation. The internet penetration rate increased to just over 58 percent. The ISP market is relatively diverse, with foreign as well as local providers competing for customers, though an urban-rural divide persists, limiting access and quality for those living outside major cities.

Availability and Ease of Access

According to the International Telecommunication Union (ITU), the internet penetration rate reached just over 58 percent in 2015, compared with 42 percent in 2013 and just 15 percent in 2009.[1] Average internet speeds more than doubled in 2015 reaching 17Mbps compared to 8.7Mbps in 2014, according to government figu es.[2]

By the end of 2015, there were 289,102 fi ed-line broadband subscriptions, representing an increase of 29,217 relative to the same period in 2014. In December 2015, mobile broadband subscriptions

1 International Telecommunication Union, "Percentage of Individuals Using the Internet," http://bit.ly/1QYT4u2. The Armenian Ministry of Transport and Communication estimated internet penetration at 55.29 percent in 2015.

2 Armenian Ministry of Transportation and Communications, "Report on Results of Work and Implementing Priority Objectives in 2015, " [in Armenian] http://bit.ly/1QwsdZ7

reached 244,443, an increase of 13,669 over 2014.[3]

The mobile penetration rate reached 124 percent in 2015.[4] Based on reports provided by mobile operators, more than 1.6 million mobile phones out of a total of 3.5 million were connected to the internet as of December 2015.[5] The use of internet connected phones increased by 2.3 percent (85,071 subscribers) compared with the same period last year.

Internet is ubiquitous in Armenia's capital Yerevan with most cafés, universities, and many schools providing free Wi-Fi access. There is also Wi-Fi connectivity in some of Yerevan's public buses, the metro, some railway stations, and some taxis. In contrast to the diverse market in Yerevan, the capital city, many villages have only one or two mobile broadband services from which to choose. Approximately 60 percent of rural towns are covered by fi ed-line broadband. 3G services are available to almost 100 percent of the population, covering 90 percent of the country (excluding mostly unpopulated mountainous regions) .[6]

Many operators are also offering three-in-one packages including IP television and fi ed telephone services; the average price for this package with an average speed of 20 Mbps is AMD 10,000 (US$22).[7]

Restrictions on Connectivity

The government does not typically restrict internet access, though in an isolated incident Facebook was reportedly unavailable for approximately 40 minutes in July 2016 during a period of civil unrest in Yerevan (see Blocking and Filtering).

In practice, the Armenian government and the telecommunications regulatory authority, the PSRC, do not interfere with or try to influence the planning f network topology. Operators plan and develop their networks without any coordination with either the government or the regulatory authority. Moreover, the regulatory authority requires service providers to indicate any technological restrictions in their public offers. Armenian internet users enjoy access to internet resources without limitation, including peer-to-peer networks, voice and instant messaging services.

Access to the internet in Armenia is ensured through four backbone networks that use fibe -optic cable systems. The international internet connection is made possible by fi e telecommunication operators[8]. At the network level they are interconnected with fibe -optic cable systems operating in the territory of the Republic of Georgia. There is also a fibe -optic connection through Iran, which is limited in capacity and mostly serves backup needs.[9] In the past, physical damage to the cables in

3 Ministry of Transportation and Communications, "Report on Results of Work and Implementing Priority Objectives in 2015, " [in Armenian] http://bit.ly/1QwsdZ7

4 Business 24 (b24.am) business newswire, "Number of Mobile Subscribers in Armenia, Q4, 2015," April 13, 2016, http://bit.ly/2c5hd8T .

5 Business 24 (b24.am) business newswire, "Number of Mobile Subscribers in Armenia, Q4, 2015," April 13, 2016, http://bit.ly/2c5hd8T.

6 This information was derived from reports published on several mobile operators' websites, including MTS (Mts.am), Beeline (Beeline.am), and Orange Armenia (Orangearmenia.am).

7 Panorama.am, "2 Million People Use The Internet in Armenia. Enterprize Incubator Foundation,"March 21, 2015, http://bit.ly/1X6i5rS.

8 Hetq.am, "The Owners of Armenian Internet," [in Armenian], October 6, 2015, http://bit.ly/1UOOp3Q.

9 Noravank Foundation, "The Problems of Armenian Internet Domain," [in Armenian], January 12, 2016, http://bit.ly/1QDh61R

the territory of Georgia has caused disruptions in internet access.[10] While there have been no major disruptions in the recent years, the limited number of connections to and from the country present challenges in ensuring uninterrupted internet access.

ICT Market

Armenia was one of the fi st post-Soviet countries to privatize the telecommunication industry. Since the mid-2000s, the Armenian mobile and ISP market became increasingly diverse, with Armenian users able to choose from three mobile service operators and dozens of ISPs, 46 percent of which are foreign-owned. Internet service providers offer ADSL, fibe -optic and cable access, WiFi and Wi-Max wireless technologies, general packet radio services (GPRS), EDGE, CDMA and 3G technologies (UMTS/WCDMA), and 4G LTE. All three current mobile operators offer 2G and 3G+ networks, and two operators offer 4G LTE network services. However, 4G LTE services are available only in limited locations, including Yerevan, Gyumri, Vanadzor, Dilijan, and Tsakhkadzor.[11]

According to the Public Services Regulatory Commission (PSRC) there are 71 ISPs in Armenia. However, an analysis of data published by service providers shows that the four leading operators together control approximately 90 percent of the market for internet access, and 96 percent of the total revenue from internet service. The regulatory authorities in Armenia primarily focus on companies with significant mar et power, one of which is Armenian, while the other three are foreign-owned.

The four major providers are Ucom with 40 percent market share, Armentel (Beeline) with 36 percent, Vivacell-MTS with 15 percent, and Rostelecom with 7 percent. The fastest growing ISP is Rostelecom, a cable provider with 31,161 subscriptions, an increase of 9,265 subscribers in one year, while Armentel (Beeline), the largest ADSL broadband internet access provider, is losing ground.[12]

There are three mobile operators in Armenia. The largest mobile internet provider is the local company Ucom,[13] followed by VivaCell-MTS and Armentel (Beeline). Armentel (Beeline) is owned by Vimpelcom, one of largest mobile operators in Russia; Vivacell-MTS is owned by Mobile TeleSystems, another of the largest mobile operators active in Russia. In 2013, Ucom was issued a license allowing its entry into the telecommunications market, but acquired Orange Armenia from France Telecom in August 2015 instead of building up its own network.

Regulatory Bodies

The concept of an independent regulatory authority was implemented in 2006 with the adoption of the Law on Electronic Communication. Armenia has chosen a multi-sector regulatory model in which one body, the PSRC, is in charge of the regulation of energy, water supply, and telecommunications services. The PSRC's authority, mechanisms of commissioners' appointments, and budgeting principles are defined under the Law on tate Commission for the Regulation of Public Services.[14] The Law on Electronic Communication contains provisions guaranteeing the transparency of the deci-

10 The Guardian, "Georgian woman cuts off web access to whole of Armenia," April 6, 2011, http://bit.ly/1nsMLau.

11 EIF, *ICT Industry Report*, (Armenia, 2014), http://bit.ly/1OYd3ri

12 Rostelecom, "Reports," http://bit.ly/1GmOszd; Roseltelecom, *Report 2015,* [in Armenian] http://bit.ly/1Sto5f2

13 *Orange Armenia 2015 Report, http://oran.ge/1QFb9OD*

14 The Law on Public Services Regulation Commission was adopted by the National Assembly of the Republic of Armenia on December 25, 2003.

sion-making procedures of the commission: all decisions are made during open meetings with prior notification and equests for comments from all interested persons posted on the website.[15] The PSRC is accountable to the National Assembly in the form of an annual report, but the parliament merely takes this report into consideration and cannot take any action.

However, one of the weakest provisions of the Armenian regulatory framework is the absence of term limits for commissioners. The members or commissioners of the PSRC are appointed by the president of Armenia in accordance with the recommendations of the prime minister. Once appointed, a commissioner can be dismissed only if he or she is convicted of a crime, fails to perform his or her professional duties, or violates other restrictions in the law, such as obtaining shares of regulated companies or missing more than fi e PSRC meetings.

This dependence on the political leadership has been shown to undermine regulatory independence in the past, including in the media sector.[16] In 1995, the broadcasting license of the independent television company A1+ was suspended for refusing to broadcast only pro-government material, and in 2002 its broadcasting frequency was awarded to another company. Despite a ruling by the European Court of Human Rights in 2008, which stated that the regulatory authority's refusal to reinstate the company's broadcasting license amounted to a violation of freedom of information, the license was never reinstated.[17]

Amendments to the Law on Electric Communication removed the need for internet service providers to obtain a license, instead requiring that they simply notify the regulator of their provision of internet services or the operation of a telecommunication network.[18] Public access points such as cafes, libraries, schools, universities, and community centers are also not required to obtain a license to offer internet access unless they offer services for a fee. According to a separate licensing law, nonprofit entities a e not required to obtain a license for the provision of internet services.[19]

In spite of three well-established ICT-related nonprofit associations, sel -regulation of the industry is significantly unde developed in Armenia. The oldest nonprofit institution is the In ernet Society (ISoc), which is the national chapter of the worldwide ISoc network. At the early stage of internet development in Armenia (1995 through 1998), ISoc Armenia was the primary internet policy advocate and industry promoter. However, after the establishment of the independent regulatory authority, ISoc no longer plays as much of a regulatory role, as most industry disputes are filed with the PS C.

ISoc continues to maintain the registration of domain names, and despite the lack of formal dispute resolution policies, it carries out the registry function effectively with minimal influence f om government authorities or the regulator. As a result, the Armenian ICT market enjoys a liberal and non-discriminatory domain name registration regime. ISoc Armenia registers domain names according to ICANN recommendations and best practices. Isoc's board is composed of service provider managers, and in general, the Society's policy agenda is strongly influenced by the in erests of traditional pro-

15 Article 11 of the Law of the Republic of Armenia on Public Service Regulation Commission.

16 There are three independent regulatory authorities in Armenia that are part of the executive, but not a part of the government. These three authorities are the public utilities regulator, the broadcasting regulator, and the competition authority.

17 In September 2012, A1+ began broadcasting on the airwaves of Armnews. During this time, A1+ was nonetheless able to continue publishing news content on its website. For further information on Meltex LTD and Mesrop Movsesyan v. Armenia: European Court of Human Rights, "Article 10 – Judgement," in "Information Note on the Court's case-law," June 2008, http://bit.ly/1MPDVhi

18 Law of the Republic of Armenia on Changes and Amendments to the Law on Electronic Communication of April 29, 2013, Official Bulletin No 05/29(969), June 5, 2013.

19 Art. 43, Law of the Republic of Armenia on Licensing, May 30, 2001, with several amendments from 2002-2012.

viders that started their business in the mid-1990s.

Another well-established industry association is the Union of Information Technologies Enterprises (UITE).[20] Though industry self-regulation is one of the main goals of the Union, so far it has not developed any significant policies for indust y regulation. Both ISoc Armenia and UITE are founders of a third notable nonprofit institution, the A mEx Foundation, which was established with the sole purpose of creating a local data traffic e change point. Other founders include leading ISPs as well as mobile and landline telecommunication operators.

Limits on Content

The Armenian government does not consistently or pervasively block users' access to content online. In an isolated incident, Facebook was reportedly briefly unavailable during clashes between police and armed groups in July 2016. The most common incidents of censorship of online content relate to blocking and filtering of platforms and websites by the Russian regulatory authority, which affects access to the same content for some internet users in Armenia, since Armenia receives some of its web traffic through Russia. However, these cases are promptly resolved by internet service providers once reported by users.

Blocking and Filtering

In general, online content is widely accessible for internet users in Armenia. However, during times of civil unrest, the government has been known to restrict access to social networks and other websites. On July 17, 2016, as a group of opposition gunmen stormed a police station in Yerevan after calling for an armed rebellion via Facebook, users reported that they were unable to access Facebook through major ISPs, including Armentel (Beeline) and Ucom.[21] Connectivity was reportedly restored within approximately 40 minutes.

The most prominent case of online censorship occurred in March 2008 during post-elections clashes.[22] The government declared a state of emergency and restricted certain media publications, including independent internet news outlets. The security services demanded that the Armenian domain name registrar suspend the domain names of opposition and independent news sites, and requested that ISPs block certain outside resources, such as some opposition pages on social network platforms, particularly the blog platform LiveJournal, which was popular among opposition and civil society activists. Armenian authorities were strongly criticized by international observers for restrictions on access to internet resources.[23] After the events of 2008, Armenian authorities have been very cautious about restricting internet content, though the most recent Facebook restriction could indicate that the government remains willing to block social media platforms.

Due to the fact that some internet users in Armenia receive fil ered traffic f om Russian ISPs, there have been a few cases where websites blocked in Russia are incidentally blocked for users in Ar-

20 Union of Information Technology Enterprises, "UITE History," accessed April 30, 2013, http://bit.ly/1PungBq

21 Mashable, "Facebook reportedly blocked in Armenia during unrest in the capital," July 17, 2016, http://on.mash.to/2c2lGGa.

22 Reports on the number of people killed vary; according to the official eport from the Council of Europe, eight people were killed. Thomas Hammarberg, "Special Mission to Armenia," Council of Europe, Commissioner for Human Rights, March 12-15, 2008, http://bit.ly/1OOJ6OH

23 Parliamentary Assembly of the Council of Europe, "Observation of the Presidential Election in Armenia," April 8, 2008.

menia. For example, in July 2015, a Russian opposition media outlet and a gambling website, both blocked in Russia by a court decision, were blocked in Armenia as well. Following the fi st reports, Beeline started to work toward unblocking the websites and restored them later that same day.[24]

According to Article 11 of the Law on Police,[25] law enforcement authorities have the right to block particular content to prevent criminal activity; in practice, such blocking cases have been limited to locally-hosted, illegal content such as illegal pornography or copyright-infringing materials. For example, in 2012 the police blocked the website Armgirls.am for disseminating pornographic content and for hosting bulletins of women working in the Armenian sex industry.[26] Article 263, section 20 of the criminal code stipulates that the production and dissemination of pornographic materials or items, including printed publications, films and videos, images or other po nographic items, advertisements, or sales is punishable by a fine in the amount f fi e hundred times the minimum monthly salary in Armenia, or imprisonment for up to two years.

Any decision of a law enforcement body to block particular content can be challenged in court by the resource or content owners, and if the court rules that the measure was illegal or unnecessary, the resource or content owners may claim compensation. Additionally, Armenia is a signatory to the European Convention on Human Rights; therefore, any such decision can also be challenged at the European Court of Human Rights.

Content Removal

In May 2015, an episode of a web series satirizing the police response to protests in Yerevan was removed by YouTube. The video was flagged by the police for emoval for copyright infringement since it contained a copyrighted clip of a news report, though it was likely targeted because it was mocking police behavior.[27] The Armenian police also took the authors of the web series, SOS TV, to court claiming the episode contained insults towards the police. The trial began on July 28, 2015, with the police seeking a public apology and a fine f AMD 2 million (US$4,200). SOS TV continued to refuse to apologize for their satirical clip.

Internet service providers involved in transmitting illegal content, such as child pornography, or content related to online crime or cyberterrorism, are not liable for carrying such content, provided that they had no prior knowledge of it.

Media, Diversity, and Content Manipulation

Armenian internet users are able to access a wide array of content online, though online media outlets based within the country are subject to financial and political p essures. Similar to traditional media outlets such as television or printed press, Armenian internet news resources are exposed to political pressure. In some cases, journalists are not allowed to deviate from the editorial policy of online media outlets, which are often linked to one of the political parties. Such pressure has the potential to affect the overall situation of freedom of speech in the country, though online publishers

24 "Ej.ru and bet365.com blocked by Russian Roskomnadzor in Armenia," *Samvel Martirosyan* (blog), July 1, 2015, http://bit.ly/1QI6NpZ

25 "Episode of Satirical Web Series Removed from YouTube After a Complaint from Armenian Police," *ePress,* May 26, 2015, http://bit.ly/1MPFw6F

26 "Armenia's Police block a site offering intimate services," *Media Max*, March 23, 2012, http://bit.ly/1W2n54J

27 SOS, Facebook Page, http://on.fb.me/1PuqZin

and individual bloggers strongly resist self-censorship. Indeed, there is a wide diversity of opinion on social media, and virtual battles between supporters and opponents of the government are often observed. A variety of independent and opposition web resources provide Armenian audiences with politically neutral, or oppositional opinions.

However, throughout the fla e up of hostilities between Armenia and Azerbaijan over the disputed Nagorno-Karabakh territory, expression online was skewed by the Defense Ministry's appeals to citizens to refrain from discussing the situation on the frontline on the internet, for fear of revealing "war secrets" to the other side. Online commentators practiced self-censorship, and discussions online often turned hostile when publications or users were perceived to be publishing unfavorable information or figu es about Armenia's standing in the conflict [28]

Digital Activism

Young activists campaigning against energy price hikes utilized Facebook to mobilize thousands of supporters in a major protest movement, which blocked Baghramian Avenue, a central street in Yerevan, for two weeks starting from June 22, 2015, and also reverberated in the regions.[29] The protest action known as Electric Yerevan attracted international media coverage after the police used force and water cannons to break up protestors on June 23, 2016. The movement regrouped and went on protesting, forcing the authorities to promise concessions, including a temporary price freeze while a special commission investigated the reasons for the increase, as well as government subsidies for some of the most vulnerable social groups.

In another example of digital mobilization, an activist group called "No Pasaran" (You Won't Pass It),[30] campaigned between September and December 2015 against constitutional amendments which may allow Armenian President Serzh Sargsyan to serve for a third term. Activists relied on social media to spread their message, sharing informative videos and communicating via Facebook. The constitutional changes were ultimately passed in a referendum held on December 6, 2015, a move which was criticized by local and international observers amid suspicion of irregularities in the voting process. [31]

Violations of User Rights

There have been few cases of prosecutions against internet users or bloggers for content posted online. While Armenia eliminated criminal penalties for defamation in 2010, concerns over high financial penalties for defamation persist, though the number of cases and the fines have decreased in recent years. Journalists from print and broadcast media have been subject to intimidation and attacks, though no cases of violence against online journalists were recorded during this coverage period.

28 "Keep the Military's Secrets," Ministry of Defense, May 4, 2015, http://www.mil.am/hy/media/video/67; Defense Ministry Statement, May 4, 2015, http://www.mil.am/hy/media/video/65

29 "No to Plunder", Facebook Page, http://on.fb.me/1YviXYl

30 "No Pasaran," Facebook Page, http://on.fb.me/1TrULXm

31 Transparency International anticorruption center, "Final Report: Observation Mission for the Constitutional Amendments Referendum of the Republic of Armenia on December 6, 2015," http://bit.ly/1TKloXX; OSCE/ODIHR Election Expert Team, "Armenia, Constitutional Referendum, 6 December, 2015, Final Report," http://bit.ly/1U37CiP.

Legal Environment

The Armenian constitution was amended following a referendum held on December 6, 2015. The new constitution continues to guarantee freedom of speech in Article 42, irrespective of the source, person, or place, applying to both individuals and media outlets.

In 2003, Armenian media legislation changed significantly with the adoption f the Law of the Republic of Armenia on Mass Media (also referred to as the Media Law).[32] One the most positive changes was the adoption of unified egulation for all types of media content irrespective of the audience, technical means, or dissemination mechanisms. The Television and Radio Law contains additional requirements on content delivery, but it does not regulate news, only erotic or violent programs, as well as advertising, the mandatory broadcast of official communications, and rules on election coverage and other political campaigns. Content delivered thorough a mobile broadcasting platform or the internet is subject to the same regulations.

In a positive development, the Constitutional Court of Armenia ruled on October 20, 2015 that journalists are not obliged to disclose their confidential sou ces, with the exception of cases involving serious crimes or where people could be in danger. The case was brought to the court after state prosecutors dropped controversial charges brought against Kristine Khanumian, editor of the ilur. am news website, for refusing to disclose the confidential sou ce behind a June 2014 report that accused a senior Armenian police officer f assaulting two men. The charges were subject to criticism from international organizations.[33]

Overall, Armenian criminal legislation grants journalists certain protections related to their profession. According to Article 164 of the criminal code, hindering the legal professional activities of a journalist or forcing a journalist to disseminate or withhold information is punishable by fines or co - rectional labor for up to one

year. The same actions committed by an official abusing their position is punishable by cor ectional labor for up to two years, or imprisonment for up to three years, and a ban on holding certain posts or practicing certain activities for up to three years.[34] However, neither criminal law nor media legislation clearly defines who qualifies as a jo nalist or whether these rights would apply to online journalists or bloggers.

In May 2010, the Armenian National Assembly passed amendments to the administrative and penal codes to decriminalize defamation, including libel and insult, and introduce the concept of moral damage compensation for public defamation.[35] The initial result was an increase in civil cases of defamation, often with large fines as penalties. In No ember 2011, the Constitutional Court ruled that courts should avoid imposing large fines on media outlets for defamation, esulting in a decrease in the number of defamation cases. Defamation has been used by Armenian politicians to restrict public criticism (see Prosecutions and Detentions for Online Activity), though it is not considered to

32 The Law of the Republic of Armenia on Mass Media of December 13, 2003, http://bit.ly/2cBhAdK

33 OSCE, "Forcing journalists to disclose confidential sou ces infringes work of media in Armenia, OSCE representative says," July 16, 2015, http://bit.ly/1R6cahX; Reporters Without Borders, "Journalist Prosecuted for refusing to reveal her source," July 21, 2015, http://bit.ly/1M6eoMZ

34 Art. 164, Criminal Code of the Republic of Armenia as amended on January 6, 2006, accessed April 30, 2014, http://bit.ly/1jxplj9

35 Concept of compensation for moral damage caused by defamation was introduced by adding Article 1087.1 to the Civil Code of the Republic of Armenia, Official Bulletin f the Republic of Armenia, 23 June 2010 No 28(762).

significantly curb oppositional viewpoints or media independence.

Since 2003, when the concept of cybercrime was first introduced in the Armenian criminal code,[36] criminal prosecution for crimes such as illegal pornography or copyright infringement on the internet demonstrates that Armenian law enforcement authorities generally follow the practices of the European legal system, and neither service providers nor content hosts have been found liable for illegal content stored on or transmitted through their system without their actual knowledge of such content. The downloading of illegal materials or copyrighted publications is not prosecuted under Armenian legislation unless it is downloaded and stored for further dissemination, and the intention to disseminate must be proved. Armenia is a signatory to the Council of Europe's Convention on Cybercrime, and further development of Armenian cybercrime legislation has followed the principles declared in the Convention.

Armenian criminal legislation also prohibits the dissemination of expressions calling for racial, national, or religious enmity, as well as calls for the destruction of territorial integrity or the overturning of a legitimate government or constitutional order.[37] These laws apply to expression both online and offline.

Prosecutions and Detentions for Online Activities

No cases of imprisonment or other criminal sanctions for online activities were recorded over the past year. However, cases of civil liability, such as moral damages compensation for defamation, have been recorded several times over the past few years.[38] There were 15 civil defamation and insult suits against journalists and the media in 2015, according to the Committee to Protect Freedom of Expression.[39] Of these cases, 13 included online media or media outlets that also have an online presence.

Surveillance, Privacy, and Anonymity

The newly adopted Law on the Protection of Personal Data came into effect on July 1, 2015.[40] The law is intended to ensure the implementation of the right to personal privacy with respect to the processing of personal data, bringing Armenian legislation regarding personal data in line with the European standards and international obligations. The law created the Agency for Protection of Personal Data, which started operating in October 2015. The agency is headed by Shushan Doydoyan, the founder of the Freedom of Information Center of Armenia, and will have the authority to appeal decisions of state agencies where they violate the right to privacy with regard to personal data.

The collection of an individual's personal data by the government is allowed only in accordance with a court decision in cases prescribed by the law. The monitoring and storing of customers' data is illegal unless it is required for the provision of services. Personal data can be accessed by law en-

36 Cybercrime was defined under the new Criminal Code of the Republic of Armenia, adopted on April 18, 2003. The first prosecution case for the dissemination of illegal pornography via the internet was recorded in 2004.

37 Art. 226 and 301 of the Criminal Code of the Republic of Armenia, accessed April 30, 2014, http://bit.ly/1jxplj9

38 "Demanding Financial Compensation from Armenian News Outlets is Becoming Trendy," Media.am, March 3, 2011, http://bit.ly/1MPHcx1

39 CPFE, "Annual report 2015", http://bit.ly/1USZ9y4

40 National Assembly of Armenia, "The Law on Protection of Persoanal Data" [in Armenian], http://bit.ly/1R7RMTT

forcement bodies only with a court decision. Motions must be justified, and if not, the defense attorney may insist on the exclusion of evidence obtained. Nonetheless, the courts support most data requests from law enforcement bodies.

Anonymous communication and encryption tools are not prohibited in Armenia; however, the use of proxy servers is not very common. Individuals are required to present identification when purchasing a SIM card for mobile phones. No registration is required for bloggers or online media outlets, though tax authorities may question bloggers or media outlets on revenue-related issues (advertisements or paid access).

Armenian legislation does not require access or hosting service providers to monitor traffic or content. Moreover, the Law on Electronic Communication allows operators and service providers to store only data required for correct billing. Cybercafes and other public access points are not required to identify clients, or to monitor or store their data and traffic information.

Intimidation and Violence

There were eight documented cases of physical violence against journalists in 2015, according to CPFE.[41]

A number involved journalists and media personnel covering the June 2015 protests against energy price hikes in Yerevan or the December 6, 2015 constitutional referendum. On June 23 2015, police attacked journalists live-streaming the Electric Yerevan rally on Baghramian Avenue (see Digital Activism). Four police officers are under investigation in connection with the attacks.

On July 29, 2016, a group of plainclothes men attacked at least 14 journalists while they were covering clashes between riot police and protesters marching in support of armed gunmen who had occupied a police compound in Yerevan.[42] Some of the journalists were hospitalized as a result of the attacks; some of their equipment was broken. Armenian authorities promised to investigate the attacks.

Technical Attacks

Technical attacks target both government websites and civil society groups in Armenia. Most of the attacks are believed to originate in Azerbaijan. On June 19 and 20, 2015, a large number of Armenian websites were hacked by groups which news reports said were based in Azerbaijan. The hackers targeted state websites, including the sites of various Armenian embassies.[43]

41 CPFE Annual Report 2015, http://bit.ly/1USZ9y4

42 Committee for the Protection of Freedom of Speech, "Statement by Armenian Media Organizations," 30th July, 2016, http://bit.ly/2drc9IZ

43 "Embassy Websites Targeted in A Massive Attack," [in Armenian] *Samvel Martirosyan* (blog), January 20, 2016, http://bit.ly/1LREvwh.

Freedom House

Australia

	2015	2016
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	2	2
Limits on Content (0-35)	5	6
Violations of User Rights (0-40)	12	13
TOTAL* (0-100)	**19**	**21**

* 0=most free, 100=least free

Population:	**23.8 million**
Internet Penetration 2015 (ITU):	**85 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2016 Status:	**Free**

Key Developments: June 2015 – May 2016

- A new section of the Copyright Act passed in June 2015 would allow a copyright owner to apply to the Federal Court to compel an ISP to block access to an overseas website or service whose primary purpose is to facilitate copyright infringement (see **Blocking and Filtering**).
- A court found Google to be liable as a secondary publisher in an internet defamation case for failure to remove defamatory content from its search results, including content from its "autocomplete" function (see **Content Removal**).
- The Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 came into effect in October 2015, requiring telecommunications companies to retain metadata on their customers for two years. Law enforcement and intelligence agencies do not need a warrant to access and review metadata, except for metadata associated with journalists or their sources (see **Surveillance, Privacy and Anonymity**).
- A review of the controversial section 35P of the Security Intelligence Organisation Act recommended adding safeguards for journalists and sources who publish information about a special intelligence operation, but a bill to amend it has not yet materialized (see **Surveillance, Privacy and Anonymity**).

Introduction

Legislative developments on government surveillance and its potential implications for privacy and freedom of expression have led to a slight decline in internet freedom in Australia.

Australians have generally enjoyed affordable, high-quality access to the internet and other digital media as access has continued to expand over the past few years with the rollout of the alternative National Broadband Network.

The Liberal government, led by the former Minister of Communications Malcom Turnbull, has demonstrated a commitment to open data for research and to improving internet connectivity throughout Australia. Under Turnbull's guidance, the government continued to roll out an alternative National Broadband Network (NBN), particularly in regional areas that have had poor internet services. While the original plan under the former Labor government was to lay copper cables throughout Australia, the alternative NBN opted for less expensive fiber to the node (FTTN) cables after much criticism of the cost and effectiveness of the original NBN plan.[1]

A new Federal election was held on July 2, 2016 with no parties winning the required 76 seats to form a majority government, resulting in the formation of a coalition government with three independent Members of Parliament supporting Prime Minister Malcom Turnbull's liberal government. Unlike in previous years, the NBN and internet blocking and filtering were not election issues. The newly formed government is not likely to introduce controversial amendments that would lead to further divisions within the party and between parties.

However, recent legislative amendments have significantly increased the government's capacity for surveillance of ICTs. Data retention amendments, which were passed in March 2015 and came into effect in October 2015, require telecommunication companies to store customers' metadata for two years and allows law enforcement and intelligence agencies to access that metadata without a warrant.[2] Moreover, despite calls to amend the Australian Security Intelligence Organisation (ASIO) Act, which includes provisions that threaten journalists and whistleblowers with a ten year prison term if they publish classified information in relation to special intelligence operations, no formal bills have been introduced to date to amend the controversial provision.

Obstacles to Access

There are few obstacles to internet access in Australia. Services continue to improve in remote and rural areas throughout Australia, with both the young and elderly embracing connectivity. The ICT sector is mature and competitive, providing Australians with fair and high-quality internet connectivity.

Availability and Ease of Access

Australia had an internet penetration rate of approximately 84.5 percent as of December 2015, com-

1 Australian Government, Department of Communications, *NBN Market and Regulation Report*, October 1, 2014, accessed June 4, 2015 http://bit.ly/1VrlDDa.

2 For a comprehensive overview of the legislative history of censorship in Australia see Libertus, "Australia's Internet Censorship System," accessed February 5, 2016, http://bit.ly/1JCpGpq; See also Australian Privacy Foundation, accessed February 5, 2016, http://www.privacy.org.au.

pared to 83 percent in 2013 and 74 percent in 2009, according to the International Telecommunication Union (ITU).[3] The internet penetration rate is expected to steadily increase over the next five years with the implementation of the NBN, which includes expanded wireless, fiber to the node, and satellite services in rural communities. Although internet access is widely available in locations such as libraries, educational institutions, and cybercafés, Australians predominantly access the internet from home, work, the homes of friends and families, and increasingly through mobile phones.[4]

Access to the internet and other digital media is widespread in Australia. Australians have a number of internet connection options, including ADSL, ADSL 2+, mobile, fixed wireless, cable, satellite, fiber, and dial-up.[5] As of June 2016, almost all of internet connections were broadband, while the number of dial-up connections declined to 90,000 users out of a total of 13.3 million users.[6] Once implemented, the NBN is expected to eliminate the need for any remaining dial-up connections and make high-speed broadband available to Australians in remote and rural areas.[7]

Roughly 80 percent of all Australians have access to broadband speeds over 8 Mbps.[8] There are still parts of Australia experiencing slower broadband speeds (approximately 2.3 million people have internet connection speeds of only 1.5 Mbps to 8 Mbps).[9] According to Akamai, the average connection speed by the first quarter of 2016 was 8.8 Mbps.[10]

Age is a significant indicator of internet use: 99 percent of Australians between the ages of 15 and 17 are internet users, compared to only 51 percent of those over 65 years old.[11] According to the 2011 Census, 63 percent of Aboriginal and Torres Strait Islanders report having an internet connection, compared with 77 percent of other households.[12] The overall mobile phone penetration rate in Aboriginal communities is unknown.

According to the ITU, there were 31.7 million mobile phone subscribers in Australia by the end of 2015, compared to 31 million the previous year.[13] Fourth generation (4G) mobile services have driven recent growth, with all networks expanding coverage and experiencing increases in the number of services in operation.[14]

Internet access is affordable for most Australians even though the government no longer subsidizes internet connections for individuals and small businesses in remote and rural areas, where internet

3 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," accessed October 9, 2016, http://bit.ly/1cblxxY.

4 Australian Bureau of Statistics (ABS), "8146.0 - Household Use of Information Technology, Australia, 2014-2015: Personal internet use," February 18, 2016, http://bit.ly/1Ny07ND.

5 ABS, "8153.0 – Internet Activity, Australia, June 2016: Type of Access Connection," http://bit.ly/1Mq30uD.

6 ABS, "8153.0 – Internet Activity, Australia, June 2016: Type of Access Connection," http://bit.ly/1Mq30uD.

7 NBNCo, "NBN set to narrow digital divide for 400,000 homes and businesses," media release, February 09, 2015, http://bit.ly/16VvWwI.

8 ABS, "8153.0 – Internet Activity, Australia, December 2015: Type of Access Connection: Advertised Download Speed."

9 ABS, "8153.0 – Internet Activity, Australia, December 2015: Type of Access Connection: Advertised Download Speed."

10 Akamai, State of the Internet: Q1 2016 Report, http://akamai.me/2cDNH9i.

11 Australian Bureau of Statistics (ABS), "8146.0 - Household Use of Information Technology, Australia, 2014-2015: Personal internet use," February 18, 2016, http://bit.ly/1Ny07ND.

12 ABS, "Census of Population and Housing: Characteristics of Aboriginal and Torres Strait Islander Australians, 2011," November 27, 2012, accessed February 5, 2016, http://bit.ly/1FIldX3.

13 International Telecommunication Union, "Mobile-cellular telephone subscriptions 2000-2015," accessed October 9, 2016, http://bit.ly/1cblxxY.

14 Australian Communications and Media Authority (ACMA), *Communications Report, 2014-15* (Canberra: ACMA, 2014) 13 and 19, http://bit.ly/1T7deYL.

affordability is not comparable to that in metropolitan areas.[15] Major internet service providers (ISPs) such as Telstra continue to offer financial assistance for internet connections to low-income families.[16]

Restrictions on Connectivity

The government does not impose restrictions on connectivity to the internet or mobile networks in Australia.

There are no limits to the amount of bandwidth that ISPs can supply, though ISPs are free to adopt internal market practices of traffic shaping. Some Australian ISPs and mobile se vice providers practice traffic shaping (also known as data shaping) under what a e known as fair-use policies. If a customer is a heavy peer-to-peer user, internet connectivity for those activities will be slowed down to free bandwidth for other applications.[17]

Under the iCode, a set of voluntary guidelines for ISPs related to cybersecurity, internet connectivity may become temporarily restricted for internet users whose devices have become part of a botnet or who are at high risk of their devices being infected with malware. Such users may have their internet service temporarily throttled or placed in a temporary wall-garden after notification [18] The ISP then supplies the user with information and helps them to clean their devices to become free from botnets and malware.

ICT Market

Australia hosts a competitive market for internet access, with 62 providers as of December 2015, ten of which are very large ISPs (over 100,000 subscribers), another 21 large ISPs (with 10,001 to 100,000 subscribers), and 31 medium ISPs (with 1,001 to 10,000 subscribers).[19] Additionally, there are a number of smaller ISPs that act as "virtual" providers, maintaining only a retail presence and offering end users access through the network facilities of other companies; these providers are carriage service providers and do not require a license.[20] Larger ISPs, which are referred to as carriers, own network infrastructure and are required to obtain a license from the Australian Communications and Media Authority (ACMA) and submit to dispute resolution by the Telecommunications Industry Ombudsman (TIO).[21] Australian ISPs are co-regulated under Schedule 7 of the 1992 Broadcasting Services Act (BSA), which combines regulation by the ACMA with self-regulation by the telecommunica-

15 Australian Government, Department of Communications, "Satellite Phone Subsidy Scheme," February 27, 2014, accessed June 18, 2015, http://bit.ly/1PNLtzM.

16 Telstra, *Bigger Picture 2015 Sustainability Report*, accessed February 5, 2016, 5-7, http://bit.ly/1FIlNUM.

17 Telstra, *Telstra Sustainability Report 2011*, (Sydney, Australia: 2011) accessed February 5, 2016, 19, http://bit.ly/1nWJ6TC.

18 *Industry Code C650:2014 iCode: Internet Service Providers Voluntary Code of Practice for Industry Self-Regulation in the Area of Cybersecurity,* (Australia, Communications Alliance, LTD: 2010) accessed February 5, 2016, http://bit.ly/1GhwCIm.

19 ABS, "8153.0 – Internet Activity , Australia: Number of Internet Service Providers (ISPs) – December 2015," accessed October 9, 2016, http://bit.ly/2dDFo1p.

20 ABS, "Internet Activity, Australia, Dec. 2009," March 30, 2010, http://bit.ly/1VnetVV.

21 ACMA, "Carrier & Service Provider Requirements, August 2, 2012, http://bit.ly/1QLdckO.

tions industry.[22] The industry's involvement consists of developing industry standards and codes of practice.[23]

Regulatory Bodies

The Australian Communications and Media Authority (ACMA) is the primary regulator for the internet and mobile telephony.[24] Its oversight is generally viewed as fair and independent, though there are some transparency concerns with regard to the classification f content. The ACMA approves self-regulatory "codes" negotiated among members of the Internet Industry Association (IIA). There are over 30 self-regulatory codes that govern and regulate Australian ICTs. In March 2014, the Communications Alliance took over the responsibilities of the IIA through a signed agreement.[25]

Small businesses and residential customers may file complaints about in ernet, telephone, and mobile phone services with the Telecommunications Industry Ombudsman (TIO),[26] which operates as a free and independent dispute-resolution service.

Limits on Content

There are relatively few limits to online content in Australia. However, the collateral blocking of legitimate content while targeting illegal content has harmed internet freedom in the past.

Blocking and Filtering

Australian law currently does not provide for mandatory blocking or fil ering of blogs, chat rooms, or platforms for peer-to-peer file sharing. ebsites are blocked or fil ered under a narrow set of restrictions. Web applications like the social-networking site Facebook, the Skype voice-communications system, and the video-sharing site YouTube are neither restricted nor blocked in Australia. However, the legal guidelines and technical practices by which ISPs fil er illegal material on websites have raised some concerns in the past years.

Controversy struck in May 2013 when it was revealed that a number of legitimate Australian websites that did not host any type of illegal or even controversial material had been blocked. Investigations revealed that the Australian Security and Investment Commission (ASIC) was using an obscure provision (section 313) of the Telecommunications Act to request the blocking of a fraudulent website.[27] ASIC's notice to the ISPs specified an IP add ess that contained the fraudulent website along with a number of legitimate websites, including that of Melbourne Free University. This was the fi st known incident of ASIC using section 313 to issue notices to ISPs to block non-Interpol material.

22 *Australian Communications and Media Authority Act* 2005, accessed February 5, 2016, http://bit.ly/1jz1CyZ; *Broadcasting Services Act* 1992, accessed February 5, 2016, http://bit.ly/1VneSrn; ACMA, "Service Provider Responsibilities," November 27, 2012, http://bit.ly/1FEL6ri, accessed February 5, 2016.

23 Chris Connelly and David Vaile, *Drowning in Codes: An Analysis of Codes of Conduct Applying to Online Activity in Australia*, Cyberspace Law and Policy Centre, Sydney, March 2012, http://bit.ly/1Vnfj54.

24 ACMA, "The ACMA Overview," August 20, 2012, http://bit.ly/1jz2hQL; ACMA, "About communications & media regulation," August 20, 2012, http://bit.ly/1OGxfn0.

25 Communications Alliance, "Internet Service Provider Industry," August 19, 2014, accessed Feb 5, 2016, http://bit.ly/1LPtIRq.

26 Telecommunications Industry Ombudsman, accessed February 5, 2016, http://www.tio.com.au.

27 Renai LeMay, "Interpol fil er scope creep: ASIC ordering unilateral website blocks," *Delimiter*, May 15, 2013, http://bit.ly/1OGxYoc.

While access to the affected websites was quickly restored, the use of section 313 in this matter was contentious. This led to a formal review of section 313(3) in 2015 to investigate public policy concerns.[28] The committee's final eport was released on June 1, 2015 but has not yet resulted in any new bills or amendments to section 313(3) or 314 of the Telecommunications Act.[29]

As of June 2015, copyright holders may now apply to the Federal Court to request that overseas copyright infringing locations (websites and services) be blocked by Australian ISPs under the newly amended section 115A of the Copyright Amendment (Online Infringement) Act 2015.[30] When making a decision, the court must take into consideration whether the overseas online location has a primary purpose of facilitating copyright infringement, whether the response is proportionate in the circumstances, and whether or not blocking is in the public interest.[31] It is yet to be seen how the courts will interpret "primary purpose" and "blocking in the public interest" as to whether blocking could extend to websites that are mostly non-infringing.

In March 2015, the Communications Alliance also developed the Industry Code Copyright Infringement Scheme, which would require ISPs to issue warnings to users who repeatedly download content illegally (predominantly songs, movies, and TV shows) within a "graduated response scheme" (GRS) warning offenders of their illegal online activity.[32] Unlike GRS systems in other countries such as France and New Zealand, the Australian Scheme does not allow an ISP to terminate an account, apply fines, or th ottle the connections of users who infringe copyright. The scheme has not yet been implemented as it was deemed to be too expensive for copyright holders and ISPs to implement at present, but it may still be implemented in the future.[33]

Content Removal

There were no cases of the government forcing content to be removed fromwebsites during the coverage period. However, a decision by the Supreme Court of South Australia in October 2015 found that Google was liable, as a secondary publisher, for defamatory content revealed in Google's search results, including results through the autocomplete function, snippets and hyperlinks to defamatory content published by third party websites against the plaintiff.[34] Google was ordered to pay damages to the plaintiff.[35] Reactions to the decision were mixed, although some commentators raised concerns that it could set a dangerous precedent for potential abuse by certain claimants seeking to censor legitimate criticism online.[36]

28 Parliament of Australia, "Inquiry into the use of subsection 313(3) of the Telecommunications Act 1997 by Government Agencies to Disrupt the Operations of Online Legal Services," accessed February 5, 2016, http://bit.ly/1zQYodS.

29 House Of Representatives Standing Committee of Infrastructure and Communications, *Balancing Freedom and Protection*, June 1, 2015, http://bit.ly/1RgfhWT.

30 House of Representatives, Copyright Amendment (Online Infringement) Bill 2015, accessed February 5, 2016, http://bit.ly/1zEHKM6.

31 There are more listed considerations. See *Copyright Act 1968*, s.115A.

32 Madeleine Hefferman, "Online Piracy crackdown looms," *Sydney Morning Herald*, May 5, 2014, http://bit.ly/1MGFwUB.

33 Claire Reilly, "Three strikes out: anti-piracy scheme shelved over prohibitive costs," February 18, 2016, C/Net, http://cnet.co/2dPPx9o.

34 *Duffy v Google Inc* [2015] SASC 170

35 Candice Marcus, "Google ordered to pay Dr Janice Duffy $100,000 plus interest in defamation case," Abc news, December 23, 2015, http://ab.co/2exdcaL.

36 Landers & Rogers Lawyers, "Duffy v Google – is this the end of the internet as we know it?" Defamation Bulletin, October 30, 2015; "Australian court rules that Google is liable for defamatory links," TechnoLlama, October 30, 2015.

Media, Diversity, and Content Manipulation

The online landscape in Australia is fairly diverse, with content available on a wide array of topics. Australians have access to a broad choice of online news sources that express diverse, uncensored political and social viewpoints. Digital media such as blogs, Twitter feeds, Wikipedia pages, and Facebook groups have been harnessed for a wide variety of purposes ranging from elections to campaigns against government corporate activities, to a channel for safety-related alerts where urgent and immediate updates were required.[37] Additionally, publicly funded television station SBS features fi st-rate news programs in multiples languages (available offline and online) o reflect the cultural diversity found in the Australian population.

There are no examples of online content manipulation by the government or partisan interest groups. Journalists, commentators, and ordinary internet users generally do not face censorship, so long as their speech does not amount to defamation or breach criminal laws, such as those against hate speech or racial vilification (see Legal Envi onment).[38] Nevertheless, the need to avoid defamation (and, to a lesser extent, contempt of court) has been a driver of some self-censorship by both the media and ordinary users. For example, narrowly written suppression orders are often interpreted by the media in an overly broad fashion so as to avoid contempt of court charges.[39] Court costs and the stress associated with defending against suits under Australia's expansive defamation laws have caused organizations to leave the country and blogs to shut down.[40]

Digital Activism

Australians use social media to sign petitions to the government, share controversial information, and to mobilize for public protest. Popular protests in 2015 included rallying against the closure of aboriginal communities in Western Australia,[41] protests against Halal meat,[42] and protests at the G20 Summit in Brisbane.[43]

Violations of User Rights

While internet users in Australia are generally free to access and distribute materials online, free speech is limited by a number of legal obstacles, such as broadly applied defamation laws and a lack of codified free speech rights. Additionally, legislative amendments have significantly increased the government's capacity for surveillance of ICTs, including a provision allowing law enforcement and intelligence agencies warrantless access to metadata.

37 Digital media, for example, is readily used for political campaigning and political protest in Australia. See Terry Flew, "Not Yet the Internet Election: Online Media, Political Content and the 2007 Australian Federal Election," *Media International Australia Incorporating Culture and Policy*, no. 126, (2008) 5-13, http://eprints.qut.edu.au/39366/1/c39366.pdf.

38 *Jones v. Toben (2002) FCA 1150, September 17, 2002,* http://bit.ly/1KSeqX0.

39 Nick Title, "Open Justice – Contempt of Court" (paper presentation, Media Law Conference Proceedings, Faculty of Law, The University of Melbourne, February 2013).

40 Asher Moses, "Online forum trolls cost me millions: filmmaker," *Sydney Morning Herald*, July 15, 2009, http://bit.ly/1VrnCY8.

41 Sarah Tallier, "Rallies held to protest against threat of remote community closures in Western Australia," *ABC*, May 1, 2015, http://ab.co/1YOVQJK.

42 John Elder, "So this Easter: Melbourne faces off at anti-Islam rally as police on horseback hold factions apart," *The Age*, April 5, 2015, accessed February 5, 2016, http://bit.ly/1O8ghOo.

43 Occupy G20 Brisbane, Facebook Community Page, accessed February 5, 2016, http://on.fb.me/1j12qN2.

Legal Environment

Australians' rights to access online content and freely engage in online discussions are based less in law and more in the shared understanding of a fair and free society. Legal protection for free speech is limited to the constitutionally-implied freedom of political communication, which only extends to the limited context of political discourse during an election.[44] There is no bill of rights or similar legislative instrument that protects the full range of human rights in Australia, and the courts have less ground to strike down legislation that infringes on civil liberties. Nonetheless, Australians benefit greatly from a culture of freedom of expression and freedom of information, further protected by an independent judiciary. The country is also a signatory to the International Covenant on Civil and Political Rights (ICCPR).

Australian defamation law has been interpreted liberally and is governed by legislation passed by the states as well as common law principles.[45] Civil actions over defamation are common and form the main impetus for self-censorship, though a number of cases have established a constitutional defense when the publication of defamatory material involves political discussion.[46]

Under Australian law, a person may bring a defamation case to court based on information posted online by someone in another country, providing that the material is accessible in Australia and that the defamed person enjoys a reputation in Australia. In some cases, this law allows for the possibility of "libel tourism," which allows individuals from any country to take up legal cases in Australia because of the more favorable legal environment regarding defamation suits. The right to reputation is generally afforded greater protection in countries like Australia and the United Kingdom than the right of freedom of expression. Freedom of expression is not explicitly protected under constitutional or statutory rights, although the High Court has held that there is implied freedom of political communication in the constitution. While the United States and the United Kingdom have recently enacted laws to restrict libel tourism, Australia is not currently considering any such legislation.

Prosecutions and Detentions for Online Activities

A number of lawsuits for defamation online have made the headlines in recent years. In a November 2015 trial, a jury found that a barrister had defamed a policeman, Sergeant Colin Dods, who was involved in the death of an armed teen, through comments he posted on a website in 2012. The incident in question occurred in December 2008, when teenager Tyler Cassidy entered a shopping mall yielding knives and advanced toward police officers, ignoring their requests to drop his weapons.[47] He was shot twice in the legs by Sergeant Dods, but when he continued to advance, he was shot dead. Some public outcry ensued, despite the coroner's findings that Dods' shots did not contribute to Cassidy's death and that the young man was shot dead after police officers were at risk of serious injury. The incident prompted a Queensland barrister, Mr. Michael McDonald, to publish a series of comments online calling for justice for Cassidy, accusing Dods of responsibility for Cassidy's death, proclaiming that Dods' shots were fired without provocation, and asserting that Cassidy's

44 Alana Maurushat and Renee Watt, "Australia's Internet Filtering Proposal in the International Context," *Internet Law Bulletin* 12, no. 2 (2009).

45 Principles of online defamation stem from the High Court of Australia, *Dow Jones & Company Inc v. Joseph Gutnick* (2002) HCA, 56.

46 Human Rights Constitutional Rights, "Australian Defamation Law," accessed February 5, 2016, http://bit.ly/1GhEp9a.

47 Dods v McDonald [2016] VSC 201

shooting was manslaughter.[48] The jury found that McDonald's statements were indeed defamatory, leading Justice Bell to award Dods aggravated damages totaling AUD $150,000 (approximately USD $114,000) due to the level of harm caused by the online publications.[49]

In an earlier case in January 2015, a Western Australian court ordered estranged wife Robyn Greeuw to pay AUD $12,500 in damages for her defamatory Facebook postings where she alleged that her former husband Miro Dabrowski had emotionally and physically abused her for over 18 years.[50] The defense of truth was not proven. This follows the widely publicized earlier decision in the case of *Mickle v Farley* from 2013,[51] where a young man in New South Wales was fined UD $105,000 plus costs for posting defamatory statements on Twitter and Facebook about his music teacher. The case was novel for the amount of damages incurred on the defendant and for being the first Australian decision where a tweet was held to be defamatory.[52] In the case, Judge Elkaim stated that "when defamatory publications are made on social media it is common knowledge that they spread. They are spread easily by the simple manipulation of mobile phones and computer. Their evil lies in the grapevine effect that stems from the use of this type of communication."[53]

There have been several cases in the states of New South Wales and Victoria of individuals being sentenced to jail terms for publishing explicit photos of women, typically former girlfriends or boyfriends, known as "revenge porn." By way of example, in 2012 Australian citizen Ravshan Usmanov pled guilty to publishing an indecent article and was originally sentenced to six months of home detention after he posted nude photographs of an ex-girlfriend on Facebook.[54] The sentence was appealed and the court commuted the original sentence in favor of a suspended sentence.

Surveillance, Privacy, and Anonymity

Over the past few years, revelations regarding global surveillance and retention of communications data by the U.S. National Security Agency (NSA) and other intelligence agencies have raised concerns regarding users' right to privacy and freedom of expression. However, the Australian government has taken few steps to remedy these concerns and has instead moved to expand the government's surveillance capabilities.

Law enforcement agencies may search and seize computers and compel an ISP to intercept and store data from those suspected of committing a crime with a lawful warrant, as governed by the Telecommunications (Interception and Access) Act 1979 (TIAA). Call-charge records are regulated by the Telecommunications Act 1997 (TA).[55] It is prohibited for ISPs and similar entities, acting on their own, to monitor and disclose the content of communications without the customer's consent.[56] Unlawful collection and disclosure of the content of a communication can draw both civil and criminal

48 The website was called Justice for Tyler, accessed July 4, 2016, http://.justice4tylercassidyjust15.com.

49 Dods v McDonald [2016] VSC 201

50 Calla Wahlquist, "Facebook defamation: man wins lawsuit over estranged wife's domestic violence post", *The Guardian*, January 2, 2015, accessed February 5, 2016, http://gu.com/p/44hax/stw.

51 *Mickle v Farley* (2013) NSWDC, 295.

52 A 2011 case involving writer and TV personality Marieke Hardy reached a legal settlement in 2012.

53 *Mickle v Farley* [2013] NSWDC 295.

54 Heath Astor, "Ex-Lover Punished for Facebook Revenge," *Sydney Morning Herald*, April 22, 2012, http://bit.ly/1N0J70Z.

55 Telecommunications Act 1997, part 13, accessed February 5, 2016, http://bit.ly/2fwwmSE.

56 Part 2-1, section 7, of the Telecommunications (Interception and Access) Act 1979 (TIAA) prohibits disclosure of an interception or communications, and Part 3-1, section 108, of the TIAA prohibits access to stored communications. See *Telecommunications (Interception and Access) Act* 1979, part 2-1 s 7, part 3-1 s 108, accessed Feb 5, 2016, http://bit.ly/1GAvajG.

sanctions.[57] The TIAA and TA explicitly authorize a range of disclosures, including to specified law enforcement and tax agencies, all of which require a warrant. ISPs are currently able to monitor their networks without a warrant for "network protection duties," such as curtailing malicious software and spam.[58]

In a troubling development, law enforcement agencies no longer require a warrant to access, review, and store metadata under the Telecommunications (Interception and Access) Amendment (Data Retention) Act, which was passed in March 2015 and came into effect on October 13, 2015. The act requires telecommunication companies store customers' metadata for two years, which law enforcement and intelligence agencies can access and review without a warrant at any point, not just in the course of an investigation as was previously required. However, law enforcement still needs a warrant to access stored communications, as well as any metadata associated with journalists or their sources.

During this report's coverage period, a disturbing incident emerged regarding potentially inappropriate access and use of journalists' metadata. In February 2016, investigative journalist Paul Farrell of *The Guardian Australia* discovered that the Australian Federal Police (AFP) had looked at the metadata of his devices without a warrant, in what was thought to be an attempt to identify a source from an asylum seeker story.[59] In writing about the incident, Farrell stated that "over the years, under both Labor and Coalition governments, sensitive stories by journalists that embarrassed or shamed governments have often been referred to the AFP… However, this is the fi st time the AFP has ever made such an admission in Australia. They've acknowledged generally that they made requests for journalists' metadata in the past – and said they were rare – but never in a specific case"[60] The AFP argued that its investigations were not targeting journalists, but rather addressed breaches under Section 70 of the Crimes Act, notably "the offence relates to a Commonwealth officer disclosing Commonwealth information without authorization."[61] The AFP also told *The Guardian* that it "ha[d] not accessed or applied to access the metadata information belonging to any journalist since 13 October 2015" – which is when the Telecommunications (Interception and Access) Amendment (Data Retention) Act came into effect.[62]

In October 2014, parliament enacted amendments to national security legislation that increased penalties for whistleblowers and potentially allows intelligence agents to monitor an entire network with a single warrant. In particular, a new section (35P) was added to the Australian Security Intelligence Organisation Act 1979, which includes provisions that threaten journalists and whistleblowers with a ten-year prison term if they publish classified info mation in relation to special intelligence operations.[63] The controversial amendment prompted a review by the independent national security legislation monitor, Robert Gyles QC, in October 2015 to specifically assess the im act of section 35P on journalists. Gyles' report concluded that section 35P was arguably invalid as it infringed on the constitutionally protected right of freedom of political communications and was inconsistent with

57 Criminal offenses are outlined in Part 2-9 of the TIAA, while civil remedies are outlined in Part 2-10. See *Telecommunications (Interception and Access) Act 1979*, part 2-9 and part 2-10, accessed February 5, 2016, http://bit.ly/1GAvajG.

58 Alana Maurushat, "Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Obfuscation Crime Tools?" *University of New South Wales Law Journal* 16, no. 1 (2010).

59 Paul Farrell, 'The AFP and me: how one of my asylum stories sparked a 200-page police investigation', *The Guardian*, 12 February 2016, http://bit.ly/2fV0tnu.

60 Paul Farrell, "Australia's attacks on journalists are about politics, not national security," *The Guardian*, April 15, 2016, http://bit.ly/2eggnZf.

61 AFP, "Fact Check: AFP Access to Journalist Metadata," April 14, 2016, http://bit.ly/2ddo2Fz.

62 Amanda Meade, "Federal police admit seeking access to reporter's metadata without warrant," *The Guardian*, April 13, 2016, http://bit.ly/2ddoFz2.

63 *National Security Legislation Amendment Act* (No. 1) 2014, s 108.

article 19 of the International Covenant on Civil and Political Rights.[64] The government announced their intention to support the six recommendations included in Gyle's report to better protect journalists and their sources; however, no changes to section 35P have materialized to date.[65] Other worrying amendments to the Australian Security Intelligence Organisation Act include changes to the scope of warrants: notably, the definition f a "computer" was broadened to allow law enforcement to access data on multiple computers connected to a network with a single warrant.

In the midst of renewed debate over encryption, the right to privacy, and law enforcement in February 2016, both the Labor party and the Coalition voted against a Senate motion to support strong encryption. Meanwhile, April 2015 revisions to the Defense Trade Controls Act introduced restrictions on encryption software that could discourage the use of these tools. The new revisions have been criticized for being overly broad, with the potential to criminalize the use of encryption for teaching and research purposes, in addition to everyday use for privacy and security.[66]

Users do not need to register to use the internet, nor are there restrictions placed on anonymous communications. The same cannot be said of mobile phone users, as verified identification info mation is required to purchase any prepaid mobile service. Additional personal information must be provided to the service provider before a phone may be activated. All purchase information is stored while the service remains activated, and it may be accessed by law enforcement and emergency agencies provided there is a valid warrant.[67]

Intimidation and Violence

There were no reported acts of intimidation or violence resulting from online activities during the reporting period.

Technical Attacks

Cyberattacks and hacking incidents remain a common concern in Australia. According to the Australian Cyber Security Centre (ACSC), the number of cyberattacks in Australia has increased since 2014, particularly on businesses and non-government agencies, with CERT Australia responding to over 11,000 cyberattacks in 2014 and over 800 confi med instances on attacks to critical infrastructure, though the number of significant comp omises of Australian Government networks has decreased.[68] Updated ACSC statistics for 2015 and 2016 are not available

Meanwhile, a 2015 Cyber Security Study showed that over 90 percent of Australian businesses had adopted at least three out of the four recommended Top 4 Strategies to Mitigate Targeted Cyber Intrusions.[69] While there are no metrics to ascertain whether significant comp omises to business networks have decreased, there is a strong likelihood that this would be the case.

64 The Hon Roger Gyles AO QC, "Report on the impact on journalists of section 35P of the ASIO Act," October 2015, http://bit.ly/29SPG7y.

65 Attorney General for Australia, :Government response to INSLM report on the impact on journalists of section 35P of the ASIO Act," February 2016, http://bit.ly/29wCZRM.

66 Sarah Myers West, "The Crypto Wars Have Gone Global," *Deeplinks Blog,* Electronic Frontier Foundation, July 28, 2015, http://bit.ly/1MTHdxk.

67 ACMA, "Pre-paid Mobile Services—Consumer Information Provision Fact Sheet," October 23, 2012, http://bit.ly/1KShSkd.

68 Australian Cyber Security Centre, 'ACSC 2015 Threat Report' (2015), accessed June 30, 2016, http://bit.ly/1DadAb0.

69 Australian Cyber Security Centre,' 2015 Cyber Security Survey: Major Australian Businesses' (2015), accessed June 30, http://bit.ly/2dYhOwj.

Freedom House

Azerbaijan

	2015	2016
Internet Freedom Status	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	13	14
Limits on Content (0-35)	19	19
Violations of User Rights (0-40)	24	24
TOTAL* (0-100)	**56**	**57**

* 0=most free, 100=least free

Population:	**9.7 million**
Internet Penetration 2015 (ITU):	**77 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- Authorities deliberately cut off internet access for 13 days in Nardaran village, a stronghold of conservative Shia Islam in Azerbaijan, following violent clashes between residents and police (see **Restrictions on Connectivity**).
- Prosecutors investigated independent online media outlet Meydan TV for allegedly criminal business practices, interrogating some of its few remaining Azerbaijan-based journalists (see **Prosecutions and Detentions for Online Activity**).
- Independent journalist Rasim Aliyev died from injuries sustained in a brutal attack in retaliation for a Facebook post criticizing a soccer player (see **Intimidation and Violence**).
- President Aliyev pardoned scores of political prisoners, including online journalists and activists, ahead of a visit to the US. However, many more remain behind bars, with several new arrests within the coverage period (see **Prosecutions and Detentions**).

Introduction

Internet freedom declined somewhat in Azerbaijan in 2015-2016 after the government deliberately restricted internet access in the village of Nardaran after police clashes.

The government insists that the internet is free and that the authorities do not engage in censorship,[1] but the reality for internet users is very different. While the government does not extensively block online content, netizens and their families face arrest and intimidation, and progovernment trolling distorts political discussions.

Dozens of political prisoners were released in March 2016 following a presidential amnesty, but many more remain behind bars serving lengthy sentences. In the wake of the Arab Spring in 2011, the Gezi Park protests in Turkey, and the Euromaidan movement in Ukraine in 2013-2014, the government feared a spillover of unrest into Azerbaijan, and cracked down on dissent online. Amid increasing economic strain in the past year, authorities kept a tight lid on criticism, punishing satirical video-bloggers and Facebook page administrators, among others. The trend looked set to continue following a failed coup attempt in nearby Turkey in mid-2016.

Despite these limitations, the internet offered more opportunities for information-sharing and political dissent than traditional media outlets, many of which shut down or moved online as print publications were pressured to follow the government line. Azerbaijan netizens rely on Facebook as an important platform for publishing corruption investigations and discussion on the ongoing government clampdown, as well as daily grievances.

Obstacles to Access

Internet access remains expensive for much of the population, with Azerbaijan lagging behind its neighbors on indicators such as internet speed and affordability. The Ministry of Communications and High Technologies has repeatedly delayed the implementation of a project to introduce countrywide high-speed broadband. Meanwhile, the government has demonstrated its willingness to shutdown connectivity in times of civil unrest, disconnecting the entire village of Nardaran from the internet for several days following police clashes.

Availability and Ease of Access

Poor telecom infrastructure along with low information and communications technology (ICT) literacy, expensive computer equipment, and high tariffs for satellite connections—owned by the Ministry of Communication and High Technologies (MCHT)—remain key obstacles to ensuring greater internet access across the country. Internet in Azerbaijan remains expensive, though this does not translate into better quality or faster connections.

The internet penetration rate reached 77 percent in 2015, compared to 73 percent in 2013 and 27 percent in 2009, according to the International Telecommunication Union.[2] Dial up connections have

1 "İlham Əliyev deyir ki, KİV tam azaddır, söz azadlığı heç cür məhdudlaşdırıla bilməz" [Ilham Aliyev says mass media outlets are totally free, and that freedom of speech cannot be limited] *Azadliq Radiosu*, June 24, 2015, http://bit.ly/1GkAVmk.

2 International Telecommunication Union, "Percentage of Individuals Using the Internet," 2009, 2013, 2015, http://bit.ly/1cblxxY;

dropped significantly in the ast fi e years.[3] Fixed broadband subscriptions increased from 100,000 in 2009 to more than 2 million in 2015, and continue to grow at an annual rate of 10 percent.[4] The mobile broadband penetration rate in Azerbaijan reached just over 46 percent.[5]

Fewer than 10 percent of connections operate at speeds of 4 Mbps or higher, and the average internet connection speed was 3.2 Mbps in 2015, significantly below that f top performing countries which offer average connection speeds of 10Mbps to 15Mbps, according to a World Bank report.[6] Akamai reported Azerbaijan was among 34 countries where connection speed was in decline in the third quarter of 2015. As a result, socioeconomic benefits associa ed with high speed internet such as online job creation, skills development, and foreign direct investment, remain limited.

Osman Gunduz, head of the Azerbaijan Internet Forum, has said that internet users in Azerbaijan get 1.5 Mbps for every 2 Mbps they pay for, in part due to underdeveloped infrastructure.[7] The vast majority of connections in Azerbaijan are based on ADSL, with Wi-Fi, WiMAX, 3G and 4G just starting to become widespread. The government is slowly upgrading network infrastructure to provide high speed internet across the country through its Fiber to Home project.[8] Despite significant delays in the implementation of the project following the economic crisis and budget issues, the MCHT said the plan would proceed in 2016.[9]

Internet service is expensive, and Azerbaijan continues to lag behind Russia, Ukraine, Georgia and other neighboring countries, where connections are available at comparatively low cost. In 2015, internet users in Azerbaijan paid US$15-40 for 4-8 Mbps unlimited ADSL connections, which cost US$7-12 in Russia. Similarly, a 4-8 Mbps unlimited fibe -optic connection cost US$12-55 in Azerbaijan and only US$4 in Russia. An unlimited 30-35 Mbps fibe -optic connection cost Russian users US$5 on average, but US$50-185 in Azerbaijan.[10]

By contrast, the average cost of mobile internet service has dropped significantly since 2011. By 2014, the average price for mobile broadband was among the lowest in Central Asia.[11] However, the average household in Azerbaijan's lower income bracket (the bottom 40 percent of the total population by income) would need 21 percent of their monthly disposable income to afford the cheapest mobile broadband package, and 28 percent for the cheapest fi ed broadband package.[12]

A July 2015 survey by the Azerbaijan Marketing Community reported 69 percent of households own a computer, of which 50 percent are notebooks. Computer ownership is higher in urban areas than in rural areas. Over 80 percent of all landlines are concentrated in the urban areas. The majority of

3 Ministry of Communication and High Technologies, October 23, 2015, http://mincom.gov.az/media/xeberler/details/11396.

4 "Azerbaijan- Telecoms, Mobile and Broadband," *Budde*, May 24, 2016, http://www.budde.com.au/Research/Azerbaijan-Telecoms-Mobile-and-Broadband.html

5 Broadband Commission, *The State of Broadband 2015: Universalizing Broadband,* September 2015, http://bit.ly/ICdQnO.

6 The World Bank, "A Sector Assessment: Accelerating Growth of High-Speed Internet Services in Azerbaijan," December 18, 2014, http://bit.ly/1LSR5tk.

7 "The number of Internet users is on the rise", *Reytinginfo.az*, November, 7, 2015, http://bit.ly/2fkcUpL

8 "Development of fiber optic in ernet access in Azerbaijan to reach its peak by 2017", *Trend*, December 22, 2013, http://en.trend.az/azerbaijan/2224186.html.

9 "The price of internet in Azerbaijan," *Apa.tv*, http://apa.tv/cast/31/17545.

10 "Internet connection that costs 5 manats in the neighboring country, costs 300 here," *Cebhe*, October 2, 2015, http://cebhe.info/oxu/2380/.

11 The World Bank, "A Sector Assessment: Accelerating Growth of High-Speed Internet Services in Azerbaijan," December 18, 2014, http://bit.ly/1LSR5tk.

12 The World Bank, "A Sector Assessment: Accelerating Growth of High-Speed Internet Services in Azerbaijan," December 18, 2014, http://bit.ly/1LSR5tk.

internet access takes place at home, followed by workplaces, internet cafes, and Wi-Fi spots.[13] In August 2016, the MCHT announced a project to establish free public Wi-Fi spots across the capital, Baku.[14]

Restrictions on Connectivity

The MCHT holds significant sha es in a handful of leading internet service provider (ISPs), and the government is authorized to instruct companies to cut internet service under very broadly defined circumstances, including war, emergency situations, and national disasters. Wholesale access to international gateways is maintained by companies with close ties to the government. Only two operators, AzerTelecom and Delta Telecom, are licensed to connect international IP traffic [15]

On November 16, 2015, Azerbaijan experienced a nationwide internet blackout lasting six hours, which the MCHT said was caused by fi e damage to a Delta Telecom data center cable. Akamai reported that traffic d opped below 10 percent during the outage,[16] and connectivity remained poor for four days.[17] During the incident, 3G services provided by Nar Mobile and Bakcell remained available, since both connect to AzerTelecom.

Service was deliberately restricted in Nardaran village during violent clashes following a police raid in November 2015. Police said they were targeting religious militants, but news reports said they attacked a prayer meeting.[18] The authorities cut off power, telephone lines, and broadband and mobile internet connections in the village for 13 days,[19] leaving residents in darkness.[20] Authorities said that the outage was due to an outstanding electricity bill. Azerisiq, an Azerbaijani electricity company, said the village's owed AZN 42 million (US $40,000) covering the past 117 years.[21] Independent observers said the shutdown was intended to stifle info mation during the unrest.

In July 2015, WhatsApp users across the Azercell and Azerfon (Nar) networks said they were unable to make calls using the Voice over IP (VoIP) function. Both providers denied interfering with the function, which was unavailable for a few days. Users on other networks experienced no disruption, and the cause remains unclear.[22] A week later, users in some regions of Azerbaijan reported they were unable to log in to use Skype. The MCHT said Skype software updates could have caused the

13 Ministry of Communications and High Technologies, "Azərbaycan hər 100 nəfərə düşən internet istifadəçilərinin sayına görə dünya orta göstəricisini 1.8 dəfə qabaqlayır," [Azerbaijan above average for number of internet users per 100 people by 1.8] June 15, 2015, http://www.mincom.gov.az/media/xeberler/details/10319.

14 "Free Wi-Fi spots to appear in public places in Baku", *Azernews.az*, August 22, 2016, http://www.azernews.az/nation/101199.html.

15 Ministy of Communications and High Technologies, "Providers," http://www.mincom.gov.az/fealiyyet/it/internet/provayder/.

16 Akamai, "State of the Internet, Q1 2016 Report," https://goo.gl/TQH7L7.

17 "Communications Ministry assures no more Internet outage in country," *Azernews.az,* November 23, 2016, http://www.azernews.az/business/90047.html.

18 "Unrest in Nardaran after six die in police raid," *Meydan TV*, November 27, 2015, https://www.meydan.tv/en/site/news/9646/.

19 "Nardaran sealed off," *Azadliq*, December 3, 2015, http://www.azadliq.org/content/article/27404740.html.

20 Human Rights in Azerbaijan, "Nardaran event: Wide-scale violations of constitutional rights," November 30, 2015, http://www.azhr.org/#!Nardaran-event-Widescale-violations-of-constitutional-rights/cjds/566de6020cf239106879c59f.

21 "Nardaran without water and telephone," *Azadliq*, November 29, 2015, http://www.azadliq.org/content/article/27394937.html.

22 "Mobile Operators in Azerbaijan Limited Using WhatsApp", Report News Agency, July 1, 2015, http://report.az/en/ict/mobile-operators-in-azerbaijan-limited-using-whatsapp/.

problem, which resolved after a few days.[23] Observers said that providers may have deliberately sought to restrict free VoIP services on grounds that it cuts into their revenue.

Delta Telecom owns the internet backbone and is the main distributor of traffic o other ISPs. It controls Azerbaijan's only Internet Exchange Point (IXP), and charges the same amount for local and international traffic. The com any is a transit operator of Azerbaijan's segment of the Europe Persia Express Gateway (EPEC) and has external fibe -optic connections with Russia (via TransTelecom) and Turkey (via RosTelecom). AzerTelecom has a fibe -optic cable network covering all major regions, including the autonomous republic of Nakhchivan.[24]

ICT Market

The ICT market in Azerbaijan is fairly concentrated. The fi ed broadband market is still in its emerging phase, with little equality between operators. The lack of regulatory reform also inhibits development of the sector. There are over 30 ISPs,[25] including three state-owned providers: AzTelekomnet, BakInternet and Azdatakom.[26] State-owned companies ultimately control over 56 percent of the market.

The market base is split along geographical lines, with BTRIB (Baku Telephone Production Association) serving the capital.[27] AzTelekomnet, the largest ISP operating outside Baku, has ownership ties to the MCHT; its shareholders include Azerfon, which has links to the president's daughters.[28]

Azercell is still the leading mobile service provider despite its overall market share falling from 50 percent to 43 percent. Bakcell and Azerfon follow behind, maintaining a steady market share of 24 and 33 percent respectively. Like Azerfon, Azercell has been found to have connections with President Aliyev's daughters.[29]

Regulatory Bodies

The government of Azerbaijan has a major role in controlling the ICT sector through state-owned companies and government institutions. ISPs are regulated by the Ministry of Communication and High Technologies (MCHT), which lacks independence. The MCHT is responsible for establishing and enforcing ICT policy, and reports to the government on how much financial suppo t should be allocated to the sector.[30]

23 "Mobile apps not banned in Azerbaijan, problems within apps themselves" *Azernews*, 8 July 2015, http://www.azernews.az/business/85163.html.

24 Ministy of Communications and High Technologies, "Providers," http://www.mincom.gov.az/fealiyyet/it/internet/provayder/.

25 According to the Ministry Communications and High Technologies website there are 34 ISPs: http://www.mincom.gov.az/fealiyyet/it/internet/provayder/.

26 "Nə üçün İnternet qiymətləri bahadır və nə üçün İnternet keyfiyyətsizdir?" [Why In ernet costs are high and why is internet poor quality] *Azerbaijan Internet Forum*, March 11, 2014, http://bit.ly/1iOdFI0.

27 The World Bank, "A Sector Assessment: Accelerating Growth of High-Speed Internet Services in Azerbaijan," December 18, 2014, http://bit.ly/1LSR5tk.

28 Khadija Ismayilova, "Azerbaijani President's Daughter's Tied to Fast-Rising Telecoms Firm," *Radio Free Europe/Radio Liberty,* June 27, 2011, http://bit.ly/1M5IcLR.

29 "TeliaSonera behind-the-scenes connection to Azebaijani President's daughters", *AzadliqRadio Radio Free Europe Azerbaijan Service,* July 15, 2014, http://www.rferl.org/content/teliasonera-azerbaijan-aliyev-corruption-investigation-occrp/25457907.html

30 Ministry of Communications and High Technologies, "Department of Regulation," [in Russian] http://bit.ly/1iOexw1.

Limits on Content

While the government is yet to implement systematic or widespread blocking or filtering of websites or social networks, a number of websites were reportedly blocked during the coverage period. In particular, the government blocked some news coverage of deadly clashes sparked by a police raid in Nardaran in November 2015. Regulations restricting foreign financial support to organizations in Azerbaijan have effectively cut off funding to a number of media outlets, causing many to close.

Blocking and Filtering

The government does not engage in extensive blocking or fil ering of online content, relying on legal, economic, and social pressures to discourage critical media coverage or political activism. YouTube, Facebook, Twitter, and other communication applications remain freely available. However, some content was newly blocked during the coverage period.

After November 2015 clashes between citizens and police in Nardaran village, where the government said they were targeting religious militants, some websites hosting Islamic content reported they had been blocked. Islamazeri.az, a daily news website focusing on Islamic topics, reported that its internet protocol (IP) address was temporarily blocked in December 2015, and again for some days on January 26, 2016. In January and February 2016, *Cenub News*, another website covering Islamic topics, reported similar disruptions. *Cenub News* said Delta Telecom twice blocked its IP address, even after it switched to a second IP address in order to bypass the fi st block.[31] Both sites were subject to cyberattacks at the same time (see Technical Attacks).

There is no established process for appeal in cases where opposition websites or other content has been blocked, and no information on the number of websites affected. Decisions to block content are not transparent, and when users try to access censored websites they receive an error message, rather than information stating that the site has been deliberately blocked.

Content Removal

In general, authorities rely on pressure and threats to remove unwanted content, rather than court orders or other established takedown procedures. These methods have resulted in the removal of social media pages that produce political satire or are otherwise critical of the Aliyev government. In January 2016, Huseyin Azizoglu, a young blogger famous for mocking Azerbaijani police and military officials on ouTube, was forced to remove videos from his social media pages while he was in detention (see Prosecutions and Detentions).

In the wake of the failed July 2016 coup attempt in regional ally Turkey, and subsequent accusations against Gulenist actors of masterminding the coup, the authorities cracked down on Gulenist associations across Azerbaijan, including shutting down the Gulen-linked Zaman Azerbaijan newspaper and associated news website.[32]

31 "Another website released statement about its blocking", *IslamAzeri*, February 1, 2016, http://islamazeri.az/daha-bir-sayt-bloklanmasi-ile-bagli-muraciet-yaydi--30711.html.

32 "Gulen operation in Baku- Caucauss University and Zaman newspaper shut down," *Anazeber*, July 20, 2016, http://anaxeber.az/fles/24395-_akida-gulen-emeliyati-qafqaz-universiteti-ve-zaman-qezeti-baglandi.html.

Content revealing personal information without consent may be subject to removal under Articles 5.7 and 7.2 of the Law on Personal Data (see Surveillance, Privacy, and Anonymity). A written demand from the individual concerned, a court, or the executive branch is required. Authorities can also remove online content in cases of defamation. Additionally, both the MCHT and the Ministry of Education run a hotline program to uncover allegedly illegal and dangerous content.

Media, Diversity, and Content Manipulation

The ongoing government crackdown against independent and opposition media outlets—in addition to the arrests of online activists—has significantly limi ed the space for free expression in Azerbaijan. Some online journalists, commentators, and ordinary internet users have resorted to self-censorship, especially if they are employed by state media outlets or progovernment platforms.

To counter such longstanding restrictions on media freedom, alternative online platforms emerged and expanded beginning in 2005, and the Azerbaijani blogosphere blossomed in subsequent years. Facebook has become increasingly important, with more people using it for information gathering, information sharing, and criticizing the government. In April 2016, hostilities between Armenia and Azerbaijan fla ed over the disputed Nagrono-Karabakh region. The government limited the traditional media's access to information about the conflict, and de elopments were reported on Facebook instead, including the number of casualties.

However, the ability for online bloggers and activists to produce and disseminate controversial content online is undermined by government pressure, which limits the diversity of content available in the online sphere. Self-censorship is pervasive among social media users, who are aware that they may face criminal charges for their expression online. Rahim Hajiyev, former editor-in-chief of the now-defunct opposition newspaper *Azadliq*, has said that the number people who have faced arrest for their activities online discourages social media users from expressing themselves freely.[33]

The vast majority of existing online media outlets publish news in favor of the government due to the owners' strong ties to government officials. The head f Turan Information Agency, Mehman Aliyev, has said that Azerbaijan's independent media has struggled to stay afl at since the 1990s. According to Aliyev, the majority of media outlets in Azerbaijan are government controlled and government funded. Many outlets spread state propaganda, in violation of the Law on Mass Media and the Journalism Code of Ethics.[34] Yet in January 2016, the Prosecutor's office issuing a wa ning that it was monitoring internet-based outlets, and several had violated the mass media law by sharing incorrect information on nationwide protests following a currency devaluation.[35] The limits imposed on independent or opposition media outlets make it difficult for them o attract advertising to sustain their work. Companies are reluctant to support them for fear of losing their business license or other reprisals from the government.

Laws regulating the foreign funding of NGOs have made it easier for the government to target local organizations and media outlets that receive grants from outside sources. In February 2014, President Aliyev approved amendments to the law on grants, further limiting civil society. In February

33 "Rashad Majid: insults on Facebook," *Azadliq*, June 5, 2015, http://www.azadliq.org/a/27055509.html.

34 "On 'Press Freedom Day' this is the state of Azerbaijan media," *Azadliq*, May 3, 2015 http://www.azadliq.org/content/article/26991333.html.

35 "Notification f om Prosecutor to mass media communication," *Azadliq*, January 29, 2016 http://www.azadliq.org/content/article/27518894.html.

2015, Aliyev signed amendments to the mass media law that allow the courts to order the closure of any media outlets that receive foreign funding or that are convicted of defamation twice in one year. The requirements for receiving grants are now so complicated that they prevented a number of online media outlets from continuing their work. Mediaforum.az, Obyektiv TV, Channel 13, and Zerkalo/Ayna (which also existed in print until May 2014[36]) have all ceased operations because of the new restrictions. The past year saw the closure of remaining independent media outlets like the Radio Free Europe/Radio Liberty's Azerbaijani service and the websites of local non-governmental organizations and media outlets that receive foreign funding were blocked.

Commercial pressures separately resulted in the closure of online news and tabloid outlets in 2015, including three websites operated by APA Holding (kulis.az, ailem.az, and avtolent.az), and three from the Daily Telegraph group (kult.az, izvestiya.az, and tabloid.az). These closures were not political in nature, but they illustrate the financial p essures affecting online media. [37]

Extensive and coordinated trolling continues to be a problem in Azerbaijan, with new social media accounts opening on a regular basis targeting sources critical of the government. Researchers report the intensity and amount of coordination behind this activity has increased, suggesting that the government has adopted a policy of actively manipulating online discussions. In advance of the launch of the European Games, which Azerbaijan hosted in June 2015, progovernment youth groups were deployed to troll international media outlets and foreign and local critics online, particularly on Twitter. These trolls and bots refuted any antigovernment and anti-Aliyev content, often using violent or degrading language. Some were students from Baku State University, Azerbaijani Diplomatic Academy, University of Languages, and Slavic University, according to their profiles. Othe s were members of progovernment youth movements such as AGAT (Integration of Azerbaijani Youth to Europe) and the youth branch of the ruling party, Yeni Azerbaijan.

Digital Activism

Activists continue to use social media platforms to disseminate information and organize campaigns, though the impact is fairly limited.

During the coverage period, several online campaigns attracted support from Azerbaijani netizens. The most recent was sparked by a series of protests which shook the country in January 2016. Residents of more than a dozen administrative districts took to the streets demanding jobs, food, and sharing their frustration about price hikes. While none of the existing media outlets covered the protests, information circulated online via independent online media outlets and social media, including video footage. Radio Liberty surveyed Baku residents who said the internet was their main source of information about the protests.[38]

Another popular campaign followed the arrest of well-known investigative journalist Khadija Ismayilova on December 5, 2014 on trumped up charges of inciting a former colleague to commit suicide. In February 2015 she was charged with additional crimes of tax evasion, abuse of power, and illegal

36 Reporters Without Borders, "Deprived of income, Azerbaijan paper is forced to stop publishing," June 20, 2014, https://rsf.org/en/news/deprived-income-azerbaijan-paper-forced-stop-publishing.

37 "Six Websites in Azerbaijan Closed" *Qafqaz Info*, March 2, 2015, http://www.qafqazinfo.az/xeber-azrbaycanda-alt-sayt-baland-t113692.html.

38 "What happened in Siyazan anyway? TV won't show anything," *Azadliq*, January 15, 2016 http://www.azadliq.org/media/video/27488179.html.

entrepreneurship in retaliation for her reporting. The #FreeKhadija hashtag was used widely to share news, statements, and updates on her case until her release in May 2016.

Violations of User Rights

Authorities continue to prosecute and arrest online activists and journalists as a means of stifling dissent and activism, and target remaining independent online media outlets with bogus criminal charges. Government surveillance and monitoring of social media accounts continues be an issue. Many activists and opposition party members who are arrested or detained report that police have referenced their online communications during interrogations. The former minister of Communications and High Technologies announced that services Facebook, WhatsApp and Skype would require a license to operate in Azerbaijan, illustrating the government's intention to monitor and control online communication.

Legal Environment

While the right to freedom of expression is guaranteed in the constitution and Azerbaijan is a signatory to binding international agreements, including the International Covenant for Civil and Political Rights and the European Convention on Human Rights, the government frequently fails to protect the right to freedom of expression, both offline and online

Libel is the most common criminal charge used against journalists. In 2013, a court ruled that social media was subject to libel laws as a form of mass media when it sentenced Mikail Talibov, a former bank employee, to one year of corrective labor for criticizing his former employer on Facebook.[39] Under legal amendments passed on May 14, 2013, defamation committed online falls under the criminal code, punishable by up to six months in prison, or up to three years for aggravated defamation. Furthermore, it is now possible for the Prosecutor and the Ministry of Interior to initiate an investigation based on content posted on Facebook.[40] The same amendments increased the duration of administrative detentions from 15 days to 3 months. Administrative detentions, which can be issued for charges such as disorderly conduct, have been used to punish activists and journalists.

Prosecutions and Detentions for Online Activities

Online activists and journalists are most often prosecuted based on trumped up charges, including drug possession, hooliganism, and, more recently, treason, tax evasion, abuse of authority, and embezzlement. In March 2016, President Aliyev pardoned a number of imprisoned activists, including blogger Omar Mammadov, political activist Sirac Karimov, and rights defender Rasul Jafarov.[41] However, many website administrators, editors of online news outlets, and bloggers in Azerbaijan remain in jail for their online activities. In some cases, authorities have also harassed activists' family members.

39 "In Azerbaijan, bank tied to EBRD breaks seal on controversial libel law," *Radio Free Europe/Radio Liberty*, August 21, 2013, http://www.rferl.org/content/azerbaijan-ebrd-libel-law/25082305.html.

40 "Can pages humiliating state officials be closed?" *Azvision*, June 6, 2015, http://www.az.azvision.az/news.php?id=62722.

41 Amnesy International, "Azerbaijan release of 10 prisoners of conscience is a glimmer of hope for those still behind bars," March 17, 2016, http://www.amnestyusa.org/news/press-releases/azerbaijan-release-of-10-prisoners-of-conscience-is-a-glimmer-of-hope-for-those-still-behind-bars.

The following activists and journalists were charged, investigated, arrested, or sentenced during the coverage period for their online activities:

- Fuad Gahramanli, deputy chair of the Whole Azerbaijan Popular Front Party, was arrested December 8, 2015 and was accused of making pro-Nardaran statements on Facebook. He was charged under Article 281 of the Criminal Code (making anti-government statements) and 283 (instilling national, religious, and racial hatred). Furthermore, those who "liked" his posts were called in to testify.[42] On March 15, 2016, Gahramanli was further charged with inciting mass disorder (Article 220.2). Gahramanli remained in prison with hearings ongoing in mid- 2016.

- In April 2016, prosecutors launched a criminal investigation against independent Berlin-based online media outlet, Meydan TV, on allegations of illegal business activities, tax evasion, and abuse of power. Fifteen individuals were named in the investigation; some were subject to questioning and had their homes searched.[43]

- Mehman Huseynov, a well-known critical blogger and brother of Emin Huseynov, the exiled former director of the Institute for Reporters' Safety and Freedom, was detained on November 29, 2014, when his passport and national ID were taken away from him. He remains without documents, cannot leave the country, and is facing criminal charges for hooliganism and resisting police in an ongoing investigation.

- Khalid Khanlarov, a student and blogger, was arrested on January 23, 2016, and served 25 days of administrative detention for resisting police. The Ministry of Internal Affairs had questioned him about his activities on social networks before his arrest.[44] Khanlarov administers the satirical Facebook page "Ditdili," which is critical of the government. Khanlarov's lawyer Shahla Humbatova, who was initially barred from seeing her client in prison, said Khanlarov was pressured to write a confession under threat of a longer jail sentence.[45]

- Huseyin Azizoglu, a well-known video blogger, was arrested on January 8, 2016 and sentenced to 15 days of administrative detention. Azizoglu shared videos which were critical of law enforcement in Azerbaijan through YouTube and his Facebook page, "Three Faces" (Uc uz). Two days after his arrest, videos ridiculing law enforcement were removed from his social media pages, though his work can still be found through other YouTube accounts.[46] The police made no official sta ements about the reasons for Azizoglu's arrest.

Despite the presidential pardons of March 2016, many online activists remain in prison, serving particularly long sentences. These include:

42 "Like" edenler sahid kimi dindirilib, [Those who "liked" were questioned as witnesses], *Azadliq*, June 29, 2016, http://www.azadliq.org/a/fuad-qehremanlinin-istintaqi/27827603.html.

43 Committee to Protect Journalists, "Azerbaijani Authorities Open Criminal Investigation into Meydan TV," April 22, 2016, https://cpj.org/2016/04/azerbaijani-authorities-open-criminal-investigatio.php.

44 "Blogger Khalid Khanlarov Barred from meeting with lawyer", *Meydan TV,* February 1, 2016, https://www.meydan.tv/en/site/politics/11582/Blogger-Khalid-Khanlarov-barred-from-meeting-with-lawyer.htm.

45 Arzu Geybulla, "How government of Azerbaijan Educates its outspoken bloggers," *Flying Carpets and Broken Pipelines*, [Blog] February 3, 2016, http://flyingcarpetsandb okenpipelines.blogspot.com/2016/02/how-government-of-azerbaijan-educates.html?spref=tw.

46 "In oil rich Azerbaijan people protest government responds with arrests," *Global Voices*, January 16, 2016 https://globalvoices.org/2016/01/17/in-oil-rich-azerbaijan-people-protest-government-responds-with-arrests/.

- Abdul Abilov remains in prison serving a fi e-and-a-half year sentence after being arrested in 2014 on drug charges. Abilov was known for his online political activity and criticism of authorities.[47]

- Araz Guliyev, former editor and writer for the religious website Xeber44.com, is serving an eight year sentence after being arrested in 2012 and convicted of various offences including insulting the national flag f Azerbaijan and inciting religious and ethnic hatred.[48]

- Ilkin Rustamzade is serving an eight year sentence for hooliganism and inciting a riot after participating in a "Harlem Shake" YouTube video. Rustamzade was arrested in 2013 and was known for his criticism of the government through the Free Youth Organization.[49]

- Nijat Aliyev remains in prison after being arrested in 2012, serving a ten year sentence for drug possession and illegal distribution of religious material. Aliyev was the editor-in-chief of news website Azadxeber.az ("free news").[50]

- Rashad Ramazanov is currently serving a nine year prison sentence after being arrested in May 2013 on drug charges. Ramazanov had worked as a blogger and activist who frequently criticized the government online.[51]

Surveillance, Privacy, and Anonymity

It is unclear to what extent security agencies monitor ICT activity or track user data in Azerbaijan, though the experience of activists and bloggers who are detained by the authorities suggests that extensive online surveillance is highly likely. Most internet users do not have licenses for the software on their computers, which leaves them vulnerable to security threats such as viruses and other malicious programs that could be implanted to monitor their activity.

While the law explicitly prohibits the arbitrary invasion of privacy, and court orders are required for the surveillance of private communications, the Law on Operative-Search Activity (Article 10, Section IV) authorizes law enforcement agencies to conduct surveillance without a court order in cases regarded as necessary "to prevent serious crimes against the person or especially dangerous crimes against the state." The unclear parameters for what constitutes preventive action leaves the law open to abuse. As such, it has long been believed that the Ministry of National Security and Ministry of Internal Affairs monitor the phone and internet communications of certain individuals, especially foreigners, known activists, and business figu es.

Rashi Hajili, the director of the Media Rights Institute, reports that the internet is heavily monitored by the government. The Ministry of Communications requires all telecom companies to make available their equipment and special facilities to the National Security Service (formerly Ministry of National Security). Mobile companies are known to surrender the content of users' phone conver-

47 "Azerbaijan Jails Opposition Blogger," *Radio Free Europe/Radio* Liberty, May 27, 2014, http://www.rferl.org/content/azerbaijan-jails-opposition-blogger/25400283.html.

48 Council of Europe, "Senior Journalist Araz Guliyev Sentenced to Eight Years in Prison in Azerbaijan," April 1, 2015, http://bit.ly/226Z61Z.

49 Human Rights Watch, "Azerbaijan Government Repression Tarnishes Chairmanship," September 29, 2014, https://www.hrw.org/news/2014/09/29/azerbaijan-government-repression-tarnishes-chairmanship.

50 Ref World, "2015 Prison Census: Nijat Aliyev," December 14, 2015, http://www.refworld.org/docid/56701fbe31.html.

51 Human Rights Watch, "Azerbaijan Bgus Drug Charges Silence Critics," May 27, 2015, https://www.hrw.org/news/2013/05/27/azerbaijan-bogus-drug-charges-silence-critics.

sations without a court order. For example, a mobile phone operator provided the Ministry of Investigation with journalist Parviz Hashimli's communications, resulting in a prison sentence.[52] He was released in the March 2016 amnesty.

In February 2014, Citizen Lab reported that Azerbaijan, along with 20 other governments, is suspected of using RCS (Remote Control System) spyware sold by the intelligence technology and surveillance company Hacking Team. RCS spyware allows anyone with access to activate a computer's webcam and microphone and steal videos, documents, contact lists, emails, or photos. The spyware has been used by governments around the world to spy on dissidents. In July 2015, leaked documents from Hacking Team revealed that the government of Azerbaijan was also a client.

All mobile phones in Azerbaijan must be registered, including the SIM card, phone serial number, and mobile network number. This requirement was introduced by the Cabinet of Ministers in December 2011—without parliamentary approval. Mobile service providers are required to limit service to any unregistered devices.

In August 2015, MCHT said it will require some social media and instant messaging services, including Facebook, WhatsApp, Skype, and Viber, to obtain a license in order to operate in Azerbaijan. The former Minister of High Communication Technologies, Ali Abbasov, stated that the new regulations are necessary due to the companies' mass data collection capacity, and that it would not impede their operations.[53] News reports said the government was negotiating with the companies over the possible requirement. Legislation in Azerbaijan subjects some communications services to licensing, but not the social networks in question.[54] It remains unclear what the license is intended to achieve, though some commentators have speculated that it will be used to give authorities greater leverage over tech companies.[55] The requirement had not been introduced in mid-2016.

The personal data law regulates the collection, processing, and protection of personal data (name, surname, patronymic, date of birth, racial or ethnic background, religion, family, health and criminal record), the formation of the section of personal data in the national information space, as well as issues related to the cross-border transfer of personal data.

Intimidation and Violence

Most harassment against online activists manifests in the form of arrests, detentions, and interrogations. The government of Azerbaijan also uses travel bans against activists and human rights defenders like Mehman Huseynov (see Prosecutions and Detentions for Online Activities), as well as members of non-governmental organizations.

Physical attacks and threats of violence against internet users have also become increasingly common in Azerbaijan. Emin Mili, the founder of Meydan TV, received death threats from Azerbaijan's

52 "TeliaSonera's behind-the-scenes connection to Azerbaijani president's daughters," *Radio Free Europe/Radio Liberty*, July 15, 2014, http://www.rferl.org/content/teliasonera-azerbaijan-aliyev-corruption-investigation-occrp/25457907.html

53 "Azerbaijan begins negotiations with social networks," *Report.az*, August 27, 2015, http://report.az/i-kt/azerbaycan-sosial-sebekelerle-danisiqlara-baslayib/.

54 "Idea of Licensing Skype, Facebook, and WhatsApp in Azerbaijan Unfounded," *Contact*, August 8, 2015, http://contact.az/search/document.php?id=62574&vr=en#.

55 "The secret of the new regulation over social platforms finally evealed," *Bizimyol*, August 28, 2015, http://www.bizimyol.info/news/59832.html.

Minister of Youth and Sport in relation to his website's critical coverage of the European Games.[56] Freelance journalists reporting for Meydan TV from within Azerbaijan have also faced harassment by authorities. In September 2015, Meydan TV reporters Izolda Aghayeva, Natiq Javadli, and Javid Abdullayev were questioned by the Serious Crimes Investigation Department of the General Prosecutor's Office egarding their coverage of protests in Mingachevir the previous month. However, the majority of the questioning concerned the activities of Meydan TV.[57]

In August, 2015, Rasim Aliyev, a freelance reporter and chairman of the Institute of Reporters' Freedom and Safety, died from internal bleeding after being attacked by the relatives of a soccer player, Javid Huseynov, who Aliyev had criticized on Facebook. Though Aliyev had reported threats he had been receiving online to authorities prior to the attack, no measures were taken to protect him[58]. Huseynov was found guilty of the murder; however, he was released from prison in October 2016.

Independent journalists and activists are often the targets of intimidation campaigns involving the use of illicitly obtained intimate footage and images, as was famously the case with investigative journalist, Khadija Ismayilova.[59] In June 2016, Arastun Orujlu, an employee of the Ministry of National Security claimed that the former Minister of National Security was in possession of over 2500 sex videos depicting Azerbaijani men and women.[60]

Technical Attacks

A number of opposition news websites continue to be subject to cyberattacks, resulting in temporary shutdowns. These include the news websites *Yeni Musavat*, *Azadliq* and the Radio Free Europe/Radio Liberty local service, Azadliq Radiosu. The majority of attacks occur during politically sensitive events, such as elections. As a result, opposition papers subject to attack have speculated that the cyberattacks were launched by the Ministry of Defense. The ministry, however, denies these allegations.

The website Islamazeri.az reported experiencing cyberattacks in November and December 2015, coinciding with the clashes in Nardaran. The website reported that the cyberattacks stopped after they complained to the Ministry of National Security. However, the website was subsequently blocked (see Blocking and Filtering).[61] In January 2016, the website's Facebook page, which has 17,000 followers, was hacked and provocative material was posted on the page by the hackers.[62] On February 1, 2016, *Cenub News* said it was facing cyberattacks, making its content inaccessible for some days before access was restored. That site was also subject to blocking (see Blocking and Filtering). The website had been blocked previously a month prior to this incident and continued operating through a new IP address and server. Five days later, Delta Telecom blocked this new IP as well.

56 "Support independent media in Azerbaijan," *Washington* Post, August 20, 2015, http://wapo.st/1E9NeXj.

57 "The main issue was Meydan TV, Mingachevir was an excuse," *Meydan* TV, September 3, 2015, https://www.meydan.tv/en/site/society/7880/.

58 "Murky circumstances of sportwriter Rasim Aliyev's death yet again shame Azerbaijan," August 16, 2015, *The Independent*, http://www.independent.co.uk/sport/football/news-and-comment/murky-circumstances-of-sportswriter-rasim-aliyevs-murder-yet-again-shame-azerbaijan-10458456.html.

59 Max Fisher "Intimate videos emerge, again, of reporter investigating Azerbaijan president's family," *The Washington Post*, August 7, 2013, http://wapo.st/2e9234W.

60 "hazirda Eldar Mahmudov kimlerse terefinden hima e olunur" [Someone is protecting Eldar Mahmudov at the moment], *Xeber Info*, June 21, 2016, http://xeberinfo.com/24243-hazirda-eldar-mahmudov-kimlerse-terefinden-hima_e-olunur.html.

61 "Islamazeri statement," *Islam Azeri*, January 28, 2016, http://islamazeri.az/islamazeriaz-muraciet-yaydi--30597.html

62 "Islamazeri statement," *Islam Azeri*, January 28, 2016, http://islamazeri.az/islamazeriaz-muraciet-yaydi--30597.html

In December 2015, Azerbaijan's Parliament reported cyberattacks on the parliament's website, claiming that Armenian hackers were responsible. Additionally, the Ministry of Labor and Social Protection Services and the Ministry of Emergency Situations reported cyberattacks on its websites during the same month.[63]

On a state level, protection of Azerbaijan Internet from cyberattacks is monitored by the Computer Emergency Response Team (CERT) which was set up in 2010 and functions under the Special Security Service's Special Communication and Information Security State Agency.[64] On December 10, 2014, AzNet announced that the American company Arbor Networks – a security solutions provider for network operators and large corporations—would provide network protection for AzNet due to ongoing attacks and, more recently, distributed denial-of-service (DDoS) attacks of 85 Gbps capacity on the network of mobile operators in Azerbaijan. DeltaTelecom also announced its decision to sign up for an additional protection against DDoS attacks.

63 "New threats to Azerbaijan's security," *ANS*, December 29, 2015, http://www.anspress.com/siyaset/29-12-2015/azerbaycanin-tehlukesizliyine-yeni-tehdid.

64 "In Azerbaijan cyberattacks originate from the countries with most developed internet infrastructure," *Trend*, April 9, 2014, http://az.trend.az/business/it/2261138.html.

Freedom House

Bahrain

	2015	2016
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	11	10
Limits on Content (0-35)	27	27
Violations of User Rights (0-40)	34	34
TOTAL* (0-100)	72	71

* 0=most free, 100=least free

Population:	**1.38 million**
Internet Penetration 2015 (ITU):	**93 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- Messaging app Telegram was blocked for several days in February in an effort to contain protests marking the fi th anniversary of Bahrain's "Day of Rage" (see **Restrictions on Connectivity**).
- 2Connect, a small mobile and internet service provider, had its licensed revoked by the regulator for failing to provide security agencies with a tool to access users' data (see **Regulatory Bodies**).
- Canadian company Netsweeper won a Bahraini government tender to implement a nationwide fil ering system in a move that will boost the sophistication of internet censorship (see **Blocking and Filtering**).
- Five users were sentenced one to fi e years in prison for tweets that were critical of Saudi Arabia, including outrage over the Saudi-led airstrike campaign in Yemen, the death of hundreds of pilgrims at the 2015 hajj, and the execution of prominent Shiite cleric Nimr al-Nimr. Numerous others were prosecuted for insulting Bahraini public official (see **Prosecutions and Detentions for Online Activities**).

Introduction

Bahraini internet freedom improved slightly in 2015-16 due to greater internet access, although the country remains "Not Free" amid tight censorship and a plethora of prosecutions for criticizing parliamentarians.

Internet access rapidly expanded in Bahrain, currently one of the most connected countries in the world. This year was marked by a number of significan decisions by the Telecommunications Regulatory Authority (TRA). The TRA bent to popular pressure and ordered mobile providers to reverse restrictions on Voice-over-IP (VoIP) in October 2015. However, providers seem likely to alter their service agreements in the future, making customers pay a surcharge for VoIP calls in a bid to increase revenue. Although the major internet service providers (ISPs) tend to comply with requests from security agencies, the TRA revoked a license from a small ISP for failing to provide sufficien monitoring capabilities. The TRA also implemented greater restrictions on the purchase of SIM cards in the name of counterterrorism, limiting the ability of Bahrainis to use ICTs anonymously.

Meanwhile, the government moved forward with plans to implement a nationwide fil ering solution. A tender was won by Netsweeper; the Canadian company was reportedly the only one to submit a bid. The move will likely boost the authorities' ability to monitor and censor banned content, which includes controversial views on the monarchy, religion, and foreign affairs. Ironically, the government minister in charge of the Information Affairs Authority (IAA), which is responsible for monitoring online content, was dismissed from his post over a photo he shared on WhatsApp.

Tensions between the ruling Sunni monarchy and majority Shiite citizenry spill over into the online domain, particularly surrounding the regime's close ties to Saudi Arabia. Three users were sentenced to fi e years in prison for the crime of spreading false news during wartime in tweets related to the Saudi-led bombing campaign in Yemen, to which Bahrain has contributed. Other users have been imprisoned for "insulting a brotherly nation" due to criticism of the Saudis' poor crowd management at the 2015 hajj that led to the death of hundreds—some say thousands—of pilgrims, or outrage over the Saudis' execution of prominent Shiite cleric Nimr al-Nimr. Nonetheless, many Bahrainis continue to look to the internet as an outlet for expressing political, economic, and social frustrations in the country. Amid widespread criticism of politicians, some parliamentarians have even threatened to stop working unless authorities take stricter action against public sector employees said to have insulted them or members of the Gulf Cooperation Council (GCC).[1]

Obstacles to Access

From a technological perspective, Bahrain is one of the most highly connected countries in the world. Competitive broadband prices have led to high levels of mobile internet penetration. Moreover, Bahrain's telecommunications regulator pushed back against an attempt by mobile providers to restrict VoIP, although payment for the use of VoIP may still follow in the future. 2Connect, one of Bahrain's

1 "MPs to the government: either strict procedures against staff electronic abuses or start non-cooperation," [in Arabic] *al-Watan News*, April 23, 2016, http://www.alwatannews.net/NewsViewer.aspx?ID=120683

smaller ISPs, had its license revoked for failing to provide security agencies with a means of monitoring its network.

Availability and Ease of Access

In 2015, Bahrain ranked fi st in the Arab region in the International Telecommunication Union's (ITU) Information and Communications Technology Development Index (IDI) and one of the ten countries that have seen the most dynamic improvements in IDI ranking over the past fi e years.[2] Internet access is widely available in schools, universities, shopping malls, and coffee shops, where Bahrainis often gather for work and study. Language is not an issue, with adult literacy at nearly 95 percent. Bahrainis also possess a high level of English language proficienc , and many ICT applications are available in Arabic.[3] The government provides free computer training programs, which have served 15,000 citizens as of November 2015.[4] The number of internet users has risen rapidly, from a penetration rate of 55 percent in 2010 to 93 percent in 2015.[5] Bahrain also has one of the highest mobile phone penetration rates in the region at 188 percent as of the fi st quarter of 2016, representing over 2.6 million subscribers.[6]

As of the fi st quarter of 2016 there were approximately 2 million broadband subscriptions in the country, of which 89 percent were mobile broadband.[7] Dial-up connections disappeared in 2010, and ADSL use has declined with the growth of mobile broadband. 4G LTE has been available since September 2013. Prices for mobile broadband are among the lowest in the region,[8] where a subscription for 10GB of data on a 4G LTE network is available for USD 21 monthly.[9] Bahrain's fi ed-broadband prices of 2 percent of average monthly income per capita are well below the international affordability target of 5 percent.[10] Speeds have also increased, as the portion of subscribers with speeds of 10Mbit/s or above grew from 2013 to 2014, according to a 2016 report by Bahrain's regulator.[11]

Restrictions on Connectivity

Although there is no centralized internet backbone in Bahrain, all ISPs are indirectly controlled by the government through orders from the Telecommunications Regulation Authority (TRA). This tight control over the country's ICT sector has allowed the Bahraini authorities to impose restrictions on connectivity. For example, in years past the authorities have occasionally throttled internet speeds around certain events, such as the anniversary of the February 14 protests. While no incidents were seen during the coverage period, there were indications the authorities imposed an internet curfew

2 International Telecommunication Union (ITU), *ITU releases annual global ICT data and ICT Development Index country rankings*, 2015 https://goo.gl/doJ1Ic.

3 International Telecommunication Union (ITU), *Measuring The Information Society*, 2014 http://bit.ly/1xrVMi8.

4 Bahrain e-government, "Qudurat Training Program", accessed July 31, 2015, http://bit.ly/1IQ1YMI and "E-government: we trained 15 thousand citizens on computers," [in Arabic] *Alwasat*, November 30, 2015, http://www.alwasatnews.com/news/1051215.html.

5 ITU, "Percentage of Individuals using the Internet," 2016, accessed August 14, 2016 http://goo.gl/Fpr41z.

6 Telecommunications Regulatory Authority (TRA), *Telecommunications Market Indicators in the Kingdom of Bahrain* (Manama: TRA, Q1 2016), slide 4 http://goo.gl/riX1l0 .

7 TRA, *Telecommunications Market Indicators in the Kingdom of Bahrain* (Manama: TRA, Q1 2016), slide 6 http://goo.gl/riX1l0 .

8 TRA, *Telecommunications Markets Indicators in the Kingdom of Bahrain, February 2016* http://goo.gl/UQulYz .

9 Batelco, "Mobile Internet Packages," accessed August 14, 2016 http://batelco.com/internet/mobile/packages/ .

10 TRA, "Bahrain compared well with developed countries in the telecom prices", December 28, 2015, http://bit.ly/1PyGTWT.

11 TRA, *Telecommunications Market Indicators in the Kingdom of Bahrain,* February 2016, slide 30 http://goo.gl/XfzgpZ .

in the town of Diraz by disabling mobile data services and disrupting fi ed-line connections in a bid to disrupt protests over the summer of 2016.[12]

Bahrain's three mobile operators simultaneously blocked Voice-over-IP (VoIP) services in October 2015.[13] The three operators moved to impose an additional US$13 subscriber charge for access to VoIP services offered by the likes of WhatsApp and Skype. After public uproar on social media, the TRA sent an emergency order noting the operators had failed to obtain the regulator's prior approval for the change in terms of service.[14] Providers complied within 48 hours and access to VoIP was restored. However, operators now publically promote VoIP as a free service with a note that it is subject to change at the operators' discretion, meaning additional charges may be written into future contracts and agreements with customers.[15]

ICT Market

Batelco, Zain, and VIVA are the three mobile phone operators in the country, and also serve as its main fi ed-line internet services providers (ISPs), along with Menatelecom, the fourth largest ISP. The government has a controlling stake in Batelco, the largest of these, while other ISPs are owned by investors from the private sector, including non-Bahraini investors.

Regulatory Bodies

Mobile phone services and ISPs are regulated by the Telecommunications Regulation Authority (TRA) under the 2002 Telecommunications Law. The TRA is responsible for licensing telecommunication providers and for developing "a competition led market for the provision of innovative communications services, available to all."[16] Although the TRA is theoretically an independent organization, in practice its members are appointed by the government and its chairman reports to the Minister of State for Telecommunications. Until June 2013, this minister also occupied the post of President of the Information Affairs Authority (IAA).[17] The IAA, which replaced the Ministry of Information in 2010, oversees both traditional and online media outlets in Bahrain and is responsible for decisions to block websites, which are then enforced by internet service providers (ISPs).

There have been no reported instances of ISPs being denied registration permits. Indeed, over 31 licenses have been granted since 2003, with 11 providers currently in business.[18] However, in early 2015 the TRA revoked the licenses of 14 small ICT companies, including some that voluntarily requested their cancellation. According to observers, the majority of these companies were offering international calling services that were adversely impacted by the growing use of VoIP applications,

12 Press Release, "New Investigation Finds Bahrain ISPs Imposing "Internet Curfew" in Protest Area," Bahrain Watch, August 4, 2016, https://bahrainwatch.org/blog/2016/08/04/press-release-bahraini-isps-impose-internet-curfew-in-protest-village/, and Faten Bushehri, "Ongoing Internet Curfew in Duraz for more than 100 Days," Bahrain Watch, October 7, 2016, https://bahrainwatch.org/blog/2016/10/07/100-days-since-internet-shutdown-in-duraz/.

13 Ahmed Ardah, accessed August 14, 2016 https://twitter.com/ArdahAhmad/status/657176883558260736.

14 TRA, "TRA issues an Emergency Order to three mobile operators," October 22, 2015, http://bit.ly/2btjnR2.

15 VIVA, "Free social for all with VIVA Unlimited Plans", accessed August 14, 2016, http://bit.ly/2bZCov5.

16 TRA, "Vision & Mission," accessed March 30, 2014, http://tra.org.bh/en/about-us/vision-mission.html.

17 In June 2013, Mohamed al-Rumaihi was named President of the IAA, replacing Fawaz al-Khalifa who remained Minister of State for Telecom.

18 TRA, *Telecommunications Market Indicators in the Kingdom of Bahrain,* slide 6 http://goo.gl/UQulYz .

leading many to bankruptcy.[19] While the official reason for the license cancellations was not made public, TRA mentioned that the order was in accordance with Article 35 of the Telecommunications Law,[20] which permits license revocation in cases of "material breach of any provision of this Law" or "serious indications or evidence that a Licensee is likely to commit such breach," and if the licensee failed to comply with TRA's directions.[21] The head of TRA said that the number of small companies in the telecommunication market would be reduced by 50 percent.[22]

In February 2016, the TRA issued a warning to the small mobile and fixed-line provider 2Connect for, among other things, "failing to provide a lawful access capability plan"[23] which would allow security units to access users' metadata sent over its network.[24] 2Connect was given seven days to comply and ordered to pay a fine of over US$4.5 million. After it failed to comply, TRA revoked 2Connect's license as of February 25, 2016,[25] and instituted a grace period up until the end of June 2016 to move all of its clients to other providers.[26]

Limits on Content

The level and sophistication of censorship remained stable over the past year, though the government plans to implement a national website filtering solution and a national search engine. Meanwhile, the government continued its efforts to silence online dissidents by forcing them to close their pages or remove content. Self-censorship is rife, particularly on issues related to the monarchy, religion, and relations with the neighboring countries of the Arabian Peninsula. Despite these limitations, many still turn to the internet to collect independent information and to call attention to gross human rights violations.

Blocking and Filtering

The Bahraini government engages in extensive blocking of online content. Multiple state organizations, including the IAA, the Ministry of Interior, and the Ministry of State for Telecommunication, can order the blocking of a website without a court order. The IAA blocks websites that violate Articles 19 and 20 of the country's Press Rules and Regulations, which include material judged as "instigating hatred of the political regime, encroaching on the state's official religion, breaching ethics, encroaching on religions and jeopardizing public peace or raising issues whose publication is prohibited by the provisions of this law."[27] Thus, any site that criticizes the government, the ruling family,

19 "Telecommunications companies licenses reduced in Bahrain by 63 percent," [in Arabic] *Alayam Newspaper*, February 19, 2015 http://bit.ly/1UeM406.

20 TRA, "Revocation of Hawar Telecommunications Co. W.L.L's ISL License awarded by the Telecommunications Regulatory Authority," press release, February 15, 2015, http://bit.ly/1VT0ftv.

21 The Telecommunications Law Of The Kingdom Of Bahrain, Legislative Decree 48, October 23, 2002, http://bit.ly/1w4edPb.

22 "Telecommunications companies tend to merging to continue in the Bahraini market," [in Arabic] *Alwasat*, December 18, 2014, http://bit.ly/1Vzuip2.

23 TRA, Article 35 Order No.2 of 2016 2Connect's breach of Article 24(b), 53 and 78 of the Telecommunications Law, February 4, 2016, http://bit.ly/2bldqnG.

24 TRA, Lawful Access Regulation, accessed August 14, 2016, http://bit.ly/2b5Xyb3.

25 TRA, "Revocation of telecommunication licenses granted by the Telecommunications Regulatory Authority," press release, February 25, 2016, http://goo.gl/ZRgbnY.

26 TRA, "Extension granted by Telecommunications Regulatory Authority to 2Connect W.L.L for providing telecommunication services," press release, April 7, 2016, http://goo.gl/d01mLS.

27 Decree—by—Law No. 47 Regarding organizing the press, printing and publishing, October 23, 2002, http://bit.ly/2blcAaB.

or the country's status quo is subject to blocking by the IAA. Authorities ramped up censorship after the 2011 protests, in which online media played a decisive role.

YouTube, Facebook, Twitter, and international blog-hosting services are freely available. However, other applications are permanently blocked, and specifi content on social networks can be inaccessible. The messaging service Telegram was blocked for several days around the fi th anniversary of the February 14, 2011 popular protests.[28] Further restrictions on the service were noted after the coverage period. Several livestreaming services are blocked,[29] such as PalTalk and Matam.tv, respectively used by Bahrainis to conduct political seminars[30] or broadcast Shiite religious ceremonies.[31] However, the livestreaming service Periscope is available.

According to estimates from several years ago, the IAA has blocked or shut down at least 1,000 websites, including human rights websites, blogs, online forums, and individual pages from social media networks.[32] A crowdsourced list of 367 blocked websites reported as of February 2016 that 39 percent of blocked sites were related to politics, while 23 percent related to the use of various internet tools, such as anonymizers and web proxies.[33]

A report from November 2015 indicated that more than 85 percent of Bahraini websites are hosted outside of the country,[34] despite its excellent telecom infrastructure. Websites hosted overseas are less liable to being removed by local hosting providers in compliance of government orders. While they may still be blocked, these websites are accessible to Bahraini users via circumvention tools. Bahrain Online, a prominent online forum, has been blocked since its launch in 1998.[35] The Arabic web portal and blog-hosting service Al-Bawaba has also been blocked since 2006. The websites of the Arab Network for Human Rights Information (ANHRI) and the Bahrain Center for Human Rights (BCHR) have been blocked since 2006. In November 2013, following a campaign by the BCHR to expose official and royal family members involved in human rights violations, an alternative link to the center's website was blocked as well.[36] The popular Bahraini online news website *Bahrain Mirror* has been blocked since its launch in 2011. According to the website's administration, the government has blocked more than six alternate addresses since then.

In August 2013, the communications minister ordered ISPs to block 70 websites[37] that were suppos-

28 "Telegram stop working in Bahrain ... No clarificatio from TRA," [in Arabic] *Alwasat*, February 11, 2016 http://bit.ly/2btlmoE and User complaints over twitter, screenshot, February 14, 2016 https://goo.gl/0nDoPx.

29 These sites include bambuser.com, ustream.tv, and other websites that stream directly to Twitter like twitcasting.tv, see, *Bahrain Freedom Index* (blog), http://bit.ly/2b8aYNJ.

30 Reporters Without Borders, "Crackdown continues in Bahrain, Bloggers go on trial in Emirates," June 16, 2011, http://bit.ly/1OUSoae.

31 BCHR, "Bahrain: The "Cyber Safety Directorate" Monitors Internet Activity In Style Similar to Big Brother," November 25, 2013, http://bit.ly/1FleBho.

32 Reporters Without Borders, "Bahrain," in *Countries Under Surveillance*, 2011, accessed July 16, 2012, http://bit.ly/1Jf0EfV.

33 "At a Glance: Bahrain," Herdict, accessed on February 22, 2015, http://www.herdict.org/explore/indepth?fc=BH.

34 Ahmed AlDosari, "Bahraini websites migrate from their homeland ... Will they come back one day?," [in Arabic] (blog), November 21, 2015, http://bit.ly/2bSztUN.

35 Ben Birnbaum, "Bahrain continues crackdown on Shi'ite opposition," *The Washington Times*, September 14, 2010, http://bit.ly/1JQCXLs.
"WebStatsDomian - Mail.bahrainonline.org," WebStatsDomain, accessed March 19, 2013, http://bit.ly/1L7Fyla.

36 "Bahrain Center for Human Rights website 2nd link blocked," *Bahrain Freedom Index* (blog), November 2013, http://bit.ly/1N5DWwE.

37 "Blocking a number of websites that promote terrorism, as per the recommendations of the National assembly," [in Arabic] *Bahrain News Agency*, August 3, 2013 http://www.bna.bh/portal/news/573943.

edly "affilia ed with internationally recognized organizations that fund and promote terrorism."[38] The minister also ordered telecom companies to take measures against text messages sent from abroad that promote violence.[39] While some sites affilia ed with Hezbollah, al-Qaeda, and other groups were blocked, others remained accessible as of June 2016, giving a sense that the figh against terrorism is being used as an excuse to censor online content from dissidents.[40]

In a new development in January 2016, the TRA awarded a US$1.2 million tender for a "national website fil ering solution" to Netsweeper, a Canadian company.[41] Netsweeper products can analyze traffi and block access to websites against customized fil ers.[42] The system had yet to be implemented by the end of this report's coverage period. Websites are currently fil ered based on keyword density, the manual entry of URLs, and certain website categories. An updated list of blocked websites is regularly sent to ISPs, which are instructed to "prohibit any means that allow access to sites blocked by the ministry."[43] Through IAA notification the TRA can revoke the license of any operator that does not cooperate with IAA blocking orders.[44]

The decision-making process and government policies behind the blocking of websites are not transparent. The list of all blocked websites is not available to the public. In addition, webmasters do not receive notification or explanations when their websites are banned. When trying to access a blocked site, users are presented with the message, "This web site has been blocked for violating regulations and laws of Kingdom of Bahrain," with no particular laws specified Although the law does technically allow affected individuals to appeal a block within 15 days, no such case has yet been adjudicated.

Content Removal

News outlets continue to face pressure to remove content. In August 2015, *al-Watan* newspaper removed an article from its website in which the writer accused the Kuwaiti government of failing to stand by the Gulf Cooperation Council against what she termed the "Iranian lobby," sparking outcry from the Kuwaiti press. It is believed that the removal of the article from the pro-government newspaper was based on a government order.[45]

Online newspapers have been banned from using audio and video reports on their websites since 2010, apart from the state-owned Bna.bh, which broadcasts video from state television.[46] In further development, The IAA warned *al-Wasat* newspaper in January 7, 2016 to immediately stop upload-

38 "Ministry of State for Communications To Regulate Websites Linked to Internationally Recognized Terrorist Organizations," *Bahrain News Agency,* August 3, 2013 http://www.bna.bh/portal/en/news/573944.

39 Manama,"Bahrain telecoms told to block online terror forums", *Trade Arabia*, August 14, 2013, http://bit.ly/1eJSp3D.

40 The websites affilia ed with ISIS remain accessible as of Jun 2016, see, *Bahrain Freedom Index* (blog), http://bit.ly/2bx0wVm .

41 Bahrain Tender Board, "Awarded Tenders Monthly Report From 1/1/2016 to 1/31/2016," page 5, [in Arabic] http://goo.gl/ilUJIF.

42 "Canadian Company Netsweeper to Censor Bahrain's Internet for $1.2M," *Motherboard,* January 8, 2016, http://bit.ly/1OXEAjl.

43 Reporters Without Borders, "Authorities Step Up Offensive Against Journalists and Websites," May 14, 2009, http://bit.ly/1hDJh2l.

44 Reporters Without Borders, "Authorities Step Up Offensive Against Journalists and Websites."

45 "Al-Watan newspaper deletes an article in which Sawsan AlShaaer had offended Kuwait," [in Arabic] *Bahrain Mirror*, August 18, 2015 http://bit.ly/2bFagdu.

46 BCHR, "Ban on audio programs on daily newspaper Al-Wasat's website," September 9, 2010, http://www.bahrainrights.org/en/node/3327.

ing videos to YouTube and embedding third-party YouTube videos on its website. The IAA claimed *al-Wasat*'s license does not include the ability to publish videos, while some noted the press law 47/2002 does include "video and audio products" as part of the definitio of publications.[47] By the end of the coverage period, the newspaper had removed the video section from its website and appealed the IAA's decision.

Website administrators face the same libel laws that apply to print journalists and are held jointly responsible for all content posted on their sites or chat rooms. In February 2016, the interior ministry stated that WhatsApp group administrators are also liable for the spread of false news in their groups, if they fail to report the incidents.[48] News emerged in April 2015 of plans to create a Bahraini national search engine with the help of Russian technology experts, based on Russia's "Sputnik" search engine. This could enable the Bahraini authorities to easily remove unwanted search results without the need to secure cooperation from U.S.-based search engine companies, such as Google.[49]

Authorities also use extralegal measures to forcibly remove online content. Through the use of arrests,[50] detentions, and torture,[51] security forces coerced many online forum moderators into permanently shutting down their websites.[52] "Bawabat al-Bahrain" (Bahrain Gateway), an online discussion forum site that was supporting progovernment views, was closed by its owner in July 2015[53] after he was put on trial for a Twitter post (See Prosecutions and Arrests for Online Activities).

Media, Diversity, and Content Manipulation

The authorities are known to manipulate online content in order to fabricate greater public support for government policies. According to the watchdog group, Bahrain Watch, the government has hired 18 public relations (PR) fi ms for promotional campaigns since February 2011, representing at least US$32 million in contracts.[54] At least one PR agency was contracted to provide "web optimization and blogging" services,[55] while others were hired for online reputation management.[56] In October 2014, one of these PR companies tried to force *The Huffington Post* not to write on the United Kingdom's investigation of torture allegations against the Bahraini king's son.[57] Meanwhile, hoax

47 "IAA prevents Alwasat from using "Video" and YouTube," [in Arabic] *Alwasat*, January 25, 2016, http://www.alwasatnews.com/news/1072283.html.

48 "Interior Ministry: Group Admin in Bahrain, is responsible to the authorities for everything published," [in Arabic] Lualua TV, February 19, 2016, http://lualuatv.com/?p=33529.

49 "Russia could help Bahrain in establishing a national search engine", *UNLOCKPWD*, July 30, 2015, http://bit.ly/1LNLSRJ.

50 Non exhaustive list of forum moderators who were subject to arrest found at: http://bit.ly/1He9SYQ; accessed via: BCHR, "Bahrain: After destruction of the actual protesting site at "the Pearl," the government shifts to eliminate virtual protests," May 17, 2011, http://bit.ly/1LmOd7Y.

51 Mona Kareem, "Bahrain: Twitter User Jailed for 66 Days for Tweeting," *Global Voices*, December 5, 2011 http://bit.ly/1JXimWe.

52 Moderator of the AlDair Forum talks about his detention, saying he was forced to show the interrogation office how to close the website: "Ahmed al-Dairi Moderator of AlDair Forums in the fi st episode of his testimony: thus eased voice of Zakaria AlAsheeri forever," [in Arabic] *Bahrain Mirror*, January 4, 2012, http://bahrainmirror.com/article.php?id=2678&cid=117.

53 Bahrain Gateway farewell tweet, accessed August 14, 2016, https://twitter.com/b4bhcom/status/622400160346341376.

54 Bahrain Watch, "PR Watch – keeping an eye on the Kingdom's PR," http://bahrainwatch.org/pr/.

55 "Trippi & Associates Manipulate Internet Content on Behalf of Bahrain Government," *Bahrain Freedom Index* (blog), July 20, 2011, http://bit.ly/1L7nCqT.

56 Marcus Baram, "Lobbyists Jump Ship in Wake of Mideast Unrest," *Huffington Post*, March 25, 2011, http://huff.to/1ePbiwQ.

57 James Dorsey, "Bahrain rattled by UK court's opening of door to investigation of torture allegations," *The World Post,* October 21, 2014, http://huff.to/10vInwO.

journalists[58] spread propaganda on Twitter and progovernment blogs such as *Bahrain Views* and *Bahrain Independent*.[59]

Similarly, an "army of trolls" has been active on Twitter since February 2011,[60] when hundreds of accounts suddenly emerged to collectively harass and intimidate online activists,[61] commentators, and journalists who voiced support for protests and human rights.[62] The government trolls have been moderately effective in silencing or reducing the activity of opposition voices both inside Bahrain[63] and abroad.[64] The trolls have also played a vital role in spreading information that is controversial, offensive, or false,[65] in order to distort the image of protesters, spread hate and conflict or discredit information posted on social networks.[66] These troll accounts usually have few followers (or sometimes none at all) and tend to appear and disappear in coordination with one another. In September 2015, trolls hijacked a hashtag dedicated to a launch event of a book on the Bahraini uprising.[67]

In August 2013, Bahrain Watch revealed evidence of connections between the Bahraini government and "extremist" accounts on Twitter and Facebook that advocated violence against both the government and protesters.[68] It was also revealed that the government impersonates opposition figu es on social media in order to send malicious links, such as IP trackers, to anonymous government critics that can be used to identify and prosecute them.[69]

The state also issues officia statements warning against the discussion of certain subjects. On January 3, 2016 the interior ministry threatened to take actions against any insult or "negative discussion" of the Saudi executions of Sheikh Nimr al-Nimr and 42 other men.[70] On March 26, 2015, the interior ministry also issued a statement warning it would take steps against anyone expressing opinions "against the approach that Bahrain has taken" in supporting and joining the Saudi-led coalition conducting airstrikes in Yemen[71] (see Prosecutions and Detentions for Online Activities). This is on top

58 Mona Kareem, "Bahrain: Liliane Khalil, Another Blog Hoax or Propaganda?," *Global Voices,* August 5, 2011, http://bit.ly/1JDPViI.

59 "The hunt for #lilianekhalil," YouTube video, 10:25, *The Stream* (blog), *Al Jazeera,* http://bit.ly/1V0eKZf; Justin Gengler, "Media Jihad: If Ya Can't Beat 'Em, Sue 'Em!", Religion and Politics in Bahrain, June 15, 2011 http://bit.ly/1IQaWtf; Dr Majeed AL Alawi, Twitter post, January 2, 2012, 2:51am, http://bit.ly/1fSHvJW.

60 Bob Hooker, "Bahrain's Troll Army," *Web 3.0 Lab* (blog), February 17, 2011, http://bit.ly/1W8HJN3.

61 See Brian Dooley, "No Stamp Required: All Too Easy for #Bahrain Twitter Trolls," Huffing on Post, September 25, 2015 http://huff.to/1WmSueM, and Brian Dooley, "'Troll' Attacks on #Bahrain Tweets Show Depth of Government Attempts to Silence Dissent," *The World Post,* November 17, 2011, http://huff.to/1iVmxf9.

62 J. David Goodman, "'Twitter Trolls' Haunt Discussions of Bahrain Online," *The Lede* (blog), *The New York Times*, October 11, 2011, http://nyti.ms/1NBl3Sv.

63 iManamaa, Twitter post, May 13, 2011, 7:39am, http://bit.ly/1iCuvtJ; Sultan al-Qassemi, "Pioneer Bloggers in the Gulf Arab States," *Jadaliyya*, December 20, 2011,http://bit.ly/1k4jzR5; Bob Hooker, "Disturbing Drop in Tweeting in Bahrain," *Web 3.0 Lab* (blog), March 22, 2011, http://bit.ly/1OcDDik.

64 "Twitter Trolling as Propaganda Tactic: Bahrain and Syria," *Jillian C. York* (blog), December 10, 2011, http://bit.ly/1hXiMFN.

65 "So Many Trolls but so Few Leaders: The Information War in Bahrain," *Marc Owen Jones* March 14, 2011, http://bit.ly/1P8SNpf.

66 David Wheeler, "In the Arab Spring's Wake, Twitter Trolls and Facebook Spies," *The Chronicle of Higher Education* (blog), November 29, 2011, http://bit.ly/1Kx8zdJ.

67 "Trolls Attempt to Hijack #BahrainUprising Twitter Event," *Marc Owen Jones* (blog), September 18, 2015 http://bit.ly/2btmsk6.

68 Bill Marczak, "Is Bahrain's Government running extremist accounts?" Bahrain Watch, August 5, 2013, http://bit.ly/1UpiYil.

69 Bill Marczak, "Bahrain Govt using fake Twitter accounts to track online critics," Bahrain Watch, press release, July 31, 2013, http://bit.ly/1hXjfrJ.

70 "Ministry of Interior (MOI): legal actions against any misuse or abuse on the implementation of the Saudi judicial rulings," [in Arabic] *Alwasat*, January 3, 2016, http://www.alwasatnews.com/news/1063913.html.

71 "MOI warns against division, sedition," March 26, 2015, *Bahrain News Agency*, http://www.bna.bh/portal/en/news/660794.

of regular warnings disseminated in the press, on television, and on the radio that there will be legal action taken against those who "misuse social media."[72]

Similarly, authorities have urged progovernment users to post about certain topics, sometimes with unintended consequences. In July 2015, Bahrain's interior minister started a media campaign against Iranian interference in Bahraini affairs, which has turned into a hate speech hashtag against Shiite citizens.[73] In January 2014, the prime minister and the minister of telecommunications held several public meetings with progovernment users to encourage them to "defend Bahrain's ruling system."[74]

Despite these numerous attempts to manipulate the online information landscape, government restrictions on online advertising have not forced the closure of any opposition websites. While it is difficul for blocked websites to secure advertising, popular sites such as *Bahrain Mirror* (390,000 views monthly) have not faced significan financia pressures. This is due to the fact that most Bahraini opposition websites are run with limited and sometimes personal resources. Furthermore, the websites continue to receive large amounts of traffi from users within Bahrain through the use of proxy services, dynamic IP addresses, and virtual private network (VPN) applications. However, the government does regularly block access to circumvention tools, including techniques such as using Google Page Translate, Google cached pages, and online mobile emulators. Adaptive and internet savvy Bahrainis tend to fin ways around these restrictions.

The internet remains the main source of information and news for many Bahrainis, particularly those active on Twitter and Facebook. The number of Bahraini users on Facebook increased to around 700,000 as of December 2015, according to a local source.[75] However, internet users exercise a higher degree of self-censorship, particularly as investigations of users' online activities have been launched at workplaces and universities.[76] On Twitter, online forums, and comment sections, most use pseudonyms due to fear of being targeted by the authorities.[77] Many have modifie their privacy settings on social media or "protected" their Twitter pages from public viewing. Some temporarily stopped tweeting after receiving threats to their personal safety.[78]

Digital Activism

Given restrictions on press freedom, the lack of international media coverage, and the inability of many prominent journalists to enter the country,[79] activists rely on digital tools to bring attention to protests and human rights violations.[80] In July 2015, the BBC reported that 21,000 tweets were post-

72 "MOI: legal action against anyone who abuses the use of social media and raises sectarian strife," [in Arabic] *Alwasat*, June 27, 2015, http://www.alwasatnews.com/news/1003344.html.

73 "Bahrain's Interior Minister Launched Hate Campaign..Sectarian Takfir Discourse Returned Under Hashtag #No_to_Iranian_Intervention," *Bahrain Mirror*, August 22, 2015, http://bahrainmirror.org/news/25858.html.

74 "HRH Premier calls for the need to use social networks to defend the nation," *Bahrain News Agency,* January 14, 2014, http://bit.ly/1L7p6S3.

75 "Two million and 200K accounts in the social networks in Bahrain in 2015," [in Arabic] *Alwasat*, December 15, 2015 http://www.alwasatnews.com/news/1057013.html.

76 Simeon Kerr, "Manama fight back in cyberspace," *Financial Times*, May 23, 2011, http://on.ft.com/maUYxm.

77 Nancy Messieh, "Online anonymity: A gateway to freedom or abuse?" *The Next Web*, August 14, 2011,http://bit.ly/1PNCI8x.

78 "Bahrain doctor @BAHRAINDOCTOR threatened with arrest because of her tweets," *Bahrain Freedom Index* (blog), accessed July 31, 2015, http://bit.ly/1DhPISu.

79 "Access Denied," a project of the independent research and advocacy organization Bahrain Watch, chronicles the many journalists, researchers, academics, and NGO workers that were expelled from or denied access to Bahrain from the 2011 uprising until now. See, http://bahrainwatch.org/access/.

80 Amira al Hussaini, "Bahrain: Tweeting Appalling Conditions at Jaw Prison," *Global Voices*, July 19, 2012, http://bit.ly/1ikgVuE.

ed using the Arabic hashtag #Scholarships_Massacre to express anger about the unfair distribution of scholarships and discrimination against Shiite students.[81] The Arabic hashtag #MassRallies14August trended for several days in August 2015, as users called for antigovernment protesters on the anniversary of the country's independence.[82] That same month, after the minister of interior denied that Shiite Bahrainis are subject to discrimination, Shiite users posted their views under the Arabic hashtag #I_feel_like_a_2nd_class_citizen.[83]

In addition, the "Coalition of February 14 Youth" protest movement continues to use social networks[84] to organize protests and bring international attention to local causes.[85] YouTube videos are uploaded to document police attacks on civilians and torture testimonies,[86] though some are promptly blocked.[87] Relatives or friends of detainees regularly use Twitter to campaign for their release and to provide updates about prison conditions.[88]

Violations of User Rights

Violations of user rights in Bahrain were rampant, with at least 32 users arrested, detained, or prosecuted over the coverage period. Collectively, 447 months of prison sentences were passed down to 10 users, while others remain on trial or in arbitrarily detention. The top reasons for user prosecution during coverage period was criticizing actions taken by Saudi Arabia, criticizing Bahraini members of parliament, and "insulting the king and instigating hatred of the regime." Bahraini law does not contain adequate protections for free speech, given provisions that ban criticism of the royal family, the spreading of false news during war, or insulting foreign nations.

Legal Environment

Bahrain's legal environment presents many obstacles to internet freedom in its current form. According to Article 23 of the Bahraini constitution, freedom of expression is guaranteed, "provided that the fundamental beliefs of Islamic doctrine are not infringed, the unity of the people is not prejudiced, and discord or sectarianism is not aroused."[89] Article 26 states that all written, telephonic, and electronic communications "shall not be censored or their confidentialit be breached except in exigencies specifie by law and in accordance with procedures and under guarantees prescribed by the law."[90] The Press and Publications Law of 2002 promises free access to information "without prejudice to the requirements of national security and defending the homeland." Bahraini journalists have argued that these qualifying statements and loosely-worded clauses allow for arbitrary interpretation

81 "BBC: 21 thousand tweets on Hashtag #Scholarships_Massacre in Bahrain," [in Arabic] *Bahrain Mirror*, July 21, 2015, http://bit.ly/2bbWOwR.

82 Nada Ramadan, "Bahraini opposition head to Twitter to call for protests," *TheNewArab*, August 13, 2015, http://bit.ly/2bFwYSz.

83 "Bahrainis respond to the Minister of Interior on #I_feel_like_a_2nd_class_citizen," [in Arabic] *BahrainMirror*, August 23, 2015, http://bit.ly/2b8t19K.

84 Coalition 14 Feb, Twitter Account, https://twitter.com/COALITION14.

85 Toby C. Jones and Ala'a Shehabi, "Bahrain's revolutionaries," *Foreign Policy*, January 2, 2012, http://atfp.co/1JBnf7R; U.S. Embassy Bahrain, "Demonstration Notice 3 – January 17, 2013," news release, January 17, 2013, http://1.usa.gov/1JDUPMH.

86 BCHR, "Blocking the Documentary 'Systematic Torture in Bahrain' on YouTube," February 8, 2011, http://bit.ly/1NBlaO4.

87 Jillian York, "Bahrain Blocks YouTube Pages and More," *Global Voices Advocacy,* February 14, 2011, http://bit.ly/1OcIEYf.

88 BahrainDetainees, Twitter Account, https://twitter.com/FreedomPrayers/lists/bahraindetainees.

89 Constitution of the Kingdom of Bahrain, art. 23, http://www.shura.bh/en/LegislativeResource/Constitution/Pages/default.aspx.

90 Constitution of the Kingdom of Bahrain, art. 26.

and, in practice, the negation of the many rights they seek to uphold.[91] In addition, there is no law that define clear penalties for violating the privacy of internet users, a concern for many bloggers who believe this allows for abuse.[92]

There were no new laws passed over the coverage period, although there were discussions over new media regulations. In August 2015, the minister of information affairs indicated that a new Press and Publications Law might regulate social media publishing.[93] One month later, the cabinet approved a proposal for new regulations on all outlets providing audio, video, written and electronic news content. Among other restrictions, the new proposal states all outlets must respect the sovereignty of the kingdom of Bahrain, as well as its regime, figu es, and institutions. It also bans broadcasting any information that would lead to disturbing the kingdom's relations with other countries. This regulation complements the existing publications law until a new one is approved.[94]

In September 2013, the cabinet greenlighted new legislation that would criminalize anyone who establishes a website, publishes information online, or uses any information technology tool to assist or aid communications with terror cells or to promote the disruption of public order or morale.[95] As of May 2016, the law had not yet been passed.[96] In August 2014, the prime minister renewed calls to take immediate measures to control the usage of social media and to hold the "abusers" of these networks accountable.[97] This was followed by similar directives from the king to figh the "wrongful use" of social media by legal means.[98] During the past year, similar officia statements were made.

Online censorship and criminal penalties for online speech are currently enforced under the 2002 Press and Publications Law,[99] which does not specificall mention online activities but was extended to mobile phones in 2010.[100] The law allows for prison sentences from six months to fi e years for repeat offenders, for publishing material that criticizes Islam, its followers, or the king, as well as content that instigates violent crimes or the overthrow of the government.[101] In addition, the 2002 Telecommunications Law contains penalties for several online activities, such as the transmission of

91 IREX, "Bahrain," *Media Sustainability Index 2008,* 2009, https://www.irex.org/sites/default/files/MSIMENA08_Bahrain.pd .

92 "Ali al-Moussawi, "On the occasion of the World Day to combat electronic surveillance," [in Arabic] *Al Wasat,* March 12, 2012, http://bit.ly/1Kr62gI.

93 "Alhammadi: No dereliction in dealing with the complaints of the misuse of social media," [in Arabic] *Alwasat*, August 4, 2015, http://www.alwasatnews.com/news/1013575.html.

94 "Cabinet: standards for monitoring of media content," [in Arabic] *Alwasat*, September 22, 2015, http://bit.ly/2bChvBq.

95 "HRH the Prime Minister Chairs the Weekly Cabinet Meeting," *Bahrain News Agency,* September 15, 2013, http://bit.ly/1JQ2RDp.

96 Mohamed Al A'Ali, "Cybercrime law amendment set", *Gulf Daily News,* September 16, 2013, http://bit.ly/1Mhjg3m.

97 "HRH Premier directs to stop exploiting platforms in inciting sectarianism, sedition," *Bahrain News Agency,* August 26, 2014, http://bit.ly/1N5v3mI.

98 "HM the King visits the General Command of the Bahrain Defence Force and directs to take the necessary immediate actions against those who instigated, mall, abused, or harmed the security of the homeland and its stability and national unity," [in Arabic] *Bahrain News Agency,* September 3, 2014, http://www.bna.bh/portal/news/631246.

99 For cases where the authorities have used the 2002 press law to censor online websites, see BCHR, "Website accused of violating press code, BCHR concerned that move is aimed at silencing critical voices," October 1, 2008, http://bahrainrights.org/en/node/2446;
"Closing a blow to freedom of opinion and expression," [in Arabic] *Alwasat,* April 25, 2010,http://bit.ly/1JQ3ahA; "Blocking users 'Twitter' caused by a violation of the Copyright Act," [in Arabic] *Alwasat*, January 3, 2010, http://bit.ly/1JQ3ahA.

100 Habib Toumi, "Bahrain imposes blackout on BlackBerry news sharing," *Habib Toumi* (blog), April 8, 2010, http://bit.ly/1IBqIM4.

101 Press and Publications Law of 2002 of the Kingdom of Bahrain (No.47 of 2002).

messages that are offensive to public policy or morals.[102] However, sentences can be longer if users are tried under the penal code or terrorism laws, especially when it comes to social media cases, where the current press and publication law is not used.[103] For instance, under the penal code, any user who "deliberately disseminates a false statement" that may be damaging to national security or public order may be imprisoned for up to two years.[104] The government has used these vague clauses to interrogate and prosecute several bloggers and online commentators.

Prosecutions and Detentions for Online Activities

Between June 2015 and May 2016, at least 32 online users were arrested, detained or prosecuted for their ICT activities.[105] While many users are still on trial as of May 2016, 447 months of prison sentences were collectively passed down on 10 Bahraini users in cases directly related to online posts during the coverage period. Ten users remained in jail as of the end of May 2016, including three users who were serving sentences from previous years.

Authorities targeted criticism of the Saudi-led coalition's military intervention in Yemen.

- On March 26, 2015, Fadhel Abbas, General Secretary of the Democratic Unity Gathering Society, was arrested shortly after the society released a statement on Twitter condemning the war against Yemen.[106] He was sentenced to fi e years in prison in June 2015 for "spreading false information that could harm the military operations of Bahrain and its allies" in Yemen based on Article 133 of the Bahraini penal code.[107]

- On September 7, 2015, prominent Twitter users Yousif al-Amm (@14kilogramme)[108] and Hussain Khamis (@BuKhamis) were arrested and had their devices confisca ed for "insulting Bahraini soldiers participating in the Saudi Arabia-led Arab Coalition" through their tweets. Both were sentenced to fi e years in prison on February 18, 2016 under Article 133 of the penal code.[109]

Criticism of Saudi Arabia was a frequent motive for arrest in Bahrain.

- Ebrahim Karimi, a Bahraini citizen who was stripped of his nationality in 2012, was sentenced to two years in prison for tweets criticizing Saudi Arabia's management of the Hajj

102 The Telecommunications Law Of The Kingdom Of Bahrain, Legislative Decree 48.

103 "Alhammadi: No dereliction in dealing with the complaints of the misuse of social media," [in Arabic] *Alwasat*, August 4, 2015, http://www.alwasatnews.com/news/1013575.html.

104 Bahrain Penal code, 1976, art. 168, http://bahrainrights.org/BCHR/wp-content/uploads/2010/12/Bahrain-Penal-Code.doc.

105 List of prosecuted online users 2015-2016: http://bit.ly/2bcefvN, accessed via bahrainrights.org.

106 BCHR, "Cease Arrests Over Talks of War and Respect International Humanitarian Law," March 28, 2015, http://bahrainrights.org/en/node/7463.

107 Article 113 of the penal code proscribes a prison term of up to ten years to anyone who "deliberately announces in wartime false or malicious news, statements or rumors or mounts adverse publicity campaigns, so as to cause damage to military preparations for defending the State of Bahrain or military operations of the Armed Forces, to cause people to panic or to weaken the nation's perseverance." BCHR, "BCHR Condemns 5-Year Prison Sentence Against Political Leader Fadhel Abbas," July 3, 2015, http://bahrainrights.org/en/node/7560.

108 Yousif al-Amm (@14kilogramme), also known as "Haji Ahmed," has some 11,000 followers while Hussan Khamis has 24,000 followers.

109 "5 years imprisonment for «Abu Khamis» and «Haji Ahmad» because of «Twitter»," [in Arabic] *Alwasat*, February 19, 2016, http://bit.ly/1XATeNP and "5 years imprisonment for «Haji Ahmad»," [in Arabic] *Alwasat*, February 19, 2016, http://bit.ly/2bF4qI5.

Season in 2015, specificall blaming the authorities for the deaths of hundreds of pilgrims.[110] The tweets were published by the anonymous account "Fareej Karimi,"[111] with which Karimi denied any connection. He had been arrested in September 2015 and charged with misusing telecommunication devices, and "insulting a brotherly country and inciting hatred against the regime" under articles 290, 165 and 215.[112]

- In April 2016, Dr. Saeed al-Samaheeji, who tweets under his real name, was sentenced to one year in prison for "misusing electronic networks to insult a sister nation and inciting unpermitted demonstrations which had led to demonstrations accompanied by violent acts" under article 168 and 215 of the penal code.[113] He had been arrested during a house raid at dawn after criticizing Saudi Arabia for executing Sheikh Nimr al-Nimr and dozens of others in January 2016. Al-Samaheeji's tweets coincided with public protests against the executions, although any link was tenuous.

In July 2015, at least four social media users were arrested for "insulting" or "defaming" Bahraini members of parliament (MPs) after the approval of the state budget for 2015 and 2016, which contained a yearly defici of around US$4 billion, as well as cuts to some subsidies.[114] Several new complaints were file with the public prosecutor in January 2016 after the parliament approved increases to fuel prices.[115] Eight users were identifie and charged by the Electronic Crimes General Directorate,[116] resulting so far in one three-month sentence, a fin of US$1,300, and a fin of US$530, the latter for an Instagram post.[117] All are charged under article 216 of the penal code, which specifie that "a person shall be liable for imprisonment or payment of a fin if he offends, by any method of expression, the National Assembly or other constitutional institutions (..)" as well as articles 364, 365, and 366 which proscribe prison sentences of up to two years for defaming a public employee. Finally, the owner of the website "Bawabat al-Bahrain" [Bahrain Gateway] was fine US$265 in November 2015[118] for allegedly defaming a candidate to parliament in a tweet one year earlier.[119] He also shut down his website and social media accounts (See Content Removal).

At least seven users were arrested or sentenced for "instigating hatred of the regime," "insulting the king," or both during the coverage period.

- Jalila al-Sayed Amin and Ali al-Maqabi, respectively detained since January and February

110 Elizabeth Whitman, "Saudi Arabia Hajj Tourism Crisis 2015: After Deadly Stampede, Will Royal Family Improve Security?," *International Business Times*, September 30, 2015, http://bit.ly/1VKyZQC.

111 Fareej Karimi is the unofficia popular name of a neighborhood in Muharraq, Bahrain, inhabited by members of Karimi family.

112 Bahrain Center for Human Rights, "More prison sentences and interrogations for free expression "crimes" in Bahrain such as "insulting the king"," April 7, 2016, http://bahrainrights.org/en/node/7780.

113 Amnesty International, "Urgent Action: Activist detained for protesting on Twitter," January 8, 2016, http://bit.ly/2bF5mMy.

114 BCHR, "Bahrain: Prison Awaits for Internet Criticism of Regime, Ministry or Even Your Elected MP," July 19, 2015, http://bit.ly/1iCyKpk

115 "The Parliament: we raised complaints against users of social networks for bypassing the guaranteed right to freedom of opinion and expression," [in Arabic] *Alwasat*, January 29, 2016, http://www.alwasatnews.com/news/1073667.html

116 "«Prosecution»: The parliament file 61 complaints against the owners of accounts on the social networks," [in Arabic] *Alwasat*, April 25, 2016, http://www.alwasatnews.com/news/1106486.html

117 "200 dinars fin for a young man who insulted the House of Representatives over Instagram," [in Arabic] *Alwasat*, March 22, 2016, http://www.alwasatnews.com/news/1093565.html

118 "The owner of a Web site is fine for defamation and publication that affects the dignity of a candidate for election," [in Arabic] *Alwasat*, November 3, 2015, http://www.alwasatnews.com/news/1041776.html

119 "Trial of defendant accused of defaming a candidate for the parliamentary elections through his website," [in Arabic] *Alwasat*, September 4, 2016, http://www.alwasatnews.com/news/1022613.html

2015, were released in January 2016 but remain on trial for "insulting the king and inciting violence" on Twitter.[120]

- Similarly, 18-year old university student Saeed Al-Singace remained on trial for "inciting hatred of the regime through his phone."[121] He was arrested during a 3am house raid in June 2015, during which authorities confisca ed his electronic devices, and held him until that November.

- On 10 March 2016, Hussain Mahdi, the owner of the satirical Twitter account "@Takrooz," was sentenced in absentia to fi e years imprisonment and a fin of US$26,525 for "insulting the king."[122] He is the fi st to receive such a harsh sentence since the modificatio of Article 214 of the penal code in February 2014.[123] He was detained for 11 months from June 2014 to April 2015, during which he was reportedly tortured; he left the country in mid-2015.[124] Given the popularity over his account which had over 97,000 followers, the harsh sentence was perceived to be a warning message to the rest of Bahrain's online community.

- On 10 April 2016, Habib Jaafar Ahmed, a 45-year-old military office , was arrested and charged by the military prosecution with inciting hatred against the regime and security forces via Twitter and Facebook.[125] He was still on trial as of May 2016.

Prisoners have even been interrogated for tweets emanating from accounts holding their name. In January 2016, Shaikh Ali Salman, leader of the largest political group in Bahrain, who is already imprisoned, was brought from detention to be questioned by the public prosecutor about tweets on "democracy" and "reform" posted by his account @AlwefaGS on Martin Luther King Day. The public prosecutor said the account "incites hatred against the regime, promotes disobedience of the law and calls for holding unauthorized protests." No officia charges were pressed, although an investigation into the account operator was ordered.[126] A few days later, the Twitter account of Salman's wife was hacked (See Technical attacks).[127]

The courts often proscribed more lenient sentences to offenders with links to the government. For instance, the owner of a largely progovernment Twitter account, @mnarfezhom, was put on trial on several defamation charges in 2015, resulting in only small fine as low as US$132[128] or suspended

120 "Release of Jalila Alsayed Amin and Ali Almqabi," [in Arabic] *Alwasat*, January 31, 2016, http://www.alwasatnews.com/news/1074582.html

121 BCHR, "Bahrain: Prison Awaits for Internet Criticism of Regime, Ministry or Even Your Elected MP," July 19, 2015, http://bit.ly/1iCyKpk

122 "5 years imprisonment and a fin of 10 thousand dinars, for the owner of Takrooz account for insulting the king," [in Arabic] *Alwasat*, March 11, 2016, http://www.alwasatnews.com/news/1089115.html

123 Article 214 proscribes "a punishment of imprisonment for a period of no less than one year and no more than seven years and a fin of no less than BD1,000 and no more than BD 10,000 will be inflic ed upon any person who offends in public the Monarch of the Kingdom of Bahrain, the fla or the national emblem." BCHR, "Bahrain King: Up to 7 Years Imprisonment if You Insult Me!," February 9, 2014, http://bahrainrights.org/en/node/6747

124 "Takrooz reveals himself: I am a situation.. I do not let the word choked in my mouth," [in Arabic] *Bahrain Mirror*, March 14, 2016, http://bahrainmirror.org/news/30001.html

125 BCHR, "More arrests and jail sentences in Bahrain over social media posts," June 20, 2016, http://bahrainrights.org/en/node/7919

126 "Bahrain Public Prosecution Orders Investigation into Who's Running Al-Wefaq Leader's Twitter Account," *Bahrain Mirror*, January 25, 2016, http://bahrainmirror.org/news/28974.html

127 "Twitter Account of the wife of Sheikh Ali Salman is hacked," [in Arabic] *Bahrain Mirror*, February 13, 2016, http://bit.ly/2ba15iG

128 "Owner of account "mnarfezhom" fine 50 dinars for defaming lawyer Hashem," [in Arabic] *Alwasat*, February 1, 2016, http://bit.ly/2ba1bHc.

sentences of a few months.[129] The owner of the account is believed to be Mohamed Salman Saqer al-Khalifa, a member of the royal family.[130] The account, which no longer exists, once had some 100,000 followers and criticized certain government policies while maintaining a staunchly progovernment message.

Nabeel Rajab, one of Bahrain's most prominent human rights defenders and most followed Bahraini Twitter user (@NabeelRajab),[131] has been in and out of prison since 2012 for various cases linked to his tweets.[132] He was imprisoned from April 2, 2015 to July 13, 2015 as part of a six-month sentence[133] on charges of insulting public institutions under article 216 of the penal code[134] for a tweet in which he questioned whether Bahraini security institutions are "ideological incubators" for the so-called "Islamic State" terrorist group.[135] He was released that July for health reasons but placed on a travel ban.[136] He still faces up to 10 years on charges of "spreading false news during a time of war" and "insulting a statutory body"[137] for tweets dating from April 2015 about the Saudi-led coalition airstrikes in Yemen and the alleged torture of detainees at Jaw prison.[138] Rajab is the president of the Bahrain Center for Human Rights, a nongovernmental organization that remains active despite a 2004 government order to close it.[139]

In addition, the public prosecutor has begun to use a legal provision that calls for the prosecution of teenagers' parents when their children are arrested for criminal activities, such as "misusing social media."[140]

Every year, a new name is added to a growing list of Bahraini photographers who faced reprisals, often using trumped up charges, for documenting protests and posting their images online:

- In 2013, award-winning photographer Ahmed Humaidan, who was arrested in 2012, was sentenced to 10 years in prison for allegedly participating in an attack on a police station in the district of Sitra,[141] though it is believed he was targeted for photographing protests.[142]

129 "Sentences of mnarfezhom reach up to total one year," [in Arabic] *Alwasat*, May 25, 2016, http://bit.ly/2b8PUv5.

130 "Mohammed AlKhalifa, from an army office to an arms dealer and eventually insulter of chaste women," [in Arabic] *Alfateh News*, October 26, 2012 http://bit.ly/1IaUxfA.

131 Rajab was ranked the "most connected" Twitter user in Bahrain according to a survey, with over 260,000 followers as of May 2015. See: Wamda, *How the Middle East Tweets: Bahrain's Most Connected Report* December 3, 2012, http://bit.ly/1Jf8vdo.

132 Nabeel Rajab was first arrested on May 5, 2012 and held for over three weeks for "insulting a statutory body" in relation to a criticism directed at the Ministry of Interior over Twitter. On June 9, 2012, he was arrested again after tweeting about the unpopularity of the Prime Minister (also a member of the royal family) in the city of Al-Muharraq, following the sheikh's visit there. A group of citizens from the city promptly sued Rajab for libel in a show of obedience to the royal family. On June 28, 2012, he was convicted of charges related to his first arrest and ordered to pay a fine of BHD 300 ($800). Shortly after he was released on bail, he was re-arrested on July 9, 2012 after a court sentenced him to three months imprisonment for the Al-Muharraq incident. The court of appeals later acquitted Rajab, although he had already served most of his sentence. He was kept in prison until May 2014 to serve two-year sentence for "calling for illegal gatherings over social networks."

133 "Bahrain: Nabeel Rajab sentenced for a tweet," *Index on Censorship*, January 20, 2015, http://bit.ly/2b8wRfX.

134 BCHR, "Bahrain: Ongoing detention of leading human rights defender Nabeel Rajab," October 20, 2014, http://bit.ly/1KW9oPw.

135 Nabeel Rajab, Twitter post, September 28, 2014, 3:55 AM, https://twitter.com/NABEELRAJAB/status/516179409720852480.

136 "Bahrain: Continuous travel ban of Mr. Nabeel Rajab, President of the Bahrain Centre for Human Rights (BCHR)," *OMCT*, December 21, 2015, http://bit.ly/1RE084G.

137 Nabeel.Rajab, Instagram post, August 2015, https://instagram.com/p/5aXYEGyGET/ .

138 BCHR, "Nabeel Rajab's case update," May 6, 2015, http://bahrainrights.org/en/node/7517.

139 BCHR, "About BCHR," http://bahrainrights.org/en/about-us.

140 "MOI: arrest of number of those who abused social media," [in Arabic] *Alwasat*, January 4, 2016, http://bit.ly/2b9ULdQ.

141 "Public Prosecution / Statement," *Bahrain News Agency*, January 5, 2013, http://www.bna.bh/portal/en/news/540555.

142 Committee to Project Journalists, "Bahrain arrests photographer who documented dissent," January 9, 2013, http://cpj.org/x/5198.

- In 2014, photographer Hussain Hubail, detained since July 31, 2013, was sentenced to fi e years in prison on charges of "inciting hatred against the regime through social media, and calling for illegal protests" after a trial that lasted around fi e months.[143]

- In December 2015, award-winning photographer Sayed Ahmed al-Mousawi was sentenced to 10 years in prison and stripped of his nationality over "terrorism" charges that included "taking photos of protests and giving SIM cards to terrorists."[144] He was detained in February 2014 and reportedly subjected to beating, hanging, and electrocution to force his confessions.[145]

- And in February 2016, the court of appeal upheld three month sentences against photographer Ahmed Al-Fardan,[146] who published his images on platforms like Instagram and Demotix. He was charged for "intending to participate in illegal gatherings."[147] His earlier arrest in December 2013 reportedly left him with two broken ribs as a result of torture.[148]

Meanwhile, the two harshest sentences ever passed on Bahraini internet users remained in place against bloggers, Abduljalil al-Singace and Ali Abdulemam, who were separately charged with possessing links to a terrorist organization aiming to overthrow the government,[149] disseminating false news, and inciting protests against the government. Al-Singace, a prominent human rights defender and blogger, has been serving a life sentence since March 2011,[150] and his blog has been blocked since 2009.[151] Abdulemam, the owner of Bahrain's popular blocked online forum, Bahrain Online, received a 15-year sentence in absentia in 2011 and is currently a political refugee in the UK. He had previously spent two years in hiding in Bahrain.[152] Both reported experiencing torture at the hands of the authorities.[153]

Surveillance, Privacy, and Anonymity

The government of Bahrain is known for active usage of spyware against dissidents. In November 2015, new evidence showed that Bahrain had used Remote Control System (RCS) from Italian cybersecurity fi m Hacking Team during 2014. The spyware allows remote monitoring, including recording phone calls, logging keystrokes, taking screenshots, and activating cameras, among

143 Reporters Without Borders, "Judicial persecution of Bahraini news providers continues," April 28, 2014, http://bit.ly/1UuLKJ5.

144 BCHR, "NGOs Condemn Imprisonment and Nationality Revocation of Photographer Sayed Ahmed al-Mousawi," November 25, 2015, http://bahrainrights.org/en/node/7661.

145 BCHR, "Bahrain: The Authorities in Bahrain Continue their Campaign against Photographers by Arresting and Torturing another Photographer: Ahmed Al-Mousawi," February 28, 2014, http://bahrainrights.org/en/node/6779

146 "Reporters Without Borders condemns the upholding of imprisonment sentence against photographer Ahmed Al-Fardan for 3 months by the Court of Appeal," [in Arabic] *Bahrain Mirror*, February 3, 2016, http://bahrainmirror.org/news/29153.html

147 Amnesty International, "Bahrain: Photojournalist arrested and tortured: Ahmad Fardan," January 7, 2014, http://bit.ly/1kEFYrL.

148 "Photographer Al-Fardan: I was tortured and beaten at «Criminal Investigation Department," [in Arabic], *Al Wasat* News, January 11, 2014 http://www.alwasatnews.com/4144/news/read/846318/1.html .

149 Reporters Without Borders, "Detained blogger Abduljalil Al-Singace on hunger strike," September 6, 2011, http://bit.ly/1N5BjuP.

150 Reporters Without Borders, "Detained blogger Abduljalil Al-Singace on hunger strike."

151 BCHR, "Activist Abduljalil Alsingace's blog blocked by authorities", February 13, 2009, http://bit.ly/1Vzs497.

152 Peter Beaumont, "Bahrain Online founder Ali Abdulemam breaks silence after escape to UK," *The Guardian*, May 10, 2013, http://bit.ly/1Xl7OtN.

153 "People & Power – Bahrain: Fighting for change," YouTube video, 24:30, posted by Al Jazeera English, March 9, 2011, http://bit.ly/1Flun6y.

other functions.[154] Malicious links are often sent from Twitter and Facebook accounts impersonating well-known opposition figu es, friends,[155] or even accounts of arrested users.[156] In October 2015, at least four cases were recorded in which opposition members received emails containing malicious spyware.[157]

Given that the authorities have been quick to identify social media users who operate under a pseudonym, many users are concerned about restrictions on the ability to use ICTs anonymously. The TRA requires users to provide identificatio when using Wi-Fi and WiMax connections, and the government prohibits the sale or use of unregistered prepaid mobile phones.[158] Further restrictions on the sale of SIM cards were introduced in December 2015. The TRA issued a regulation that limits individuals from purchasing no more than 10 pre-paid SIM cards from a single service provider. The individuals must be present in person when registering the SIM cards and providers must re-check the identity of all subscribers on annual basis. Fingerprints will be used for subscriber identification [159] Additionally, SIM cards will only be available for sale directly from service providers.[160] The move may have a connection to recent prosecutions of individuals accused using SIM cards in bomb attacks.[161]

Since March 2009, the TRA has mandated that all telecommunications companies keep a record of customers' phone calls, emails, and website visits for up to three years. The companies are also obliged to provide the security services with access to subscriber data upon request.[162] Following implementation of the National Safety Status emergency law in March 2011, security personnel began searching mobile phones at checkpoints, behavior that was documented on YouTube.[163]

Cybercafes are also subject to increasing surveillance. Oversight of their operations is coordinated by a commission consisting of members from four ministries, who work to ensure strict compliance with rules that prohibit access for minors and require that all computer terminals are fully visible to observers.[164] In May 2014, the government announced that it is considering new restrictions on cybercafes, including the enforcement of surveillance cameras as well as storage of user's personal identificatio and activity.[165]

A Cyber Safety Directorate at the Ministry of State for Telecommunications Affairs was launched in

154 Bahrain Watch, "How The Government of Bahrain Acquired Hacking Team's Spyware," November 13, 2015, http://bit.ly/2bVNSQ5

155 Bahrain Watch, "The IP Spy Files: How Bahrain's Government Silences Anonymous Online Dissent", May 15, 2013, accessed March 31, 2014, https://bahrainwatch.org/ipspy/viewreport.php.

156 Bahrain Watch, Twitter Post, March 13, 2015, 12:28 PM, https://twitter.com/BHWatch/status/576464787422339072.

157 Bahrain Watch, "Urgent Security Alert for Bahraini Activists," October 18, 2015, http://bit.ly/2ba422J.

158 Geoffrey Bew, "Technology Bill Rapped," *Gulf Daily News,* July 20, 2006, http://bit.ly/1UduN5E.

159 "Adoption of the use of fingerprin to record phone chip," [in Arabic] Alayam Newspaper, July 28, 2016, http://goo.gl/ytz8Zu.

160 TRA, "TRA issues SIM-Card Enabled Telecommunications Services Registration Regulation," February 7, 2016, http://bit.ly/1Q1eK8l.
and TRA, "Resolution No. (13) of 2015, Promulgating the SIM-Card Enabled Telecommunications Services Registration Regulation," accessed August 14, 2016, http://bit.ly/2bv8bmV.

161 "7 and 3 years imprisonment for three Bahrainis who have registered phone chips in the names of Asians," [in Arabic] *Alayam*, November 9, 2015, http://goo.gl/hHqupc.

162 Geoffrey Bew, "Big Brother' Move Rapped," *Gulf Daily News*, March 25, 2009, http://bit.ly/1MULfsL.

163 "الموردات : مرتزقة الظلام تفتش هاتف امرأة," [Policeman checking the private mobile content of a woman driving past a check point in area of Nuwaidrat] YouTube video, 1:05, posted by Nuwaidrat Feb, January 2, 2013, https://youtu.be/9an_lK57QTU.

164 Reporters Without Borders, "Countries Under Surveillance: Bahrain."

165 "The government plans to install cameras in Internet cafes and record identity «for security reasons»" [in Arabic] *Bahrain Mirror,* May 24, 2014, http://bahrainmirror.com/news/16145.html.

November 2013 to monitor websites and social media networks, ostensibly to "ensure they are not used to instigate violence or terrorism and disseminate lies and fallacies that pose a threat to the kingdom's security and stability."[166] The IAA had earlier created a unit to monitor social media and foreign news websites to "respond to false information that some channels broadcast" in 2011, when it was run by the telecommunications ministry.[167] Ironically, the head of the IAA, Isa Al-Hammadi, was dismissed from all of his positions by royal decree in March 2016[168] because of a photo he shared over a WhatsApp group and then circulated widely on social media. The photo showed a rude finge gesture with a background text of "Go Sports," mocking a sports event sponsored by the king's son Nasser bin Hamad.[169]

A computer crimes law was approved by the House of Representatives and ratifie by the government in December 2014. The law (60/2014) criminalizes the illegal access of information systems, illegal eavesdropping over transmission, and the access and possession of pornographic electronic materials.[170] It also criminalizes the encryption of data with criminal intentions at a time when freedom of expression is often considered a criminal act in Bahrain.

Intimidation and Violence

Typically, arrests of Bahraini users involve extralegal methods of intimidation, such as physical violence and torture. Jaleela al-Sayed Ameen, who was arrested and put on trial for inciting hatred against the regime and insulting the king, was reportedly subjected to ill-treatment while held at the criminal investigation department and was later taken to the prison hospital. She was denied contact with her family or lawyer for several days after her arrest and denied visits from her family until the beginning of March 2015.[171]

The government has also used extralegal methods to punish users for their online posts. On January 31, 2015 the ministry of interior revoked the citizenship of renowned blogger Ali Abdulemam,[172] as well as Ali al-Dairi, the founder of the popular news site *Bahrain Mirror*.[173] Both are currently living abroad and continuing their digital activism for democracy in exile. In February 2016, Abdulkhaleq Abdulla (@Abdulkhaleq_UAE), a UAE citizen and a professor of political science was denied entry at Bahrain airport, and was told he is "Persona non grata"[174] because of a rare tweet in which he indirectly criticized the revoking of citizenship to hundreds of Bahraini citizens.[175]

166 "Shaikh Fawaz praises Cyber Safety Directorate", *Bahrain News Agency,* November 18, 2013 http://www.bna.bh/portal/en/news/588716.

167 Andy Sambridge, "Bahrain sets up new units to monitor media output," *Arabian Business,* May 18, 2011, http://bit.ly/1JmHKqP.

168 Bahrain Mirror, "Bahrain's King Dismisses Information Minister from All his Duties," March 4, 2016, http://bit.ly/2bgnzjX

169 Bahrain Mirror, "Al-Hammadi's "Finger" to Nasser bin Hamad Costed him his Job," March 4, 2016, http://bahrainmirror.org/news/29814.html

170 General Directorate of Anti-Corruption & Economic & Electronic Security, Law No. (60) for the year 2014 on information technology crimes, [in Arabic] accessed July 31, 2015, http://bit.ly/1QMpBFD.

171 BCHR, "March Champions for Justice: Bahrain's Imprisoned Women," March 6, 2015, http://bit.ly/1JQAf8T.

172 "Ali Abdulemam: 'I Have Not Lost My Identity. I Am Bahraini'," *Global Voices,* February 20, 2015, http://bit.ly/1JQdXZd.

173 BCHR, "Bahrain revokes citizenship of 72 people, including journalists, doctors and activists," February 02, 2015, http://bit.ly/1Kr9isH.

174 Abdulkhaleq Abdulla, Twitter Post, February 18, 2016, 10:37 AM, https://twitter.com/Abdulkhaleq_UAE/status/700388653755981825

175 Freedom Prayers, Twitter Post, February 19, 2016, 12:34 AM https://twitter.com/FreedomPrayers/status/700599258370670592

Technical Attacks

Cyberattacks against opposition and progovernment pages, as well as other websites, are common in Bahrain. Accounts operated by the opposition are frequently subjected to mass reporting campaigns to have them closed by Twitter.[176] In June 2015, Bahraini Human Rights Watch Society, a government-owned nongovernment organization working to promote a positive image of the government, stated that its website and Twitter account were hacked a few days before its participation in the 29th session of the United Nations Human Rights Council (HRC) in Geneva.[177] In August 2015, the Twitter account of the February 14 Coalition was temporarily hacked.[178] In December 2015, a report mentioned that there are around 2,000 to 3,000 electronic threats per month on Bahraini fi ms.[179] Further, there was an average of 120 weekly cyberattacks on e-government systems in Bahrain, mainly emanating from Iran.[180]

176 Bahrain Detainees, Twitter post, May 12, 2015, 8:23 AM, A tweet mentioning one opposition accounts that has been suspended due to reports, accessed July 31, 2015 https://twitter.com/BH14Detainees/status/598146464934547456.

177 "Bahrain human rights watchdog says victim of hacking," *Arabian Business*, June 15, 2015, http://bit.ly/1GWK7Rp.

178 Manama Press, Twitter Post, August 14, 2015, 6:38 AM https://twitter.com/ManamaPress/status/632184478325084160

179 "Bahraini fi ms facing cyber attack threats," *Dilmun Times*, accessed August 14, 2016, http://www.dilmun-times.com/?p=22072

180 "EGovernment Authority organizes the fi st meeting of "Hawks of information security" to counter electronic intrusions," [in Arabic] Bahrain News Agency, May 12, 2016, http://www.bna.bh/portal/news/726988.

Freedom House

Bangladesh

	2015	2016
Internet Freedom Status	Partly Free	Partly Free
Obstacles to Access (0-25)	12	14
Limits on Content (0-35)	12	14
Violations of User Rights (0-40)	27	28
TOTAL* (0-100)	**51**	**56**

* 0=most free, 100=least free

Population:	**161 million**
Internet Penetration 2015 (ITU):	**14 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- Religious extremists claimed responsibility for the April 2016 murder of Xulhaz Mannan, the founder of a magazine that promoted LGBTI issues both online and off; as well as the October 2015 murder of Faisal Arefin Di an, a publisher of books authored by slain blogger Dr. Abhijit Roy; and the murder of blogger Niladri Chattopadhyay Niloy in August 2015 (see **Intimidation and Violence**).
- Journalist Probir Sikdar was arrested under the ICT Act for publishing a comment about a government minister on his Facebook page (see **Prosecutions and Detentions for Online Activities**).
- In November 2015, the government ordered service providers to temporarily block Facebook, Facebook Messenger, WhatsApp, and Viber; the same day, internet service was inaccessible nationwide for more than an hour (see **Restrictions on Connectivity** and **Limits on Content**).

Introduction

Internet freedom declined after the highest number of fatal attacks by religious extremists targeting online activists in Bangladesh on record in 2015.

During the coverage period of this report, blogger Niladri Chattopadhyay Niloy, and publisher Faisal Arefin Dipon, who was closely associa ed with another blogger, were fatally attacked. In the earlier part of the year, Abhijit Roy, Washiqur Rahman, and Ananta Bijoy Das were killed in separate incidents, each in reprisal for views they had expressed online. Attacks continued in 2016: Xulhaz Mannan, who founded Roopbaan, a magazine which used social media to advocate for the LGBTI community, was killed in April.

Attacks on secular bloggers started in 2013, when Asif Mohiuddin was attacked by extremists, and blogger Ahmed Rajib Haider was killed outside his home. They were singled out in part because of their prominence in the 2013 Shahbag Movement, broad antigovernment protests which grew out of the response to a war crimes tribunal verdict against a religious leader. Protesters said the verdict was too lenient, and religious extremists organized to punish the movement's leading figu es and others they perceived as promoting secular, liberal values. In the past year, Facebook and other social media services were blocked for more than two weeks to prevent unrest after the Supreme Court upheld death penalties handed down by the same tribunal for war crimes committed in 1971.

The government of the Bangladesh Awami League party under Prime Minister Sheikh Hasina officially encourages open internet access and communication as core tools for development. Private commercial stakeholders have also helped in the proliferation of internet usage. Bangladesh further benefits f om a vibrant—if often partisan—traditional media industry, though journalists face threats and legal constraints. Online news outlets were required to register with the government in 2015.

Checks on bloggers and online activity are arguably harsher due to the 2006 Information and Communication Technology (ICT) Act. The act was used for the fi st time in 2013 to arrest four bloggers who had been vocal on different social issues and religious extremism. In August 2013, an amendment was passed increasing the penalty to a minimum of 7 years, up to a maximum 14 years in prison.[1] Police no longer need a warrant to make arrests under the amended act, and the number of prosecutions is increasing.

On August 2015, journalist Probir Shikdar was arrested under the ICT Act on charge of defaming a minister online. He was later freed on bail. There were at least four other arrests for criticizing or making fun of the government or sharing "harmful links" on Facebook. At the end of the reporting period, the government was looking to revise some clauses of the ICT Act.

The attacks by religious extremists, along with the fear of arrest under the ICT Act, have created a climate of intimidation that fosters self-censorship among bloggers and internet users.

1 Mohosinul Karim, "Punishment increased in amended ICT act," *Dhaka Tribune,* August 20, 2013, http://bit.ly/1UBQH85.

Obstacles to Access

The number of internet users in Bangladesh is steadily on the rise. More than 90 percent of users access the internet via mobile phone providers, which recently began offering faster 3G service. The government has decreased the price of bandwidth significantly over the last decade. However, users complain about the high cost of private internet service.

Availability and Ease of Access

The International Telecommunication Union reported internet penetration in Bangladesh at 14.4 percent in 2015, the lowest in South Asia.[2] Government estimates were closer to 39 percent.[3] Mobile phone penetration was just over 80 percent, according to the Bangladesh Telecommunication Regulatory Commission.[4] While ICT usage is increasing fast, Bangladesh is lagging behind globally. The World Economic Forum 2015 Global IT report ranked Bangladesh 109 out of 143 countries worldwide, with infrastructure and regulatory environment scoring poorly, though overall communication service was comparatively affordable, a factor that is driving growth.[5] The government has decreased the price of bandwidth significantly o er the last decade.[6] According to the Alliance for Affordable Internet, 80 percent of the population in Bangladesh can afford a 500 MB mobile broadband plan based on income – one of the highest percentages among less developed countries.[7] However, users complain about the high cost of private internet service in rural areas. The ability to access localized information and create content in Bengali has contributed to the popularity of local blog hosting services.[8]

Although no statistics are available, the higher concentration of economic activities and critical infrastructure in urban areas indicates there are likely to be more internet users in cities. The government's 2009 "Digital Bangladesh by 2021" program seeks to integrate internet access with development efforts in national priority areas, such as education, healthcare, and agriculture.[9] In 2016, 4,547 Union Digital Centers had been established by the government to provide low-cost internet access and related e-services in poorer communities.[10]

Restrictions on Connectivity

The government occasionally restricts the use of mobile service during elections and other times of

2 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1cblxxY; Muhammad Zahidul Islam, "Bangladesh has lowest internet penetration in South Asia: ITU", July 28, 2016, http://www.thedailystar.net/business/bangladesh-has-lowest-internet-penetration-south-asia-itu-1260400.

3 Bangladesh Telecommunication Regulatory Commission, "Internet Subscribers in Bangladesh June 2016", accessed on August 1, 2016, http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-june-2016.

4 Bangladesh Telecommunication Regulatory Commission, "Mobile Phone Subscribers in Bangladesh June 2016", accessed on August 1, 2016, http://www.btrc.gov.bd/content/mobile-phone-subscribers-bangladesh-june-2016.

5 "The Global Information Technology Report 2015", World Economic Forum, accessed in August 1, 2016, http://reports.weforum.org/global-information-technology-report-2015/economies/#economy=BGD.

6 Muhammad Zahidul Islam, "BTCL cuts the price of bandwidth by 42%", *Dhaka Tribune*, April 4, 2014, http://bit.ly/PySyKZ.

7 http://a4ai.org/wp-content/uploads/2016/04/A4AI-2015-16-Affordability-Report.pdf

8 ThinkTechHawaii, "Somewherein: The First Social Media Company in Bangladesh with Syeda Gulshan Ferdous Jana," *YouTube* video, 45:53, August 28, 2014, https://youtu.be/iVXsFDYLcQU.

9 "Strategic Priorities of Digital Bangladesh," Access to Information Program, October 2010,http://bit.ly/1g9Zqvs.

10 "Union Digital Center", Access to Information (a2i) Programme, accessed in August 1, 2016, http://www.a2i.pmo.gov.bd/content/union-digital-center.

possible unrest. No directives to shut down the internet were confi med during the coverage period, though access was interrupted at the end of 2015, when the government blocked Facebook and other popular social media services, supposedly to ensure state security (see Blocking and Filtering). At the same time as the order was given, internet service was shut down for more than an hour due to what news reports described as a "misunderstanding,"[11] adversely affecting communication and commercial activities, especially in the aviation industry.[12]

Bangladesh's physical internet infrastructure was historically vulnerable, relying on the undersea cable SEA-ME-WE-4, which connects Southeast Asia, the Middle East, and Western Europe.[13] Since late 2012, however, Bangladesh is also connected via an international terrestrial cable managed by private companies, reducing the risk of being completely cut off.[14]

ICT Market

Approximately 96 percent of users access the internet via mobile phone providers, which only recently began offering faster 3G service. The remainder subscribe to fi ed lines, either through a traditional internet service provider (ISP), the fi ed telephone network (around three percent), or via one of the three wireless WiMax operators (one percent).[15] In 2015, 119 ISPs were operating nationwide, with no clear market leaders.[16]

Mobile connections are provided by six operators.[17] Grameen Phone, owned by Telenor, had the biggest market share with 43 percent of the total customer base, followed by Banglalink with 24 percent, and Robi with 21 percent. The remaining three, Airtel, Citycell, and the state-owned Teletalk, had a total customer base of 11 percent in June 2016.

Regulatory Bodies

The Bangladesh Telecommunication Regulatory Commission (BTRC), established under the Bangladesh Telecommunications Act of 2001, is the official egulatory body overseeing telecommunication and related ICT issues. The current administration amended the act in 2010, passing telecommunications regulation to the Ministry of Post and Telecommunications and making the BTRC an auxiliary organization.[18] This move created administrative delays in a number of basic processes like

11 "Internet restored after an hour's block", The Daily Star, November 18, 2015, http://www.thedailystar.net/country/internet-blocked-across-country-temporarily-174304.

12 "Internet access restored in Bangladesh after brief shutdown", BDnews24, November 18, 2015, http://bdnews24.com/bangladesh/2015/11/18/internet-access-restored-in-bangladesh-after-brief-shutdown.

13 Faheem Hussain, "ICT Sector Performance Review for Bangladesh," *LIRNEasia*, 2011, http://bit.ly/1VNLUh2.

14 "Bangladesh Connected with Terrestrial Cable," *BDNews24*, December 8, 2012, http://bit.ly/1ga1Gmk.

15 Faheem Hussain, "License Renewal of Mobile Phone Services: What a Country Should Not Do (A Case Study of Bangladesh)," (paper, Telecommunication Policy Research Conference, George Mason University, VA, USA, September 21-23, 2012), http://bit.ly/1FyaNEc.
Abdullah Mamun, "New Player in WiMAX," *The Daily Star,* July 15, 2013, http://archive.thedailystar.net/beta2/news/new-player-in-wimax/ Bangladesh Telecommunication Regulatory Commission, "Internet Subscribers in Bangladesh February, 2014," accessed on April, 2014, http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-february-2014

16 Bangladesh Telecommunication Regulatory Commission, "List of Internet Service Provider (ISP)", accessed on August 1, 2016, http://www.btrc.gov.bd/sites/default/files/opera er_list/Internet_Service_Provider(ISP)_%E2%80%93_Nationwide.pdf.

17 Bangladesh Telecommunication Regulatory Commission, "Mobile Phone Subscribers in Bangladesh in June 2016", accessed on August 1, 2016, http://www.btrc.gov.bd/content/mobile-phone-subscribers-bangladesh-june-2016.

18 S.M. Shahidul Islam and Abdullah-Al Monzur Hussain, "Bangladesh Telecommunication (Amended) Act, 2010," *Manual of Cyber Law in Bangladesh*, (Dhaka: Central Law Book House, 2011), 241-264.

the announcement of new tariffs or license renewals.[19] In 2014, the Ministry of ICT merged with the Ministry of Post and Telecommunications, with the goal of streamlining many ongoing projects and related industries.[20] In addition, the prime minister's office has an Access o Information (A2I) program supported by the United Nations Development Program, which has considerable influence over top-level ICT-related decision making.[21]

Limits on Content

The BTRC blocked Facebook and several other social media service and communication applications for more than three weeks on November 2015, citing reasons of state security. There were no reports of state manipulation of online content. Online news portals were instructed to complete mandatory registration.

Blocking and Filtering

Content relating to religious issues or offending state leaders is subject to censorship in Bangladesh. Domestic websites, including the most popular news sites, *ProthomAlo*, *BDNews24*, and *Banglanews24,* were not subject to targeted blocking during the coverage period of this report. Immediately after, however, in August 2016, news reports said the BTRC had ordered the blocking of 35 news websites for the fi st time.[22] Officials ga e no reason for the blocking, though many of the sites were affilia ed with the political opposition.

International social media and communication apps, however, are regular victims of government censorship. On November 18, 2015, the BTRC ordered service providers to block Facebook, Facebook Messenger, WhatsApp, and Viber, supposedly in order to ensure state security. The shutdown was ordered an hour after the country's Supreme Court upheld the death penalties handed down to 1971 war criminals Salauddin Quader Chowdhury and Ali Ahsan Mohammad Mojaheed by a tribunal in 2013.[23] The government ordered Facebook to be unblocked after 22 days. On December 13, the BTRC emailed an order to ISPs to block Twitter, Skype, and Imo.[24] A day later, the order was rescinded for reasons that remain unclear**.** All other services were also unblocked by mid-December.[25] In early 2015, several social network applications were also blocked or severely disrupted for four days. Mobile service providers were ordered to block Viber, WhatsApp, LINE, Tango, and mypeople,[26] supposedly on grounds that terrorists were using the platforms, which are also used by opposition

19 Faheem Hussain, "Telecom Regulatory Environment in Digital Bangladesh: Exploring the Disconnects between Public Policies/Regulations and Real World Sector Performance," (presentation, Sixth Communication Policy Research South Conference by LIRNEasia and Chulalongkorn University, Bangkok, 2011).

20 "Telecoms, ICT ministries merge," *Telegeography*, February 11, 2014, http://bit.ly/1K8lBK6.

21 UNDP Bangladesh, "Access to Information (II)," accessed on August 8, 2015, http://bit.ly/1ixvvPu

22 "BTRC orders blocking of 35 news sites," *The Daily Star,* August 4, 2016, http://www.thedailystar.net/backpage/btrc-orders-blocking-35-news-sites-1264981.

23 "Social networking sites closed for security reasons, says Minister Tarana Halim," BDNews24, November 18, 2015, http://bdnews24.com/bangladesh/2015/11/18/social-networking-sites-closed-for-security-reasons-says-minister-tarana-halim.

24 Ishtiaq Husain, "Twitter, Skype, Imo blocked in Bangladesh," December 13, 2015, http://www.dhakatribune.com/bangladesh/2015/dec/13/government-blocks-twitter-skype-and-imo.

25 Agence France-Presse, "Bangladesh Lifts Ban on All Social Media," via *Express Tribune,* December 14, 2015, http://tribune.com.pk/story/1010061/bangladesh-lifts-ban-on-all-social-media/.

26 Muhammad Zahidul Islam, "Viber, Tango blocked in Bangladesh," *Dhaka Tribune,* January 19, 2015, http://bit.ly/1OzIY3z; "WhatsApp, mypeople, line also blocked," *TheDaily Star*, January 19, 2015, http://bit.ly/1KEythE.

activists and other internet users. In 2012 and 2013, netizens in Bangladesh also experienced blocks on YouTube and Facebook.

The BTRC censors content primarily by issuing informal orders to domestic service providers, who are legally bound through their license and operations agreements to cooperate. Service providers have described official censo ship as ad hoc in nature, without proper follow-up mechanisms in place to ensure compliance,[27] though orders appear to be becoming more formal. On January 19, 2015, mobile operators reported receiving official, writ en directives from the BTRC to block access to specific social media applications until anuary 21, when the services became accessible again.[28] No appeals have been documented in response to censorship directives.

Content Removal

During the 22-day period when Facebook was blocked, news reports said government officials met with representatives from the company and requested them to set up an office in Bangladesh, su - ject to local content restrictions and government requests for user data perceived to be threatening security in Bangladesh. Facebook representatives did not comment after the meeting.[29] Between July and December 2015, Facebook reported restricting four pieces of allegedly blasphemous content based on government requests; no content was restricted during the same period the previous year.[30]

Media, Diversity, and Content Manipulation

Bangladesh enjoys a vibrant offline and online media indust y, though self-censorship on specific topics is increasing among particular communities. Blocking of social media platforms and communications apps also threatened the diversity of online content (see Blocking and Filtering), though many people used VPNs to bypass blocking.[31]

In 2015, Bangladeshi online news outlets and the online versions of daily newspapers were directed to go through mandatory registration by December 15. The country's print media has been subject to registration requirements like this since the pre-independence period. Through an official P ess Information Department handout,[32] the government justified egistration as a tool to stop the abuse of media to destabilize society.[33] No penalties were reported for noncompliance. There were no other documented economic constraints imposed by the government or other institutions specifically targeting online media outlets, nor documented instances of commentators with undeclared sponsorship manipulating political debate online.

27 UNDP Bangladesh, "Access to Information (II)," accessed June 2013, http://bit.ly/1ixvvPu
Interviews with seven experts who requested anonymity, 2013, Bangladesh.

28 "Viber, WhatsApp unblocked in Bangladesh", *BDNews24*, January 22, 2015, http://bit.ly/1FyaAkv.

29 Muhammad Zahidul Islam, "Bangladesh asks Facebook to fil er content", December 7, 2015, http://www.thedailystar.net/frontpage/facebook-asked-fil er-content-183622.

30 Facebook, "Bangladesh, July 2015-December 2015," *Government Requests Report,* https://govtrequests.facebook.com/country/Bangladesh/2015-H2/.

31 "Internet users defy Facebook ban in Bangladesh", Deutsche Welle, November 20, 2015, http://www.dw.com/en/internet-users-defy-facebook-ban-in-bangladesh/a-18863635

32 Press Information Department (PID), accessed in July 25, 2016, http://www.pressinform.portal.gov.bd/

33 "Registration mandatory for online newspapers", Dhaka Tribune, November 9, 2015, http://archive.dhakatribune.com//bangladesh/2015/nov/09/registration-online-newspapers-made-mandatory.

Online media practitioners and social media commentators reported a climate of self-censorship on political and religious topics during the coverage period of this report, which saw fatal attacks on bloggers and several criminal charges in relation to digital activity (see and Prosecutions and Detentions for Online Activities). Dozens of bloggers have fled the count y, and associates of other victims have closed their blogs or sought refuge with diplomatic missions (see Intimidation and Violence).[34]

Digital Activism

The Shahbag movement, which was initiated by Gonojagoron Mancha (a group primarily comprised of the Bangladesh Online Activists' Network), is the country's most significant example f online activism to date. The protests began in response to a February 2013 war crimes tribunal verdict involving the leader of the country's largest political Islamic party Jamaat-e-Islami—critics said the verdict was lenient—but quickly grew to encompass broader political and economic issues.[35] In its early stages, the movement spread through blogging, Facebook, and mobile telephony.[36] Twitter, which was not widely used in Bangladesh, gained popularity as a tool to broadcast information about Shahbag.[37]

During the coverage period of this study, no comparable instances of online activism with national impact took place in Bangladesh, though internet users continued to use digital tools and social networks to raise funds for social causes.[38] The blocking of popular platforms and messaging services undermined these activities (see Blocking and Filtering). In addition, the government warned users of tools like WhatsApp and Viber of possible censorship or arrest. Officials said they ere concerned about the use of the tools to advance criminal activities and terrorism.[39]

Violations of User Rights

The year 2015 saw the most casualties for online activists in Bangladesh on record. During the coverage period of this report, blogger Niladri Chattopadhyay Niloy, and publisher Faisal Arefin Dipon were fatally attacked by religious extremists, along with an LGBTI activist. In August, 2015, a public university teacher was found guilty of sedition and sentenced in absentia to three years of rigorous imprisonment, which includes hard labor. He had made a derogatory comment about the prime minister on Facebook in 2011. Other arrests under the ICT Act within the coverage period of this report included that of journalist Probir Sikdar.

Legal Environment

Article 39 (1, 2) of Chapter 2 in the Constitution of the People's Republic of Bangladesh recognizes

34 Geeta Anand and Julfikar Ali Mani , "*Bangladesh Says It Now Knows Who's Killing the Bloggers,*" June 8, 2016, http://www.nytimes.com/2016/06/09/world/asia/bangladesh-killings-bloggers.html?_r=0.

35 Mohammad ShahidUllah, "Shahbag People's Movement: New Generation Challenging the Unjust Structure," *Voice of the Oppressed*, February 18, 2013, http://www.voiceoftheoppressed.in/tag/bangladesh-online-activist-network/

36 Tamanna Khan, "Shahbag beyond Boundaries," *The Daily Star*, March 29, 2013, http://bit.ly/1OdiSoR.

37 Faheem Hussain, Zyma Islam, and Mashiat Mostafa, "Proliferation of Twitter for Political Microblogging in a Developing Country: An Exploratory Study of #Shahbag," Research funded by the Asian University for Women Faculty Research Fund, 2013.

38 "Concert for Kombol," *Dhaka Tribune*, December 12, 2014, http://www.dhakatribune.com/entertainment/2014/dec/12/concert-kombol

39 "WhatsApp, Viber to be blocked, when needed: PM", The Daily Star, November 11, 2015, http://www.thedailystar.net/country/whatsapp-viber-be-blocked-pm-170767.

freedom of thought, conscience, and speech as a fundamental right.[40] Online expression has been traditionally considered to fall within the scope of this provision. The judicial system of Bangladesh is independent from the executive and the legislative branches of government, but critics say it can be partisan. Police and regulators generally bypass the courts to implement censorship and surveillance without oversight.[41]

The Information and Communication Technology Act of 2006 is the primary legal reference for addressing issues related to internet usage. Though it defines and os ensibly protects freedom of expression online,[42] it introduced punishments for citizens who violate others' rights to communicate electronically: Section 56 of the act defined hacking as a crime punishable by up o three years in prison, a fine f BDT 10,000,000 (US$125,000), or both. However, under Section 57, different types of violations involving social, political, and religious content distributed electronically are punishable by a minimum of seven years of imprisonment and fines up o BDT 10,000,000 (US$125,000).[43] On August 19, 2013, the ICT act was amended, increasing the maximum prison term from 10 to 14 years.[44] Sections 68 and 82 respectively contain provisions for a Cyber Tribunal and Cyber Appellate Tribunal to expedite judicial work related to any cybercrime. In 2016, there was one Cyber Tribunal in Dhaka, headed by a low-ranking member of the judiciary. The Appellate Tribunal, which can dissolve the Cyber Tribunal's verdicts, had yet to be formed.[45]

Before the 2013 amendment came into effect, police had to seek permission before making ICT-related arrests.[46] Now no warrant is required, and offences under the act are non-bailable, meaning suspects must apply for bail at a court.[47] The harsher provisions in the ICT Act may reflect the go ernment's insecurity regarding internet activism and security.

More legal revisions were underway during the coverage period of this report, when the government was actively formulating the Digital Security Act 2015 to address cybercrime. This law will replace Sections 54-57 of the ICT Act when passed, according to Law Minister Anisul Huq.[48]

While introducing harsher penalties for freedom of expression online, however, the government has simultaneously made some progress in catching the killers and masterminds responsible for the assassinations of bloggers. The biggest success was the fast-tracked trial and verdict delivered in the

40 S.M. Shahidul Islam and Abdullah-Al Monzur Hussain, "Right to Information Act, 2009," *Manual of Cyber Law in Bangladesh*, (Dhaka, Central Law Book House, 2011) 1-47.

41 "The Historic Masdar Hossain Case and the Independence of Judiciary of Bangladesh: A Compilation," *WahabOhid Legal Aid*, March 12, 2013, http://wahabohidlegalaid.blogspot.com/2013/03/the-historic-masdar-hossain-case-and.html
M. Moneruzzaman, "Judiciary independence still on paper," *The Bangladesh Chronicle*, January 15, 2013, http://bit.ly/1MbZnO5.

42 S.M. Shahidul Islam and Abdullah-Al Monzur Hussain, "Information and Communication Technology Act, 2006", *Manual of Cyber Law in Bangladesh*, (Dhaka, Central Law Book House, 2011) 90-91.

43 Bangladesh National Parliament, Act No. 39, Information and Communication Technology Act, 2006, http://bit.ly/1Nqa8wC.

44 A Legal Aid and Human Rights Organizations (ASK), "ICT (Amendment) Act, 2013: Right to Information and Freedom of Expression under Threat," October 9, 2013, http://www.askbd.org/ask/2013/10/09/ict-amendment-act-2013-information-freedom-expression-threat/

45 A Legal Aid and Human Rights Organizations (ASK), "ICT (Amendment) Act, 2013: Right to Information and Freedom of Expression under Threat," October 9, 2013, http://www.askbd.org/ask/2013/10/09/ict-amendment-act-2013-information-freedom-expression-threat/

46 Ellery Roberts Biddle, "Bangladesh's ICT Act Stoops to New Lows," *Global Voices Advocacy,* September 18, 2013, http://bit.ly/1O1Lxy9.

47 "Changes To ICT Law Act against freedom of speech: Rizvi," *TheBangladesh Chronicle,* September 10, 2013, http://bit.ly/1K8oz1l.
"Changes to Info Technology Law: Ominous draft cleared by govt," *Priyo News,* August 20, 2013, http://bit.ly/1LXLZdm.

48 "Bangladesh making Digital Security Act to tackle cyber crimes," BDNews24, January 10, 2016, http://bdnews24.com/bangladesh/2016/01/10/bangladesh-making-digital-security-act-to-tackle-cyber-crimes.

case of Ahmed Rajib Haider, a secular blogger who was murdered in 2013 (see Intimidation and Violence). On December 30, 2015, eight members of the extremist group Ansarullah Bangla Team were found guilty of carrying out or assisting in the murder. Two were sentenced to death, one in absentia, and another was sentenced to life imprisonment. Five other members of the same group received jail terms ranging from three years to ten years[49]

Prosecutions and Detentions for Online Activities

Arrests and prosecutions under the ICT Act have been documented since 2013, when the law was fi st widely applied. The most talked about arrest within the coverage period of this report concerned journalist Probir Sikdar. On August 16, 2015, Probir Sikdar was arrested and later sued for libel under the ICT Act for publishing a comment about a government minister on his Facebook page. In that comment, he said that the minister, a businessman, and a convicted war criminal were responsible for putting his life in danger.[50] He had previously reported on the three men and their alleged activities during the 1971 war in a 2001 news report**.** Following protests from local and international civil rights organizations, he was released on bail on August 19.[51] In mid-2016, the charges remained pending.

A disproportionate sentence was also reported during the coverage period, though the defendant did not report to the court to serve the time. On August 12, 2015, a court in Dhaka sentenced public university teacher Ruhul Amin Khandker in absentia to three years of rigorous imprisonment, which includes hard labor, and a fine f BDT 10,000 (US$ 125) for sedition. The charge was filed in elation to a comment about the prime minister made on Facebook in 2011.[52]

Other cases were reported during the coverage period:

- On August 18, 2015, ruling party politician Wasim Sajjad Likhon filed a case under the ICT Act against Islam Jahurul, who the politician said desecrated an image of Prime Minister Sheikh Hasina and disseminated it on Facebook.[53]
- On December 3, office s of the special Rapid Action Battalion (RAB) forces in Dhaka arrested Towhid Hasan from Pirojpur, Tanvir Ahmed from Shariatpur, and Omar Faruk from Sirajganj, apparently for using Facebook while it was blocked. The three men, 21, 18, and 22 years old respectively, "propagated against the country's constructive activities" by "using blocked Facebook…to share harmful links and provoke others to use the links," news reports said, citing an RAB press release.[54] It was not clear which law they were charged under, and the nature of the content they are accused of sharing was not reported. Though other officials

49 "Bangladesh court awards death to 2, life term to 1 for blogger's murder," *International Business Times,* December 31, 2015, http://www.ibtimes.co.in/bangladesh-court-awards-death-2-life-term-1-bloggers-murder-661570.

50 "Journalist Probir Sikdar sued for libel under ICT Act for writing against Minister Khandker Mosharraf Hossain," *BDNews24,* August 17, 2015, http://bdnews24.com/bangladesh/2015/08/17/journalist-probir-sikdar-sued-for-libel-under-ict-act-for-writing-against-minister-khandker-mosharraf-hossain.

51 "Journalist Probir Sikdar released on bail," *Daily Star,* August 19, 2015, http://www.thedailystar.net/country/journalist-probir-sikdar-gets-bail-129166.

52 "University teacher jailed for Facebook post on Bangladesh PM," *The Daily Star*, August 13, 2015, http://bit.ly/1VNPKXq.

53 "Case filed for dis orted image," *BDNews24,* August 19, 2015, http://bangla.bdnews24.com/bangladesh/article1013243.bdnews.

54 "3 held for using Facebook in alternate ways," *New Age,* December 3, 2015, http://newagebd.net/181108/3-held-for-using--in-alternate-ways/.

threatened the users of proxy servers with repercussions in 2015,[55] VPNs are widely used in Bangladesh.

- On December 10, RAB office s arrested satirical writer Refayet Ahmed, the administrator of the popular Facebook page *MojaLosss?* ("Are You Making Fun?"), for making "provocative Facebook posts against the government and the state." [56] The page won popularity for using satire to talk about corruption and other social problems. A case was filed against efayet under the ICT Act. On December 14, he was freed on bail.[57]

Outstanding cases under the ICT Act against four bloggers prominent in the Shahbag Movement, Asif Mohiuddin, Rasel Parvez, Mashiur Rahman Biplob, and Subrata Ashikari Shuvo, appear to be on hold.[58] The four, whose blogs were briefly bloc ed in 2013, were then detained for harming religious sentiment and released on bail.

Surveillance, Privacy, and Anonymity

According to Article 43 of the country's constitution, Bangladesh recognizes its citizens' right to privacy and correspondence.[59] However, there is no specific pri acy or data protection law in Bangladesh, leaving internet and mobile phone users vulnerable to privacy violations, predominantly through the voluntarily sharing of information via mobile phones and the internet.[60]

Although the government does not require individuals to register to blog or use the internet, registration became mandatory for online news portals during the coverage period (see Media, Diversity, and Content Manipulation). Since the end of 2015, citizens are also required to provide biometric details, in addition to national identity cards and related personal information, to obtain a mobile connection.[61] Citizen rights groups raised concerns about the security of the process and possible usage of biometric data by third parties.[62]

The government can request telecommunications providers retain the data of any user for an unspecified period under the Bangladesh elecommunication Regulatory Act 2001.[63] The Act was amended in 2010 and allows government mechanisms to intercept electronic voice or data communications from any individual or institution to ensure the security of the state without a court order;

55 "Proxy servers to access Facebook will soon be unavailable: State Minister Tarana," BDNews24, November 29, 2015, http://bdnews24.com/bangladesh/2015/11/29/proxy-servers-to-access-facebook-will-soon-be-unavailable-state-minister-tarana.

56 "Hours after lifting ban on Facebook, Bangladesh arrests satirist for anti-govt posts," *First Post,* December 11, 2015, http://www.fi stpost.com/world/hours-after-lifting-ban-on-facebook-bangladesh-arrests-satirist-for-anti-govt-posts-2542090.html.

57 "'Moja Losss' admin freed on bail," *New Age,* December 14, 2015, http://newagebd.net/184424/moja-losss-admin-freed-on-bail/.

58 "I have to help the people of Bangladesh", *DW,* April 22, 2014, http://bit.ly/1Kaf2vd. Email interview with Asif Mohiuddin's legal counsel.

59 Constitution of the People's Republic of Bangladesh, March 26, 1971, http://bdlaws.minlaw.gov.bd/pdf_part.php?id=367

60 Faheem Hussain and Mohammad SahidUllah, "Mobile Communication and Internet in Bangladesh: Is Privacy at Risk for Youth Population?," *Media Watch*, Centre for Communication Studies, 2013.

61 "Bangladesh launches registration of mobile phone SIMs with biometric details, *BDNews24,* December 16, 2015, http://bdnews24.com/bangladesh/2015/12/16/bangladesh-launches-registration-of-mobile-phone-sims-with-biometric-details.

62 Md. Joynul Abedin, "Biometric SIM Registration and Public Anxiety," *Daily Sun,* March 10, 2016, http://www.daily-sun.com/printversion/details/119870/Biometric-SIM-Registration-and-Public-Anxiety-.

63 Telecommunications Industry Dialogue, "Bangladesh," https://www.telecomindustrydialogue.org/resources/bangladesh/.

the act also requires domestic service providers to cooperate, though without clear provisions detailing procedures or penalties for noncompliance.[64]

During the coverage period, local news reports said the home ministry had submitted a proposal to purchase approximately US$ 25 million worth of equipment from foreign companies to upgrade its mobile telephony, internet, and related surveillance networks. The proposal asked the cabinet committee on economic affairs to relax procurement regulations to facilitate the purchase, which would enable the National Telecommunication Monitoring Center (NTMC) to conduct "lawful interception" to assist local law enforcement agencies. The center has operated under the home ministry since February 2014, the news reports said. Foreign companies listed in the proposal include U.S. fi ms Verint Systems and SS8, German fi ms Trovicor and UTIMACO, the Italian fi m RCS, the Chinese fi m Inovatio, and the Swiss fi m New Saft.[65] The companies advertise equipment capable of analyzing data traffic, calls, emails, and audiovisual ma erials online.

In 2014, the UK-based nonprofit Pri acy International reported that Bangladesh's Rapid Action Battalion, a special forces unit implicated in human rights abuses, was seeking to purchase mobile surveillance technology from a company based in Switzerland. The technology would allow police to "indiscriminately gather data from thousands of mobile phones in a specific a ea and at public events such as political demonstrations," according to Privacy International.[66] The same year, leaked documents about a Bangladesh law enforcement agency's 2012 purchase of FinFisher software distributed by Gamma International to monitor digital traffic was published on Wikileaks [67]

According to Facebook, the Bangladesh government made three requests to the social network service provider for information on three Facebook users between January and June 2015, but Facebook did not comply.[68]

Intimidation and Violence

Blogger Niladri Chattopadhyay Niloy and Xulhaz Mannan, the founder of a magazine on LGBTI issues with a well-established online following, were murdered between June 2015 and May 2016. Faisal Arefin Dipon, a publisher who orked with another murdered blogger, was also killed.

This continued a violent trend. Between February 2013 and June 2016, at least 39 people were murdered in Bangladesh by religious extremists targeting high profile proponents of secular viewpoints.[69] "Atheist bloggers" were particularly singled out as key instigators behind the 2013 Shahbag Movement (see Digital Activism) which catalyzed the campaign of killings.[70] Armed assailants hospitalized blogger Asif Mohiuddin with serious stab wounds in January 2013;[71] now overseas, he believes he

64 Abu Saeed Khan, "Bangladesh Telecommunication (Amended) Act, 2010," (presentation, Third South Asian Meeting on the Internet and Freedom of Expression, Dhaka, Bangladesh, 14-15 January 2013).

65 Rejaul Karim Byron, "Bangladesh to purchase modern surveillance equipment," August 3, 2015, http://www.thedailystar.net/frontpage/govt-buy-new-surveillance-tools-120967.

66 EdinOmanovic and Kenneth Page, "Who is Selling Surveillance Equipment to a Notorious Bangladeshi Security Agency," Privacy International, April 29, 2013, https://www.privacyinternational.org/?q=node/427

67 RezaulHauqe, "WikiLeaks reveals Bangladesh's spyware purchase," *BDNews24*, November, 2, 2014, http://bit.ly/1NqbIhO.

68 https://govtrequests.facebook.com/country/Bangladesh/2015-H1/#.

69 http://www.nytimes.com/2016/06/09/world/asia/bangladesh-killings-bloggers.html?_r=0 .

70 Al Jazeera, "Bangladesh Opposition Protests turn Deadly," February 22, 2013, http://www.aljazeera.com/news/asia/2013/02/2013222103554838445.html.

71 "Blogger knifed in Dhaka," *BDNews24*, January 14, 2013, http://bdnews24.com/bangladesh/2013/01/14/blogger-knifed-in-dhaka1

remains on a hit list.[72] In February, leading Shahbag activist Ahmed Rajib Haider was murdered.[73] Police found a series of posts targeting Rajib and other key figu es in the movement on the blog *Sonar Bangladesh*, which the BTRC subsequently blocked.[74]

Though Al-Qaeda networks claimed responsibility in some cases,[75] police have say local radical groups, notably Ansarullah Bangla Team, recruited and trained students and religious teachers to execute the targets, frequently using machetes.[76] Eight members of the group have been convicted for their involvement in the killing of Ahmed Rajib Haider in 2013, though two remain at large (see Legal Environment). In 2016, Deputy Inspector General Monirul Islam, who heads a counterterrorism unit established in February, told the *New York Times* that these arrests had slowed the group's activity in 2013 and 2014, but that it had reorganized and resumed its campaign with renewed intensity since then.[77]

In April 2016, armed men killed Xulhaz Mannan in his apartment in Dhaka along with a friend.[78] Mannan founded *Roopbaan*, a print magazine serving the LGBTI community, in 2014. Homosexuality is a criminal offence in Bangladesh.[79] The magazine had limited distribution because of the sensitivity of the topic,[80] but formed part of a wider advocacy network that used social media to create community online and advocate for LGBTI causes, including an annual Rainbow Rally coinciding with Bengali new year celebrations, which was cancelled in 2016 as a result of permit issues and threats.[81] Ansarullah Bangla Team claimed responsibility for the murders.[82]

The year 2015 saw unprecedented physical violence against online activists and their colleagues:

- On February 25, two unknown assailants attacked the Bangladeshi-American atheist blogger Dr. Abhijit Roy and his wife Rafida Ahmed Bonya on the Dhaka Uni ersity campus. Abhijit Roy managed the blog *Muto-Mona* ("Free Thinker") from America, and had returned to attend an annual book fair. Dr. Roy died and his wife was badly injured.[83] The Ansarullah

72 Pantha and Rezwan, "Bangladeshi Blogger Writes About Prison Experience," *Global Voices,* July 28, 2013, http://bit.ly/1LXOeh4. Austin Dacey, "Bangladesh's Atheist Blogger Still Wants to Talk," *Religion Dispatches,* December 12, 2013, http://bit.ly/1UHFYE7.

73 "Blogger Brutally Killed," *The Daily Star*, February 16, 2013, http://archive.thedailystar.net/newDesign/news-details.php?nid=269336

74 "12 Blogs, Facebook Pages Blocked," *BDNews24*, February 20, 2013, http://bit.ly/1EVHMHB.

75 "Al-Qaeda branch claims responsibility for murder of writer-blogger Avijit Roy, "*The Daily Star*, May 13, 2015, http://bit.ly/1QoOBm8.

76 Geeta Anand and Julfikar Ali Mani , "*Bangladesh Says It Now Knows Who's Killing the Bloggers,*" June 8, 2016, http://www.nytimes.com/2016/06/09/world/asia/bangladesh-killings-bloggers.html?_r=0 .

77 Geeta Anand and Julfikar Ali Mani , "Bangladesh Says It Now Knows Who's Killing the Bloggers," June 8, 2016, http://www.nytimes.com/2016/06/09/world/asia/bangladesh-killings-bloggers.html?_r=0 .

78 Saad Hammadi and Aisha Gani, "Founder of Bangladesh's fi st and only LGBT magazine killed," *The Guardian,* April 25, 2016, https://www.theguardian.com/world/2016/apr/25/editor-bangladesh-fi st-lgbt-magazine-killed-reports-say-roopbaan .

79 Ashif Islam Shaon, "Where does Bangladesh stand on homosexuality issue?" *Dhaka Tribune,* April 27, 2016, http://archive.dhakatribune.com/bangladesh/2016/apr/27/where-does-bangladesh-stand-homosexuality-issue.

80 "First local magazine for gays launched," *Daily Star,* January 20, 2014, http://www.thedailystar.net/fi st-local-magazine-for-gays-launched-7611.

81 Rezwan, "LGBT Activists Arrested at Bengali New Year March, Later Released," *Global Voices Advocacy,* April 15, 2016, https://advox.globalvoices.org/2016/04/15/lgbt-activists-arrested-at-bengali-new-year-march-later-released/; Agence France-Presse, "Bangladesh 'rainbow rally' cancelled over permit issues," via *Daily Mail,* April 13, 2016, http://www.dailymail.co.uk/wires/afp/article-3538373/Bangladesh-group-hold-rainbow-rally-despite-threats.html.

82 Eliott C. McLaughlin, Don Melvin, and Tiffany Ap, "Al Qaeda group claims responsibility for Bangladesh LGBT hacking murders," April 25, 2016, http://www.cnn.com/2016/04/25/asia/bangladesh-u-s-embassy-worker-killed/.

83 "Assailants Hack to Death Writer Avijit Roy, Wife Injured," *BDNews24,* February 26, 2015, http://bit.ly/1LKI5SS.

Bangla Team claimed responsibility on Twitter.[84] On March 2, Rapid Action Battalion officials arrested Farabi Shafiur Rahman, a radical Islamist who had th eatened Roy and shared his location and photographs with others.[85] On June 19, 2016, a key suspect in Abhijit Roy's murder was killed during a gun battle with police in Dhaka.[86]

- On March 30, blogger Washiqur Rahman, known for his critical writings about Islam, was hacked to death near his home in Dhaka.[87] Bystanders detained two of the attackers, both students from Islamic seminaries, at the scene; a third fled. The police la er charged four people with murder, including the alleged mastermind.[88]

- On May 12, Ananta Bijoy Das, another prominent contributor to *Muto-Mona,* was killed by four masked men armed with machetes in the northeastern Bangladeshi city, Sylhet.[89] Ananta Bijoy was one of the founding members of Gonojagoron Mancha, the coalition of activists who started the Shahbag Movement.[90] News reports say he had received death threats from extremists and had tried to leave the country to attend a press freedom event in Sweden, but was denied a visa. On June 8, 2015, police arrested a suspect in connection with the murder.[91]

- On August 7, Niladri Chattopadhyay Niloy, a blogger and member of Gonojagoron Mancha, the main organization behind the Shahbag Movement, was killed in his home by four unidentified assailants a med with cleavers. Ansarulla Bangla Team claimed responsibility.[92] On August 14, two suspected members of the group were arrested in connection with the murder.[93] On August 18, police arrested three more members of the same organization, suspected of planning and executing the murders of Abhijit Roy and Ananta Bijoy Das.[94] On November 18, three more people were arrested in connection with Niloy's murder; one had threatened Niloy on Facebook, and two who claimed responsibility for the murder online.[95]

- On October 31, Faisal Arefin Dipon, a publisher f books by Abhijit Roy, was hacked to

84 "Ansar Bangla-7 Claims Avijit killing responsibility," *ProthomAlo*, February 27, 2015, http://bit.ly/1XMijXa.

85 Oliver Naughland and SaadHammadi, "Atheist blogger Avijit Roy 'was not just a person … he was a movement'," *The Guardian*, March 7, 2015, http://gu.com/p/46dez/stw.

86 BBC News, "Bangladesh Avijit Roy murder: Main suspect killed by police," June 19, 2016, http://www.bbc.com/news/world-asia-36570021 .

87 "Knife attack kills Bangladesh blogger Washiqur Rahman," BBC, March 30, 2015, http://www.bbc.com/news/world-asia-32112433

88 Jason Burke, "Bangladesh police charge four men with murder of blogger," *The Guardian*, March 31, 2015, http://gu.com/p/475tn/stw.

89 Joseph Allchin and Victor Mallet, "Third Secular Blogger Killed on Bangladesh Street," *Financial Times*, May 12, 2015, http://on.ft.com/1IYL2wO.

90 "Bangladesh Blogger Ananta Bijoy Das Hacked to Death," *BBC*, May 12, 2015, http://www.bbc.com/news/world-asia-32701001

91 "CID Arrest Sylhet Press Photographer as a Suspect Over Blogger Ananta Bijoy Das Murder,"*BDNews24*, June 8, 2015, http://bit.ly/1ga9t3z.

92 "Bangladesh blogger Niladri hacked to death in Dhaka," *Daily Star,* August 8, 2015, http://www.thedailystar.net/frontpage/blogger-killed-once-again-123493.

93 BBC News, "Bangladesh blogger Niladri hacked to death in Dhaka," August 14, 2015, http://www.bbc.com/news/world-asia-33926342.

94 BBC News, "Bangladesh blogger killings: police arrest three people," August 18, 2015, http://www.bbc.com/news/world-asia-33971810.

95 Al Jazeera, "Bangladesh arrests three men over murder of blogger," November 18, 2015, http://www.aljazeera.com/news/2015/11/bangladesh-arrests-men-murder-blogger-151118140032685.html.

death in his office in Dhaka [96] Ahmed Rahim Tutul, another publisher of Abhijit Roy's work, was attacked and badly injured in Dhaka on the same day, along with two secular writers, Ranadeep Basu and Tareque Rahim.[97] In early 2016, no one had claimed responsibility for these attacks and no arrests had been made, though Ansarullah Bangla Team was suspected.[98] On June 15 of 2016, the police arrested a suspected militant Sumon for the attack on Tutul. On August 23, a suspected leader of Ansarullah Bangla Team, Moinul Hasan Shamim was arrested for Dipon's murder. On September 3, Abus Sabur was arrested on suspicion of masterminding both of those accounts.[99]

This disturbing series of fatal attacks on secular bloggers has increased security concerns in the online activist community. A handful of bloggers left the country or sought asylum abroad during the coverage period of this report.[100] Others have expressed their determination to continue writing.[101]

Technical Attacks

No cyberattacks on online news sites and blogs were documented in Bangladesh during the coverage period. A high profile in asion of a computer at the central bank took place, and was used to transfer millions of dollars to a bank in the Philippines, highlighted cybersecurity vulnerabilities.[102] ISPs have informally organized a Cyber Emergency Response Team to deal with malicious online threats.[103]

96 The Associated Press, "Secular publisher hacked to death in latest Bangladesh attacks," via *The Guardian,* October 31, 2015, http://www.theguardian.com/world/2015/oct/31/faisal-abedin-deepan-bangladesh-secular-publisher-hacked-to-death.

97 The Associated Press, "Publisher of secular books killed, three bloggers wounded in Bangladesh," via *Indian Express,* December 25, 2015, http://indianexpress.com/article/world/neighbours/bangladesh-three-bloggers-attacked-one-critical/.

98 "DB suspects Ansarullah's link to Dipan murder," *Daily Sun,* November 1, 2015, http://www.daily-sun.com/printversion/details/87753/DB-suspects-Ansarullah%E2%80%99s-link-to-Dipan-murder.

99 Arifur Rahman Rabbi, "Publisher Dipan murder mastermind held," *Dhaka Tribune,* September 4, 2016, http://www.dhakatribune.com/bangladesh/2016/09/04/publisher-dipan-murder-mastermind-held/.

100 Communication with local rights organizations reflec ed this information. However, rights organizations do not publicize the details of individual cases for security reasons.

101 Saeed Ahmed, "Washiqur Rahman: Another secular blogger hacked to death in Bangladesh,"*CNN*, March 31, 2015, http://cnn.it/19v17k8.

102 Raju Gopalakrishnan and Manuel Mogato, "Bangladesh Bank official s computer was hacked to carry out $81 million heist: diplomat," Reuters, May 19, 2016, http://www.reuters.com/article/us-cyber-heist-philippines-idUSKCN0YA0CH.

103 Bangladesh Cyber Emergency Response Team, accessed April 2013, http://www.bdcert.org/v2/

Freedom House

Belarus

	2015	2016
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	15	13
Limits on Content (0-35)	21	21
Violations of User Rights (0-40)	28	28
TOTAL* (0-100)	**64**	**62**

* 0=most free, 100=least free

Population:	**9.5 million**
Internet Penetration 2015 (ITU):	**62 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- Belarusian users enjoyed considerable improvements in internet speed in 2015-2015 (see **Availability and Ease of Access**)
- Independent online media and social networks increased in importance as sources of news for Belarusians, especially in the lead up to the October 2015 presidential elections (see **Media, Diversity, and Content Manipulation**).
- As of 2015, the government began utilizing new amendments to the Media Law to block, close down, and intimidate critical websites (see **Blocking and Filtering** and **Content Removal**).
- The authorities continued their persecution of independent journalists reporting online, targeting freelance and unaccredited journalists with administrative penalties (see **Prosecutions and Detentions for Online Activities**).
- The government boosted its legal and technical capabilities to monitor and conduct surveillance on internet users, acquiring sophisticated surveillance technology from Chinese fi ms (see **Surveillance, Privacy, and Anonymity**).

Introduction

Internet freedom improved in Belarus in the past year, with faster internet speeds, and relaxed rules facilitating more public Wi-Fi access, while independent online media outlets increased their reach.

The internet has increased in importance as a source of independent information, with greater numbers of Belarusians going online to find eliable news, while state sponsored mass media declines in popularity. More Belarusians are able to access the internet, with gradual improvements in coverage and speed as well as further development of internet infrastructure. The government has also relaxed some laws relating to public Wi-Fi access, meaning public venues are no longer required to obtain a license before offering Wi-Fi.

Despite improvements in connectivity, the authorities have continued censoring some information online, with newly amended media laws granting authorities greater powers to control content. In addition to blocking access to websites, the Ministry of Information issues warnings to websites, prompting the removal of articles and pages.

Since late 2014, structural weaknesses, aggravated by Russia's economic crisis, have produced rising inflation and unemployment. Belarus experienced a ecession in the last year, with GDP falling 3.5 percent and the ruble losing more than half its value against the dollar. GDP fell another 4 percent in early 2016. These challenges have placed additional economic pressure on non-state media.

Nevertheless, the online sphere in Belarus is relatively vibrant, and citizens regularly launch campaigns online, such as a crowdmapping election monitoring initiative launched in the lead up to the October 2015 presidential elections.

As the EU lifted a fi e-year freeze on relations with Belarus in February 2016, the regime has practiced relative restraint in relation to online expression, with fewer arrests and instances of violence against journalists and social media users in the coverage period. However, freelance journalists continue to operate in a legal limbo which allows authorities to hamper their work by issuing administrative penalties, and at least 25 administrative cases were launched against freelancers working online within the past year. The authorities continue to boost their considerable surveillance powers, enacting a law which requires internet service providers (ISPs) to retain user information about their subscribers' activities online, and hand the information to authorities on request.

Obstacles to Access

Despite several years of economic stagnation and a significant downturn in 2015-2016, the Belarusian government continued to invest in the country's internet and ICT infrastructure. In its 2015 Report, the International Telecommunication Union (ITU) found Belarus to be among the world's most dynamic countries in terms of growth of households with computers and internet access, mobile broadband penetration, mobile cellular subscriptions and international internet bandwidth per internet user. In terms of the ITU's ICT Development Index (IDI), Belarus continued to advance in the rankings. It ranked

36th in 2015, climbing 14 spots since 2010, and has the highest IDI in the Commonwealth of Independent States region.[1]

Availability and Ease of Access

The International Telecommunication Union (ITU) reported Belarus' internet penetration rate as 62 percent in 2015, compared to just 32 percent in 2010.[2] The independent organization Gemius reported that the number of Belarusian internet users increased by almost 81,000 in 2015. Though this growth in the overall online audience was not pronounced, the increase in the number of daily users is a major trend.[3] More than 5 million Belarusians—70 percent of the population aged 15 to 74—were regularly accessing the internet by the end of 2015, 87 percent of them daily.[4]

Since 2010, the proportion of female internet users rose from 48.7 percent to 52.1 percent.[5] As of December 2014, the share of internet users concentrated in the capital city of Minsk had decreased to 29 percent, and the number of users in towns and rural areas had risen to 39 percent.[6] Some 75 percent of Belarusians live in urban areas, but a digital divide separates the capital and other regions. More than half of urban households have access to the internet, reaching around 57 percent. In rural areas, this figu e drops to around 40 percent.[7]

The State of Broadband Report 2015 ranked Belarus 23rd among developing countries, with 57 percent of households connected to the internet,[8] along with 97 percent of companies. The government reported that 84 percent of households accessing the internet did so using broadband.[9] The fi ed broadband subscriber base reached 2.8 million by the end of 2015, a penetration rate of almost 30 percent.[10] Belarus has the highest fi ed-broadband penetration in the post-Soviet region, with over 3.6 million broadband ports available.[11] During the past year, however, growth has tapered off.

1 International Telecommunication Union (ITU), "ICT Development Index 2015," http://www.itu.int/net4/ITU-D/idi/2015/#idi2015countrycard-tab&BLR; Belarus is one of only four countries that have joined the upper quartile of countries between 2010 and 2015, demonstrating a consistency of improvement: ITU, "Measuring the Information Society Report 2015: Executive Summary,"2015, http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-ES-E.pdf.

2 International Telecommunication Union, "Percentage of Individuals Using the Internet," 2000-2015, http://bit.ly/1FDwW9w.

3 The daily audience from October 2011 to October 2014 increased by 90 percent. See Mikhail Doroshevich, "Users of Social Media in Belarus and their Behavior," *Gemius*, July 1, 2015, http://www.slideshare.net/MikhailDoroshevich/doroshevich-01072015?related=1, p. 7.

4 Mikail Doroshevich and Marina Sokolova, "WWW: The Limits of Developing Extensive Infrastructure," *Belarusian Yearbook 2016*, Agency for Social and Political Expert Appraisal, *Nashe Mnenie*, http://nmnby.eu/yearbook/2016/en/page16.html.

5 "Five Years of Belarusian Internet Audience," *e-belarus*, February 5, 2015, http://www.e-belarus.org/news/201502051.html. 2015 SAITO poll sited by Doroshevich and Sokolova, "WWW: The Limits of Developing Extensive Infrastructure," Belarusian Yearbook 2016, Agency for Social and Political Expert Appraisal, *Nashe Mnenie*, http://nmnby.eu/yearbook/2016/en/page16.html. For a detailed gender breakdown, see Mikhail Doroshevich, "Gender Inequality in the Belarusian Internet," *Gemius*, September 29, 2015, http://www.slideshare.net/MikhailDoroshevich/gender-inequality-in-belarusian-internet-audience?next_slideshow=1.

6 "Five Years of Belarusian Internet Audience," *e-Belarus*, February 5, 2015, http://www.e-belarus.org/news/201502051.html.

7 Mikail Doroshevich and Marina Sokolova, "WWW: The Limits of Developing Extensive Infrastructure," *Belarusian Yearbook 2016*, Agency for Social and Political Expert Appraisal, *Nashe Mnenie*, http://nmnby.eu/yearbook/2016/en/page16.html.

8 Broadband Commission, *The State of Broadband 2015: Universalizing Broadband,* September 2015, http://bit.ly/1QTuNrB, Annex 4, p. 90.

9 "Information and communication technology infrastructure improving in Belarus," *Belarus News Belarusian Telegraph Agency (BelTA)*, September 30, 2014, http://bit.ly/1LS6r2K.

10 "Ministry of Communications: Number of landline broadband subscribers in Belarus is close to 3 million" (in Russian), *Providers.by*, January 30, 2016, http://providers.by/2016/01/news/minsvyazi-kolichestvo-abonentov-stacionarnogo-shpd-v-belarusi-priblizhaetsya-k-3-millionam; "Belarus telecom subscriber base hits 4.5 mln in 2014," *e*-Belarus, February 21, 2015, http://bit.ly/1GhLVq3.

11 , "Belarus telecom subscriber base hits 4.5 mln in 2014," *e*-Belarus, February 21, 2015, http://bit.ly/1GhLVq3; "ITU Ranks Belarus as IDI Leader in CIS Region," *Development.by*, November 27, 2014, http://bit.ly/1RMskQ3.

The number of subscribers to Belarus' fi ed telephone line network, through which the majority of Belarusian access the internet, remained steady at about 4.4 million. As of July 2015, Belarus had 11.3 million mobile telephone subscribers. The current mobile penetration level in Belarus suggests a saturation of the market. Mobile subscribers are served by 6,500 base stations covering 97.9 percent of the country's territory.[12] Smartphones are becoming cheaper and their share in the mobile market is rising. MTS, the largest of Belarus' three mobile providers, noted that smartphones now make up the vast majority of devices purchased in its stores; providers estimate that smartphones comprise 38 to 50 percent of their networks.[13] This percentage is likely to rise following the launch of 4G and the expansion of 3G service during the past year. In 2015, state-owned Beltelecom added about public 75,000 Wi-Fi hotspots and now operates a total of almost 375,000 throughout the country.[14]

Numbering only 1.8 million in 2011, mobile internet access subscribers had grown to 4.3 million by 2014, with a penetration rate of 46 percent.[15] A government poll conducted in late 2015 found that 59 percent of internet users access the web from mobile devices, and more than 77 percent of Belarusian youth aged 16 to 29 use mobile internet.[16] Nevertheless, only 6 percent of page views in Belarus are made via mobile phones or tablets.[17]

Technological advances in 2015-2016 should improve Belarus' internet capabilities. GPON fibe -optic technology is replacing ADSL lines.[18] Commercial 4G LTE service, which will increase the speed of mobile broadband internet access launched in December 2015. Initially available in Minsk via 150 base stations, the service will be made available in the country's fi e regional capitals in 2016.[19] The service will be fi st offered by MTS, and Belarus' other providers are expected to offer the service later in 2016.[20] Belarus providers continue to move towards full 3G coverage;[21] as of October 2015, 3G mobile networks covered 53 percent of the country, where 96 percent of the population lives.[22] In

12 Alyaksey Areshka, "Communications ministry reports decrease in number of mobile subscribers," *BelaPAN*, July 29, 2015, http://en.belapan.by/archive/2015/07/29/en_20250729H.

13 "The share of smartphones in the MTS network – 38%, annual average monthly internet traffic ose by 22%" (in Russian), *Providers.by*, November 18, 2015, http://providers.by/2015/11/mobile/mts-mobile/dolya-smartfonov-v-seti-mts-38-za-god-srednemesyachnyj-rasxod-internet-trafika-u-abonen ov-vyros-na-22; "Velcom: Minsk in 15th place in internet-active cities – Brest in fi st place" (in Russian), *Providers.by*, December 16, 2015, http://providers.by/2015/12/mobile/velcom/velcom-minsk-v-rejtinge-internet-aktivnyx-gorodov-na-15-om-meste-na-pervom-brest/#more-21185.

14 "Beltelecom has installed 375,000 Wi-Fi access points throughout the country" (in Russian), *Providers.by*, January 21, 2016, http://providers.by/2016/01/provajdery-minska/beltelecom/beltelekom-ustanovil-375-tysyach-tochek-dostupa-wi-fi-po-vsej strane/#more-21451; "Beltelecom internet base passed two million mark in 2014, paper says," *eBelarus*, February 18, 2015, http://bit.ly/1VWRqBr.

15 "Belarus prioritizes innovation-driven development, information society," *e*-Belarus, April 4, 2014, http://bit.ly/1KdqkKq.

16 "More than 87% of Belarusian users turn to the internet almost daily" (in Russian), *BelTA*, January 11, 2016, http://www.belta.by/tech/view/bolee-87-belorusskih-juzerov-obraschajutsja-k-internetu-prakticheski-ezhednevno-176980-2016.

17 Gemius, "Consumers go mobile in CEE: Mobile market overview," 2014, http://bit.ly/1qWeJg7.

18 "Beltelecom: By 2020, GPON will be in each city high-rise building" (in Russian), *Providers.by*, January 21, 2016, http://providers.by/2016/01/provajdery-minska/beltelecom/beltelekom-k-2020-godu-gpon-poyavitsya-v-kazhdoj-gorodskoj-mnogoetazhke/#more-21447.

19 "4G launch to improve Belarus' standing in ICT Development Index," *BelTA*, December 17, 2015, http://eng.belta.by/society/view/4g-launch-to-improve-belarus-standing-in-ict-development-index-87728-2015.

20 At present, providers estimate that 9-15% of their networks include 4G-capable devices. See "iPhone – the most common LTE-device in Belarus" (in Russian), *Providers.by*, November 27, 2015, http://providers.by/2015/11/news/iphone-samoe-rasprostranennoe-lte-ustrojstvo-v-belarusi/#more-21011.

21 "Velcom will increase 3G network coverage in Belarus to 97% by the end of the year" (in Russian), *Providers.by*, February 4, 2015, http://providers.by/2016/02/mobile/velcom/velcom-do-konca-goda-uvelichit-pokrytie-3g-seti-po-belarusi-do-97/#more-21583.

22 "Ministry of Communications counts number of new users of internet and TV for January-September" (in Russian), *Providers.by*, November 2, 2015, http://providers.by/2015/11/news/v-minsvyazi-poschitali-kolichestvo-novyx-abonentov-interneta-i-tv-za-yanvar-sentyabr/#more-2083.

January 2016, a Chinese rocket placed a Belarusian communications satellite into orbit; Belintersat 1 will offer broadband internet, among other commercial services..[23]

On its official ebsite, the government stated that the country's international internet gateway capacity had increased to 783 Gbps in 2015.[24] However, other sources indicated that the gateway had slipped from 770 to 610 Gbps by October of that year.[25]

In general, the speed of the internet improved in Belarus, but the country continues to underperform in comparison to its neighbors.[26] According to Akamai, Belarus' average internet connection speed was 6.1 Mbps in the third quarter of 2015, compared to 3.73 Mbps during the same period in 2014.[27] Ookla ranked Belarus 52nd of 200 countries in its 2015 Household Download Net Index, with an average broadband download speed of 19.85 Mbps. The average broadband upload speed was 16.86 Mbps, which ranked 26th. The mobile download and upload speeds, 8.8 Mbps and 3.3 Mbps respectively, ranked 65th and 71st.[28]

The cost of broadband access via DSL and cable is generally tied to volume, reflecting the pricing structure that Beltelecom uses when selling bandwidth to downstream ISPs. Volume surcharges do not create a barrier for most users. Current prices for unlimited internet access from Beltelecom are approximately US$4–$20 per month for individuals, depending on the speed and volume of traffic [29]

Though internet access continues to be affordable in Belarus, prices for internet access grew as a percentage of Belarusians' household budgets. While Belarus generally ranks well in the CIS in regard to costs, internet access remained relatively expensive compared to European countries.[30] Nevertheless, prices do not generally constitute a barrier to ICT uptake in Belarus.[31]

While Belarus has two official languages—Belarusian and Russian—the majority f citizens use Russian in daily life. In fact, Russian-language broadcast, print, and online outlets dominate Belarus' media and information spheres. As a result, the Belarusian internet is dominated by sites based in Rus-

23 Steven Clark, "Belarusian communications satellite launched from China," *Spaceflight Now*, January 15, 2016, http://spaceflightno .com/2016/01/15/belarusian-communications-satellite-launched-from-china.

24 "Communications infrastructure in Belarus," Belarus.by: Official ebsite of the Republic of Belarus, http://www.belarus.by/en/business/business-environment.

25 "Belarus' external internet gateway dcreased by 160 Gbit/s since beginning of year" (in Russian), *Providers.by*, November 2, 2015, http://providers.by/2015/11/news/vneshnij-internet-shlyuz-belarusi-s-nachala-goda-umenshilsya-na-160-gbits. Even at 610 Gpbs, that would be a 15-fold boost in bandwidth since 2010. "Belarus reports 15-fold expansion in its international internet gateway since 2010," *TeleGeography*, October 8, 2010, https://www.telegeography.com/products/commsupdate/articles/2014/10/08/belarus-reports-15-fold-expansion-in-its-international-internet-gateway-since-2010.

26 Viktor Shkel, "Internet Quality in Belarus (Data as of Q1 2015)," *Business Data Processing*, http://businessdataprocessing.com/internet-quality-in-belarus-data-as-of-q1-2015.

27 Akamai, "State of the Internet" Map Visualization, https://www.stateoftheinternet.com/trends-visualizations-connectivity-global-heat-map-internet-speeds-broadband-adoption.html.

28 Ookla, "Net Global Index," May 2015. Ookla no longer maintains the *Net Global Index*.

29 While mobile phone and internet access prices in Belarusian rubles increased a number of times in 2015-2016, the amounts remained roughly the same in dollars due to Belarus' chronic inflation.

30 See Chapter Four, "Monitoring the price and affordability of ICTs" in the *ITU's Measuring the Information Society Report 2015*, http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf, pp. 93-144.

31 Belarus ranked 16th in the Fixed-telephone sub-basket, 53st in the Mobile-cellular sub-basket, 51th in the Fixed-broadband sub-basket, and 29th in Mobile-broadband prices. See Chapter Four, "Monitoring the price and affordability of ICTs" in the ITU's *Measuring the Information Society Report 2015*, http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf, pp. 93-144.

sia. Beltelecom reports that foreign websites make up 95 percent of online traffic in Belarus [32] Only two or three Belarusian sites are in the top 10 most popular internet sites in Belarus.[33]

By April 2015, almost 75 percent of Belarusian internet users were visiting social media sites.[34] VKontakte is used by about 2.5 million Belarusians a month, and Odnoklassniki is accessed by 1.1 million Belarusians monthly.[35] Facebook is less popular, with 780,000 Belarusian users in January 2016. Young people from 18 to 34 constitute the overwhelming number of social network users in Belarus.[36]

In November 2015, Decree No. 475 abolished the need to have a license from the Ministry of Information to offer Wi-Fi in restaurants, cafes, and other public venues. The decree came into effect on March 1, 2016.[37] However, in that same month, the State Telecommunications Inspectorate ruled that public transportation vehicles can only offer Wi-Fi with its authorization and in consultation with the Ministry of Defense.[38]

Restrictions on Connectivity

The Belarusian government has not imposed restrictions on ICT connectivity or access to particular social media or communication apps permanently or during specific e ents. However, the authorities possess this capability, since the backbone connection to the international internet is owned by the government.

The state-owned Beltelecom and the National Center for Traffic E change are the only entities permitted to handle connections with ISPs outside of Belarus. All commercial providers must purchase internet access from Beltelecom's Belpak gateway. In 2012, the Center replaced Beltelecom in providing access to the points of sharing national traffic (peering) [39] While the government does not limit the amount of bandwidth that access providers can supply, the fact that ISPs depend on Beltelecom allows the authorities to control access speeds for the entire country.

Launched in 1994, the Belarusian domain zone (.BY, often called the "BYnet"), had more than 124,000 registered domain names by February 2016;[40] more than half of these have been registered in the last three years. Since 2014, it has been one of the fastest growing country domain zones in Eu-

32 "Russian content cedes Positions in Belarus," *Belarusian Association of Journalists*, January 21, 2016, http://baj.by/en/content/russian-content-cedes-positions-belarus.

33 Ryhor Astapenia, "How Russian Culture and Media Shape Belarusian Politics," *Belarus Digest*, February 6, 2014, http://bit.ly/1GhMQXg; Gemius, *Online Landscape: Russian speaking markets*, June 2014, 6, http://bit.ly/1RMtFX0.

34 Mikhail Doroshevich, "Users of Social Media in Belarus and their Behavior," *Gemius*, July 1, 2015, http://www.slideshare.net/MikhailDoroshevich/doroshevich-01072015?related=1, p. 8.

35 VKontakte, "Belarus in VK," https://vk.com/doc7337161_437282008?hash=25ba20277cc167bb96, p. 3.

36 "Age groups of social media users," *Gemius Global*, May 11, 2015, https://www.gemius.com/all-reader-news/age-groups-of-social-media-users.html.

37 "Ministry of Information abolishes licenses for Wi-Fi in bars and restaurants" (in Russian), *Providers.by*, December 4, 2015, http://providers.by/2015/12/news/v-marte-2016-go-otmenyat-neobxodimost-imet-licenziyu-minsvyazi-na-organizaciyu-wi-fi_v-barax-i-restoranax.

38 "Documents from BelGIE and coordination with Ministry of Defense needed to install Wi-Fi in shuttles and taxies" (in Russian), *Providers.by*, October 28, 2015, http://providers.by/2015/10/news/dlya-ustanovki-wi-fi-v-ma shrutkax-i-taksi-neobxodimy-dokumenty-iz-belgie-i-soglasovanie-s-ministerstvom-oborony.

39 "National Center for Traffic E change replaced Beltelecom in providing peering services," [in Russian], *TechOnliner*, April 3, 2012, http://bit.ly/1GKgTIA.

40 See http://cctld.by/en/statistics.

rope.[41] According to legislation passed in 2010, all legal entities operating in the ".BY" domain must use Belarusian hosting services.

In 2014, ICANN approved Belarus' request for a Cyrillic domain .БЕЛ (.BEL) as an alternative national domain. As of February 2016, the .БЕЛ domain contained over 16,700 registered names.[42] In February 2016, the cost to register or renew a domain increased by 68 percent. Neither current owners nor new registrants were notified f the increase.[43]

ICT Market

The IT sector continued to develop strongly in Belarus.[44] The 2015 Global Innovation Index ranked Belarus 67th of 141 countries in terms of ICT development, including infrastructure, a slight improvement over the year before. In terms of ICT access and ICT use, Belarus improved, rising from 35th and 38th place in 2015, up from 45th and 44th place in 2014, respectively.[45] Nevertheless, the country's economic troubles hinder the development of the IT sector.[46]

The Ministry of Communications has issued 180 licenses for ISPs in Belarus; 65 were active in early 2016.[47] The number of licensed providers has declined since 2010.[48] There is competition between internet providers, but more than half the market is controlled by the state-owned Beltelecom.[49] The largest selection and best quality of internet access is available in Minsk, where some 37 companies offer access through ADSL, Ethernet, cable TV, and mobile networks; smaller cities have fewer options.[50]

Despite inflation and de aluation, prices for internet access in Belarus have remained relatively stable. One possible reason is Beltelecom's alleged practice of flooding the mar et with underpriced packages to reduce competition from private operators.[51] Google and other digital companies which generate significant online traffic also h e preferential agreements with Beltelecom, which allow it to engage in predatory pricing.[52]

41 See http://cctld.by/news/2015/the-bynet-21-fresh-stats.

42 See Official Si e of the Domain Zones .BY and .БЕЛ, http://cctld.by/statistics/stats-bel.

43 "Domains .BY and .БЕЛ rose to 252,000 rubles" (in Russian), *Providers.by*, February 3, 2016, http://providers.by/2016/02/news/domeny-by-i-bel-podorozhali-do-252-000-rublej.

44 Volha Charnysh, "Belarus–An Outsourcing Haven?", *BelarusDigest*, September 2, 2014, http://belarusdigest.com/story/belarus-outsourcing-haven-19134; Tatiana Kalinovskaya, "Programmers create unlikely IT boom in Belarus," *Phys.org*, December 9, 2015, http://phys.org/news/2015-12-programmers-boom-belarus.html; and, Viktor Shkel, "Belarus Hit the Top 10 Global Talent," *BDP*, August 17, 2015, http://businessdataprocessing.com/belarus-hit-the-top-10-global-talent.

45 See "The Global Innovation Index 2015" and "The Global Innovation Index 2014," Cornell, INSEAD and WIPO, Geneva, https://www.globalinnovationindex.org/userfiles/file eportpdf/gii-full-report-2015-v6.pdf (see p.173 for the Belarus country profile) and https://www.globalinnovationindex.org/userfiles/file eportpdf/GII-2014-v5.pdf.

46 "Digital government, digital economy in focus in Belarus in 2016-2022," National Legal Portal of the Republic of Belarus, November 3, 2015, http://law.by/main.aspx?guid=35783.

47 See "All providers," *Providers.by*, accessed February 15, 2016, http://providers.by/by-providers.

48 Mikhail Doroshevich and Marina Sokolova, "Internet: Infrastructure, users, regulation," *e-Belarus*, http://e-belarus.org/article/yearbook2014.html.

49 Anne Austin, Jonathan Barnard, and Nicola Hutcheon, "New Media Forecasts 2015, *ZenithOptimedia*, October 2015, http://www.zenithoptimedia.com/wp-content/uploads/2015/11/NewMediaForecasts2015_Report.pdf, p. 14.

50 See "By city," *Providers.by*, http://providers.by/by-providers/?by_cities.

51 Ibid.

52 Vladimir Volkov, "Google in Belarus Supports State Telecom Monopoly Against Fair Competition-and Its Own Principles," *Digital.Report*, March 1, 2016, https://digital.report/google-in-belarus-supports-state-telecom-monopoly.

Regulatory Bodies

There is no independent regulator overseeing ICTs in Belarus. There is strong state regulation and involvement in the telecommunications and media market. The Ministry of Communications founded Beltelecom in 1995 and continues to regulate the company, undermining regulatory independence. In addition, the Presidential Administration's Operations and Analysis Center (OAC), which was initially a subdivision of the State Security Committee (KGB), has the authority to oversee ISPs, conduct online surveillance, and manage Belarus' top-level domain (.By). Other governmental bodies with authority over this sector include the State Telecommunications Inspectorate, the State Control Committee, the KGB, and the Prosecutor General's Office.

Limits on Content

In the past year, the government has utilized the newly amended Media Law to restrict access to some political content online. The amended laws expand the state's powers to limit online content which falls within broad categories such as threatening national interests or promoting extremism. As the internet in Belarus is dominated by Russian outlets, Russian progovernment propaganda and trolls continue to distort the online media landscape. Meanwhile, independent Belarusian outlets struggle for resources, an issue exacerbated by Belarus' economic crisis.

Blocking and Filtering

In 2015-2016, the government began to utilize the recently amended Media Law to restrict access to websites without a court order. The authorities are empowered to block any site they deem to be problematic. Previously, blacklisted websites were restricted only in public institutions. While the lack of reliable statistics makes it difficult to compare, website administers and netizens report that blocking became a greater problem during the past year.

The amendments, passed in January 2015, treat online media as traditional media, permitting the Ministry of Information to issue warnings, suspend, and file closure suits against online outlets.[53] The Ministry can block access to sites if two warnings have been issued within 12 months, and the scope of reasons to issue warnings has been expanded. The Ministry can also order sites blocked without a warning for posts it deems illegal.[54] The types of information considered illegal has been expanded to include "information, the distribution of which can harm the national interests of the Republic of Belarus." This and other provisions are subject to broad interpretation and can be used to stifle critical media. Whereas it was previously the responsibility of courts to decide what internet posts were illegal, the amendments now empower officials to do so. There are no legal avenues to appeal the blocking of websites in Belarus. The amendments are seen by the Organization for Security and Co-

53 For a critical analysis of the amendments, see Andrei Bastunets, "Analysis of Amendments to Media Law," *BAJ*, January 22, 2015, http://bit.ly/1Le32bb.

54 The updated subparagraph 1.3 of Article 38 specifies information illegal for distribution and reads as follows, "information aimed at the propaganda of war, extremist activity or containing calls for such activity, pornography, violence and cruelty, as well as other information, the distribution of which can harm national interests of the Republic of Belarus or banned by this Law, and other legislative acts of the Republic of Belarus."

operation in Europe (OSCE) Representative on Freedom of the Media and other media rights experts as posing a major threat to free speech.[55]

Under the amended Media Law, a blacklist of websites is now maintained by the Telecommunications Ministry's State Inspectorate for Electronic Communication, which makes changes to the list on instructions from the Ministry of Information. Only government agencies and ISPs have access to the blacklist, which is to be reviewed daily. Any government body can add to the blacklist by informing the Ministry of Information about sites that, in its opinion, violate the law. A website can be blocked by a provider after 24 hours, while it may take the Ministry of Information up to a month to restore access to it once all violations are corrected. The blacklist of restricted websites and procedures for adding websites to it remains non-transparent. Experts note that the government's decisions are made arbitrarily, do not require judicial approval, and allow no course for appeal.[56]

In May 2015, the Ministry of Information began warning websites, including a number of political and news sources, that they were allegedly violating the amended Media Law. Freeregion.info, Radio Racyja, Tuzin.fm (a music portal), the website of the opposition United Civic Party, and the lifestyle website KYKY received letters indicating that their websites contained some unspecified "violations of the mass media legislation."[57]

The fi st official use f the amended Media Law took place on June 18, 2015, when the lifestyle website KYKY.org was blocked by the Ministry for Information without warning for distributing content harmful to the country's national interests.[58] According to the Ministry, certain articles contained "offensive" remarks about the celebration of Victory Day (May 9) and questioned the importance of the holiday, "thereby distorting the historical truth about the Great Patriotic War" (World War II). The Ministry also claimed that articles included profane language and offensive remarks about "representatives of certain social groups, ethnicities and religious denominations." Public access was restored in six days, after the controversial materials were removed (see Content Removal). Experts speculated that the blocking of KYKY might also have been a warning to other critical media ahead of the October 2015 presidential election.

Ruling No. 6/8, which laid out the mechanisms and procedures for restricting access to websites under the new law, came into force in February 2015.[59] According to the directive, sites will be blocked if they contain information about drug trafficking or other illegal info mation. Websites also may be blocked if their owners fail to correct violations of the Media Law as required by the authorities. The directive allows not only state agencies but also any individual to propose the blocking of specific websites. Tor and other circumvention tools can also be blocked under the directive.[60] To date, the

55 Organization for Security and Cooperation in Europe (OSCE), "New regulation and recent blockings threaten free speech on Internet in Belarus, says OSCE Representative," press release, December 22, 2014, http://bit.ly/1QAuUb4; Committee to Protect Journalists, "Belarus adopts restrictive media law amendments, blocks websites," December 23, 2014, https://cpj.org/x/5e76; Reporters Without Borders, "Belarusian authorities impose alarming Internet controls," May 19, 2015, http://bit.ly/1G9BWmW; Official ersion of amendments at: "Amendments to the Law on Media," [in Russian] December 21, 2014, http://bit.ly/1QAvqFT.

56 Tanya Korovenkova, "Edict No. 60 less restrictive than feared, but authorities can tighten screws," *BelaPAN*, July 1, 2013, http://bit.ly/1Le7Ddp.

57 "Information Ministry Targets Independent Websites," *BAJ*, May 15, 2015, http://old.baj.by/en/node/28691.

58 "Belarus Blocks Art, Lifestyle Website For 'Harming National Interests'", *Radio Free Europe/Radio Liberty*, June 18, 2015, http://www.rferl.org/content/belarus-art-lifestyle-website-harming-national-interests/27079737.html.

59 ПОСТАНОВЛЕНИЕ ОПЕРАТИВНО-АНАЛИТИЧЕСКОГО ЦЕНТРА ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ И МИНИСТЕРСТВА СВЯЗИ И ИНФОРМАТИЗАЦИИ РЕСПУБЛИКИ БЕЛАРУСЬ 19 февраля 2015 г. № 6/8, February 25, 2015, http://bit.ly/1VWX32N.

60 Ibid, http://bit.ly/1VWX32N.

government has not implemented this aspect of the Ruling, and circumvention tools remain generally accessible in Belarus.

According to the Ministry of Information, the government officially bloc ed access to 40 websites in 2015. Access to four of the sites was restored. The authorities blocked the sites for allegedly distributing extremist materials, advertising alcoholic beverages, selling drugs, using forbidden language, and promoting child pornography. The Ministry also issued 36 warnings to independent print media, most of which also have corresponding webpages and social media pages.[61] A minimum of four websites were also warned in 2015.[62] At least two have been warned in early 2016.[63]

The authorities increased their efforts to block, close, and regulate e-commerce sites, a practice that began in 2014. The Ministry of Trade reported that it had suspended the operations of 35 internet stores and fi e electronic trading platforms for various irregularities in 2015. It also drew up as many as 130 claims against online businesses and imposed penalties totaling about BYR 50 million ($2,830) in the fi st nine months, 2.5 times more than in the same period of 2014.[64] One internet expert noted that the Ministry of Trade has assumed the functions of an economic and political censor.[65]

Due to its diplomatic and financial in erest in reestablishing relations with the EU, the Belarusian government has been relatively restrained in using the new legislation to repress independent news and information websites in the past year. However, there are disturbing indications that this may change. Recently, Belarusian officials ha e declared that the government should tighten control of the internet. In December 2015, Minister of Education Zhuravkov stated: "You see now on the internet, in social networks, a complete orgy. They should be regulated."[66] In February 2016, Pavel Yakubovich, the editor in chief of the largest government newspaper *Sovetskaya Belorussia* (Soviet Belarus), warned about the internet's ability to "split society." He called for "improving" Belarus' Media Law to prevent the "degradation of minds" and "confrontational clashes."[67] Henadz Davydzka, chairman of the National State TV and Radio Company, declared that "Anonymity on the Internet must be banned. It is not the fi st time when we are discussing that. I am a supporter of strict measures."[68]

As in the past, basic techniques such as IP fil ering and disabling DNS records were employed. It appears that the authorities do not perform regular or automated monitoring of the accessibility of banned websites, and it generally takes several hours for a new IP address to be blocked. To date, no

61 "Situation in Belarusian Mass Media Field in 2015 (Short Summary)," Mass Media in Belarus Review #6 (46), *Belarusian Association of Journalists*, February 1, 2016, http://baj.by/en/analytics/e-newsletter-mass-media-belarus-bulletin-646-brief-annual-review.

62 "Information Ministry starts blocking websites for criticism of authorities," *Belarus in Focus*, June 23, 2015, http://belarusinfocus.info/p/6733.

63 "Two Websites Warned by the Information Ministry," *Belarusian Association of Journalists*, March 3, 2016, http://baj.by/en/content/two-websites-warned-information-ministry.

64 Maryna Nosava, "Trade ministry has suspended operation of 35 Internet stores and fi e electronic trading platforms this year, deputy minister says," *BelaPAN*, December 14, 2015, http://en.belapan.by/archive/2015/12/14/en_21451214H.

65 Ihar Karnej, "'Clearing' internet-shops: Nuclear bomb dropped on a single house," [in Russian] *Svaboda*, January 10, 2015, http://bit.ly/1MtRQVI.

66 Mikail Zhurakov, "Democracy in the social networks should not be associated with complete anarchy," *BelTA*, December 14, 2015, http://www.belta.by/opinions/view/demokratija-v-sotssetjah-ne-dolzhna-assotsiirovatsja-s-polnoj-anarhiej-4541.

67 Anastasiya Salanovich, "Pro-government newspaper's chief editor calls for closer supervision over Internet," *BelaPAN*, February 4, 2016, http://en.belapan.by/archive/2016/02/04/en_22230204H.

68 "Belarusian TV Head Demands Outlawing Anonymity On Internet," *Charter 97*, February 8, 2016, https://charter97.org/en/news/2016/2/8/190305.

documented instances of deep-pocket inspection (DPI) fil ering have been recorded. However, the Belarusian government is reported to be in possession of equipment and software necessary for DPI.[69]

Content Removal

Until this past year, content removal has not been broadly used by the Belarusian authorities. However, the 2015 amendments permit the Ministry of Information to demand the deletion of information that the authorities deem illegal within broad categories, such as content related to extremism or considered harmful to national interests.[70] The amendments require the owners of websites to remove any online report disputed by any person and to post a refutation in its place. If the publishers do not comply, their sites can be blocked. Website owners are held liable for any illegal content posted on their sites, and can also be punished for abusive or "incorrect" comments left on message boards.[71] These decisions are no longer made by courts but by executive bodies, with no dispute mechanism or right to appeal. Even before the new amendments, online publishers threatened with a claim of defamation or harm to reputation often chose to preemptively remove controversial materials from their websites.

In June 2015, the content removal provision of the new amendments was used for the fi st time. The Ministry of Information blocked the internet magazine KYKY.org without warning (see Blocking and Filtering).

In addition, the Ministry told the website to remove four articles containing "forbidden vocabulary, disparaging, and sometimes insulting remarks against members of certain social groups, nationalities, and religions."[72] Six days after the administrators complied, access to the website was restored.[73]

In November 2015, the UN Special Rapporteur on human rights in Belarus noted that "critical opinion and fact-finding a e curtailed by the criminalization of content that is deemed 'harmful for the State'." The Special Rapporteur noted that, until last year, Belarusians had benefi ed from free expression on the Internet. However, the recent amendments put practically all internet-based forms of expression under direct government control, authorizing a long list of authorities to remove unwanted content.[74]

Media, Diversity, and Content Manipulation

Destabilizing developments in the region, including Russia's propaganda campaign following its invasion of Ukraine, an economic crisis in both Belarus and Russia, and the 2015 presidential election

69 Mikhail Doroshevich and Marina Sokolova, "Internet Development and Usage," ed. Anatoly Pankovsky and Valeria Kostyugova, *Belarusian Yearbook 2012*, Minsk, 2013, http://bit.ly/1hJ9XhL, p. 174.

70 "Lozovik: Some websites are set up to flood In ernet with negative information," *BelTa,* December 17, 2014, http://bit.ly/1OIM0V6.

71 Anastasiya Salanovich, "Minister warns of crackdown on websites for "incorrect" comments on message boards."

72 "Report on the state of media in Belarus and other Eastern Partnership Countries issued now," *Belarusian Association of Journalists*, Information Policy, December 15, 2015, http://www.i-policy.org/2015/12/report-on-the-state-of-media-in-belarus-and-other-eastern-partnership-countries-issued-now.html.

73 Alyaksey Areshka, "Blocked website`s team promises to delete objectionable content," *BelaPAN*, June 18, 2015, http://en.belapan.by/archive/2015/06/18/en_19440618H.

74 "UN rights expert urges "broad reform" of oppressive media governance in Belarus," *UN News Centre*, November 6, 2015, http://www.un.org/apps/news/story.asp?NewsID=52486#.WAPJPzU9Xic.

in Belarus, have had an adverse effect on the online media landscape. With the internet serving as an important source of information for Belarusians, the government has stepped up its efforts to influence and manipula e online content. The authorities also continued to use preferential subsidies to favor progovernment media outlets and accreditation requirements to punish freelance journalists. These measures were not always successful, as more people turned to independent online sources in 2015 and 2016, finding them mo e credible than state-run media.

Under pressure abroad and at home, the Belarusian authorities attempted to limit independent views and criticism by independent and online media. In his 2015 State of the Nation speech, President Lukashenka said that the government must take a "fresh look" at protecting the information space in order to shield citizens from manipulation.[75] Minister of Information Ananich called on the media to "resist speculation on economic difficulties [and rather] focus the audience s attention on the achievements of Belarus". In her view, information must not only be accurate, but also must "promote the development of society and the state." Ananich criticized the internet's "destructive component" and accused unnamed media outlets of magnifying petty problems to stir up society.[76]

Through selective use of oppressive laws, threats, and force, the government actively promoted self-censorship, which has long been a pervasive phenomenon for web-based media. In particular, the new amendments to the Media Law have had a chilling effect on journalists and editors. According to the Belarusian Association of Journalists, "the authorities want to force mass media into self-censorship, all the time considering which materials they can or cannot publish."[77] In 2015, an increase in official wa nings for spurious reasons reinforced self-censorship prior to the October presidential election.[78] Selective official and un fficial blocking also boos ed self-censorship.[79] For example, media experts believe the June 2015 blocking of KYKY.org (see Blocking and Filtering and Content Removal) was a warning for other online media, designed to encourage self-censorship.[80]

Trolling is one of the government's less direct methods of manipulating online content. Since the 2010-2011 political and economic protests, the number of trolls and paid commentators has significantly increased on independent Belarusian websites. In the past year, trolls were employed to reassure readers that the economic situation was under control and that outsiders were to blame for the crisis. Trolls also were asked to criticize opposition protests and positively rate Lukashenka's election platform.[81] As more Belarusian internet users move to social networks, trolls have also migrated to popular online communities. While it is difficult o prove that trolls are being paid for their services,

75 Alexander Lukashenka, "Address to the Belarusian People and the National Assembly," April 29, 2015, http://president.gov.by/ru/news_ru/view/obraschenie-s-poslaniem-k-belorusskomu-narodu-i-natsionalnomu-sobraniju-11301.

76 Tanya Korovenkova, "Opposed to media freedom, officials could still ta e measures to protect Belarus from Russia's bad influence, *BelaPAN*, June 16, 2016, http://en.belapan.by/archive/2015/06/16/en_783719_783720; Dzmitry Ulasaw, "Information minister concerned about growing role of online media," *BelaPAN*, February 8, 2016, http://en.belapan.by/archive/2016/02/08/en_08021735b; "Belarusian propaganda is not as destructive as Russian, it's just miserable," *Mediakritika*, February 4, 2016, http://mediakritika.by/article/3623/belaruskaya-prapaganda-ne-takaya-termayadzernaya-yak-rasiyskaya-yana-prosta-ubogaya.

77 "The authorities want to force journalists into self-censorship – Bastunets," [in Belarusian] *Svaboda*, February 15, 2015, http://bit.ly/1Pxbntx.

78 "Report on the state of media in Belarus and other Eastern Partnership Countries issued now," Belarusian Association of Journalists, *Information Policy*, December 15, 2015, http://www.i-policy.org/2015/12/report-on-the-state-of-media-in-belarus-and-other-eastern-partnership-countries-issued-now.html.

79 "Information Ministry starts blocking websites for criticism of authorities," *Belarus in Focus*, June 6, 2015, http://belarusinfocus.info/p/6733.

80 Zahar Shcherbakov, "The independent media in Belarus. The Number 1 threat changes its face" (in Russian), *Naviny*, January 24, 2016, http://naviny.by/rubrics/society/2016/01/24/ic_articles_116_190797.

81 Sergey Kozlovsky, "Belarus Catches Up to Russia With Its Own Pro-government 'Troll Factory'," *Global Voices*, October 10, 2015, https://globalvoices.org/2015/10/10/belarus-catches-up-to-russia-with-its-own-pro-government-troll-factory.

especially by the government, a level of coordination behind their activities is evident. They are constantly present on popular and influential in ernet forums and social networks, immediately react to new developments, and frequently work in teams.[82] In 2015, evidence surfaced that members of the state-supported Belarusian Union of Youth were being employed as trolls.[83] Bad behavior by regular internet users also remains a challenge; online rudeness and vulgarity often render discussions on forums more divisive.[84]

Russian propaganda continues to play a divisive role in Belarus, where the Russian language and Russian outlets dominate the media scene. As a result, Belarusians are heavily influenced by Russian media content.[85] Russian propaganda encourages the view that Belarusians are not a separate nation but are part of the "Russian world," and the idea is influential in Belarus—acco ding to a 2015 poll, roughly a third of Belarusians believe in Putin's idea of a "Russian world".[86] Though traditionally close to Russia, President Lukashenka has come to fear an aggressive Kremlin in the wake of its invasion of Ukraine. Russia's economic problems also have made it less attractive as a source of support for Belarus' ailing economy, prompting Lukashenka to encourage more national sentiment at home and improved relations with the West.

The response from the Kremlin and Russian nationalists has been harsh. Russian media outlets, including websites, increased their pro-Russian propaganda, and unleashed a "black propaganda" campaign against both state and non-state actors in Belarus. In many ways, the Russian operation resembles the trolling campaign organized against westward-leaning Ukraine. Russian websites have accused Lukashenka of being disloyal, too independent, and pro-Western. Long critical of the national symbols, culture, and history embraced by the Belarusian democratic opposition, Russian media now allege that the Belarusian authorities and their opponents have allied in promoting "dangerous" nationalism and "Russophobia".[87]

This situation has put Lukashenka in a difficult position. The go ernment restricts independent media, but does not curb Russian propaganda. It sees the former as a threat and not a part of the solution to the peril posed by the latter.

Russian trolls have become more active on Belarusian websites and social media pages, and purportedly outnumber Belarusian trolls. These trolls not only attack pro-democratic online forums and activities but seek to influence vie ers and manipulate content on Russian-Belarusian issues.[88] In February 2016, for example, Russian trolls targeted the *Nasha Niva* portal during a live report on an entrepreneurs' strike, which they thought was taking place in Ukraine. Upon figuring out that the

82 "Yuri Zisser: Popularity of the opposition websites grows thanks to censorship," [in Russian] *Eurobelarus*, October 10, 2013, http://bit.ly/1kakUei.

83 "Factory of BRYU trolls," *Charter 97*, September 23, 2015, https://charter97.org/en/news/2015/9/23/170244.

84 Volha Prudnikava, "Bynet: rudeness is an issue," *BelaPAN*, August 8, 2012, http://bit.ly/1X9BQQ5.

85 Ryhor Astapenia, "How Russian Culture And Media Shape Belarusian Politics."

86 "The Most Important Results of the Public Opinion Poll in December 2015," *IISEPS*, December 29, 2015, http://www.iiseps.org/?p=3865&lang=en.

87 Alexander Cajcyc, "Russian Media Attack Belarus: Minsk Remains on the Kremlin Radar," *BelarusDigest*, February 2, 2016, http://belarusdigest.com/story/russian-media-attack-belarus-minsk-remains-kremlin-radar-24482.

88 "KGB hires trolls urgently?" *Charter97*, April 11, 2012, http://bit.ly/1LSsgJn; "Troll from Olgino: They would mock Lukashenka as hard as possible," *Charter97,* September 9, 2014, http://bit.ly/1jsJbfm; "Yuri Zisser: Popularity of the opposition websites grows thanks to censorship," [in Russian] *Eurobelarus*, October 10, 2013, http://bit.ly/1kakUei.

strike was taking place in Belarus, they swiftly switched to criticizing the protestors and praising Lukashenka as a great leader of all Slavs.[89]

In 2015-2016, the government increased its use of administrative laws to restrict non-state journalists' ability to work, enforcing stringent requirements for accreditation.[90] Journalists, including those publishing online, are not allowed to work professionally if not accredited by the state, making it impossible for freelancers to work legally.[91] In the past year, many freelance journalists were harassed and prosecuted by the authorities for not possessing appropriate accreditation (see Violations of User Rights).

While Belarus' 2009 Law on Information, Informatization and Protection of Information guarantees access to, and the distribution of, information of interest to the public, the government routinely restricts information from independent journalists and the media, including online websites. Some 60 state bodies can classify their information as secret, state officials cannot speak with jou nalists without the approval of their superiors, and media can only gain information from official p ess services or state ideological departments.[92] Since 2003, the government has operated ideological structures in all state enterprises and organizations.

The government controls all broadcast media and more than 600 newspapers and information websites. Since May 2015, the government has been operating the site, *Belsmi*, which promotes state-controlled local media and strives to create a favorable image of the country. Experts have criticized the site for its one-sided content.[93]

The government also determines online content through significant financial supp t to pro-government media outlets. The country's worsening economic conditions make this state support even more influential. While the otal funding provided to pro-government online media is unknown, the 2015 state budget allocated EUR 60 million (US$73 million)—an increase of approximately EUR 8 million over 2014—to support all state-run media, though the budget for 2016 fell to about EUR 45 million.[94] These funds are used to "collect, prepare and disseminate state orders on official info mation."[95] As Belarus faced its worst crash in 15 years, the authorities indicated the state would provide additional financial suppo t for 26 government-controlled newspapers and magazines, and presumably their websites, in 2016.[96] The state also provides preferential advertising (70 percent of the economy is in state hands) and subsidizes rent and other operating costs.

89 "Russian trolls massively commented on NN.by video in YouTube," *Nasha Niva*, February 22, 2016, http://nn.by/?c=ar&i=165612.

90 The Law on Mass Media envisages an authorization-based procedure of accreditation. Moreover, it does not allow the possibility to appeal against a refusal of accreditation. A journalist is forbidden to carry out professional activities, if he or she is not accredited. "Comments on Suggestions to Media Law," *BAJ*, January 24, 2013, http://old.baj.by/en/node/19255.

91 "Comments on Suggestions to Media Law," *BAJ*, January 24, 2013, http://old.baj.by/en/node/19255.

92 IREX, "Belarus," in *Europe & Eurasia Media Sustainability Index 2013*, 182, http://bit.ly/1LoPZlh; IREX, "Belarus," in *Europe & Eurasia Media Sustainability Index 2015,* http://bit.ly/1NgcjA5.

93 Aliaksandr Klaskowski, "Authorities launch official media si e, keep independent media under thumb," *BelaPAN*, May 7, 2015, http://bit.ly/1OJe6j2.

94 "Draft budget 2016: around 45 million euros on state media" (in Russian), *Belarusian Association of Journalists*, December 28, 2015, http://baj.by/ru/content/proekt-byudzheta-2016-okolo-45-millionov-evro-na-gosudarstvennye-smi.

95 "Mass Media Week in Belarus," *BAJ*, December 12-22, 2013, http://bit.ly/1RfkAoI; "Figures of the year," *BAJ*, January 3, 2015, http://baj.by/en/analytics/figu es-year.

96 Alyaksey Alyaksandraw, "Government to provide financial assistance o 26 print media outlets in 2016,"*BelaPAN*, http://en.belapan.by/archive/2015/11/24/en_24111451b.

In contrast, non-state media receive no government subsidies and suffer from a constant lack of funding. The government employs direct and indirect economic pressure to limit financial suppo t for free media, including independent online media outlets, making it nearly impossible for these sites to be profitable. As one expe t put it, "The inefficient economy captained by big sta e-owned businesses cannot create decent conditions for the development of media."[97] Forced to operate in semi-underground conditions and facing constant pressure, independent online media and opposition sites are unable to monetize their growing audiences and popularity. Most independent news websites are at an economic disadvantage because state and private companies are afraid to advertise on them. There have also been cases when foreign companies, especially those cooperating with state agencies, have avoided placing ads on independent sites due to political concerns. Additionally, restrictive amendments to the Law on Public Associations and the Criminal Code that were passed secretly in 2011 made it a criminal offense for NGOs to receive foreign funding. Since most non-state online outlets are run as NGOs, the amendments pose a direct threat to the viability of Belarusian independent media.[98] These challenges are compounded by Belarus' worsening economic problems. Internet advertising fell by 15 percent in 2015.[99]

Despite two decades of autocratic government and one of Europe's most challenging media landscapes, Belarus continues to have a vibrant and diverse online presence. In 2015-2016, greater numbers of Belarusians viewed news and information from independent online sources because they found them to be more credible than the government's version. The vast majority of the top 50 news and information websites continue to be either independent or opposition run.[100] According to a September 2015 poll, more Belarusians received information about the October presidential election from independent than government online media (16 percent compared to 13 percent). Due to the government's inability to deal with the country's economic crisis, trust in virtually all state institutions – including state media[101] – decreased in 2015-16.[102] As one expert website noted, the state and its ideologues are losing the battle to independent media, despite the disparity in funding and restrictive laws.[103]

In the past year, social networks and blogs continued to grow as important sources of news, driven by a desire for objective information regarding Belarus' political and economic challenges and the conflict in neighboring Ukraine. In Belarus, social media plays a mo e important role as a source of news and information than as a driver of traffic o news and information websites.[104] Almost a quarter of respondents to a September 2015 poll received information about the October presidential election from social networks and blogs.[105]

97 IREX, "Europe and Eurasia Media Sustainability Index 2015-Belarus," https://www.irex.org/sites/default/files/2015-msi_belarus.pdf, p. 12.

98 Human Rights Watch, "Belarus: Open Joint NGO Letter to the Parliament of Belarus," October 20, 2011, http://bit.ly/1KdT1H4.

99 "Internet advertising market in Belarus by the end of 2015 will be about $18 million," *BelTA*, December 14, 2015, http://www.belta.by/economics/view/rynok-internet-reklamy-v-belarusi-po-itogam-2015-goda-sostavit-okolo-18-mln-174020-2015.

100 Akavita internet ranking site, accessed February 25, 2016, http://bit.ly/1LoRJe0.

101 Sergei Nikoliuk, "The country under dark shadows," *Belrynok*, April 12, 2016, http://www.belrynok.by/ru/page/column/2922.

102 Independent Institute of Socioeconomic and Political Studies, "The most important results of the public opinion poll in December 2015, http://www.iiseps.org/?p=3865&lang=en.

103 "Belarusian ideological workers are preparing for presidential campaign," *Belarus in Focus*, June 30, 2015, http://belarusinfocus.info/p/6742.

104 Pavluk Bykovsky, "Social networks give way to other traffic channels for Belarusian media" *Belarusian Association of Journalists*, February 18, 2016, http://baj.by/be/analytics/sacsetki-sastupayuc-inshym-kanalam-trafiku-u-belaruskih-medyy .

105 September 2015 monitoring, Nowak.

Comparative analysis of the media communities on popular social networks demonstrate that information posted and shared by independent media is much more in demand than content published by state media. Links from the social network accounts of independent media are actively clicked, shared, and discussed by users, while the social network accounts of the state media are lifeless.[106] Progovernment websites have few readers, and state officials do not use social net orks.[107] The ten most-visited Facebook pages of media outlets in Belarus are dominated by independent or opposition news and information sources.[108]

Belarus has a vibrant blogosphere due to government restrictions over traditional media. For independent-minded commentators, blogs serve as an alternative tool for disseminating uncensored information and fostering discussion on social, political and economic issues. The most popular Belarus blogs have over 10,000 followers,[109] which is more than the circulation of many independent newspapers. In the last year, microblogs on Twitter have become trendy; the most popular have 40,000 to 100,000 followers. Leading independent media figu es and outlets have from 44,000 to 164,000 followers.[110] No government figu es or outlets appear on these rankings.

Websites such as those of the Belarusian Association of Journalists (Baj.by) and Viasna Human Rights Center (Spring96.org) also seek to hold Belarus to its domestic and international human rights obligations. The country's constant economic crisis has stimulated more online initiatives designed to foster greater economic transparency and accountability. The best known is the *Koshturada* (Price of the State) website, which monitors budgetary expenditures.

Because of government repression, many political, civic and media activists have chosen or been forced to emigrate over the last two decades. As a result, the editorial offices f some of Belarus' most popular and influential ebsites are based outside of the country: in Poland (*Charter97*, Euroradio.fm), Ukraine (*Belaruspartisan*), and the Czech Republic (*Svaboda*). Nevertheless, the vast majority of these websites' viewers and reporters are based in Belarus.

In past years, websites related to the LGBTI (lesbian, gay, bisexual, transgender, and intersex) community have been targeted by the government. Gaybelarus.by, the online human rights project overseen by Belarusian LGBTI groups, has been intermittently blocked by the government since 2013. Rather than trying to circumvent the blocking of the old website, the administrators created a new portal, Yag ("Berry"), in July 2015.

Digital Activism

As more Belarusians turn to the internet for news and information, it has also grown as a tool for activism. Online activism proved to be particularly significant during the 2015 p esidential election, during which the crowdmapping platform Electby.org received over 1,300 reports about election violations from observers around the country, twice as many as in 2010. The organizers coordinated

106 BAJ, "Independent media in Belarus: Achievements, challenges and perspectives," November 23, 2013.

107 Artyom Shraibman, "Authorities control but do not gag Internet," *BelaPAN*, February 8, 2013, http://bit.ly/1Rfn3Qd; Pauliuk Bykouski, "Government Websites a Decade Behind," [in Belarusian] *Tut i Ciaper*, January 21, 2013, http://bit.ly/1GhWbP2.

108 Socialbakers, "Facebook stats – media in Belarus," http://www.socialbakers.com/statistics/facebook/pages/total/belarus/media, accessed February 27, 2016.

109 The First Rating of Belarusian Blogs, accessed March 23, 2015 http://ratings.by/?sort=readers; LiveJournal, "User ratings," http://bit.ly/1PmKJEJ.

110 Twitter Counter, "Top 100 Followers in Belarus," http://twittercounter.com/pages/100/belarus?utm_expid=102679131-70.Cf2Z6uGtR42NAFBYKQT74A.0&utm_referrer=http%3A%2F%2Ftwittercounter.com%2Fpages%2F100, accessed February 2016.

with monitoring groups to verify most of the reports.[111] Taking advantage of the growth of smartphones, civic observers and digital activists worked together to develop Belarus' first mobile application, "Vochy" (Eyes), to collect reports for the Electby map.[112] Launched two weeks before Election Day, the app drew the media's attention and was downloaded by almost 1,500 users. The creators said they would improve the app for the September 2016 parliamentary elections.

Over the past year the number of citizen petitions to state bodies increased significantly. According to the Law on Citizens' Appeals, state institutions are obliged to provide written responses to electronic appeals. The Belarusian petition platform Zvarot.by has been a pioneer in this field. In 2015, the site submitted over 5,700 individual and collective appeals to various state institutions, compared to 2,500 in 2014. In January 2016 alone, Zvarot.by submitted more than 3,500 civil society campaign petitions. While the state's responses tend to be negative or formal, several campaigns led to changes in legislation and policies. In one example, officials ceased harassing to human rights defenders who were regularly searched when crossing the border. In some cases, thanks to the petition campaigns and follow-up activities, joint working groups were created at state institutions. Zavrot.by and similar platforms, such as Petitions.by (*Удобный город* /Comfortable City) and *Одно Окно Онлайн* (One Window Online)—both launched in 2015—foster better communication and interaction between citizens and state institutions, which otherwise remain closed to and isolated from the public.[113]

Other online campaigns and initiatives started by citizens and civil society organizations generated significant engagement, often leading to offline action:

- In August 2015, Facebook activists launched the solidarity campaign #Sky4Statkevich, calling for people to take selfies outside to share their freedom with Mikola Statkevich, an opposition candidate in the 2010 presidential election and a political prisoner as he celebrated another birthday in jail.

- In September 2015, a campaign against the government's plan to allow a Russian military base in Belarus was launched on Twitter and Facebook. Its #NoRussianBaseinBelarus became the year's most popular hashtag, and was used to organize a series of street protests.

- In October 2015, a virtual flash mob was launched through social networks in support of four students who were expelled from a military school for posting a photo of themselves wearing tee shirts with a national symbol underneath their uniforms in a popular patriotic community in Vkontakte (see Violations of User Rights). Hundreds of Belarusians posted selfies with similar "Pahonia" tee shirts on social media. Independent media also put pressure on the school's administration, which reinstated the students, a decision likely influenced by the social media campaign.[114]

- In November 2015, students at Belarusian State University started a campaign on Vkontakte

111 "Chronicling violations for the civic platform observing the 2015 elections," *Elect.by*, November 12, 2015, http://2015.electby.org/report/Electby_Report_2015_BY.htm.

112 Tetyana Lokot, "New Mobile App Helps Belarusians to Keep an Eye on Violations in Presidential Election," *Global Voices*, September 21, 2015, https://globalvoices.org/2015/09/21/new-mobile-app-helps-belarusians-to-keep-an-eye-on-violations-in-presidential-election.

113 "Head of Petitions.by project: Belarusians prefer to complain to each other in kitchens. But the situation is changing," *Naviny*, January 30, 2016, http://naviny.by/rubrics/society/2016/01/30/ic_articles_116_190865.

114 "Public campaign on social networks prompted authorities to soften repressions," *Belarus in Focus*, October 27, 2015, http://belarusinfocus.info/p/7100.

and Facebook, against fees for repeat exams introduced by the university administration. The virtual protest led to the first offline student demonstrations in recent years. Despite threats from the university authorities, student activists continue their online and offline campaign.[115]

- In December 2015, when state TV ignored the ceremony at which the pro-opposition Belarusian writer Svetlana Alexievich received the Nobel Prize for Literature, Belarusian civil society self-organized a *Nobel Razem* (Nobel Together) campaign through social networks, gathering in cafes, galleries, and bookstores to watch the ceremony broadcast online. Facebook was used to organize a public meeting with Alexievich at Minsk International Airport upon her return from Stockholm.[116]

- Three crowdfunding platforms emerged in 2015 as success stories: *Talaka.by* platform, *Ulej.by* (Beehive) by Belgasprombank, and *MaeSens.by* (Makes Sense). Local crowdfunding platforms first appeared in 2011, it has taken time to adapt them to Belarusian conditions.[117] In June 2015, the first successful crowdfunding campaign on Talaka.by met its goal. Project Peppa Pig aimed to develop a Belarusian language version of the well-known British cartoon. By the end of 2015, thousands of citizens had donated more than BYR 3 billion rubles ($140,000) to the sites,[118] a significant amount by Belarusian standards.

Violations of User Rights

While detentions of online journalists and social media users were rare in the past year, authorities have punished independent freelance web journalists through administrative proceedings and penalties. Technical attacks against opposition and independent outlets continue to take down websites during strategic periods, often for days at a time. Meanwhile, the government continues to boost its capacity for online surveillance, acquiring technology from Chinese vendors to conduct in-depth analysis of activity online.

Legal Environment

While the rights to freedom of expression and information are guaranteed by the Belarusian constitution, they remain severely restricted and violated in practice. Since 2007, the government has enacted a series of repressive laws to stifle critical voices online. The 2015 amendments to the 2008 Media Law extended the government's restrictive laws against independent print media to cover the online sphere (see Blocking and Filtering). In January 2015, amendments to Articles 188, 361, and 367 of the Criminal Code also came into force. These amendments specifically made information distributed via the internet subject to criminal penalties for defamation, defamation of the president,

115 "Students protesting against paid repeat exams," *Novy Chas*, December 2, 2015, http://novychas.by/hramadstva/studenty_pratestujucj_supracj

116 Pavel Ros, "How Facebook affects the lives of Belarusians" (in Russian) *Salidarnast*, February 4, 2016, http://gazetaby.com/cont/art.php?sn_nid=108915.

117 ODB Brussels, "How Does Fundraising and Crowdfunding Work in Belarus?" October 2, 2015, http://odb-office.eu_capacity-building_/trainings/how-does-fundraising-and-crowdfunding-work-belarus#sthash.G0qhI5b8.dpuf.

118 Pavluk Bykovsky, "Crowdfunding: the right to choose the future" (in Russian), *Direktor*, No. 1 (199), January 2016, http://director.by/index.php/arhiv-nomerov/-2016/163--2016/4529-2016-02-12-08-05-04.html. See also *The 2015 CSO Sustainability Index for Central and Eastern Europe and Eurasia*, USAID, https://www.usaid.gov/sites/default/files/documents/1861_EuropeEurasia_CSOSIReport_2015.pdf#page=51, p. 47.

and threats to national security.[119]

Prosecutions and Detentions for Online Activities

Within the past year, authorities have ramped up harassment and intimidation against Belarusian journalists working for foreign media without accreditation. Between June 2015 and May 2016, 25 legal cases were launched against freelance journalists resulting in fines totaling more than $8,000.[120] Journalists are charged with the "illegal production and distribution of information" online under Article 22.9 of the Administrative Code. In particular, the government is pursuing Belarusian journalists cooperating with Belsat and Radio Racyja, Poland-based online media outlets reporting on Belarus. The campaign targets journalists in the country's regions, which are generally more conservative and quick to punish independent voices for fear of spotlighting local social or economic problems.[121] Some journalists have been prosecuted multiple times. Freelance journalist Kastus Zhukouski from Homel, whose video reports on social and economic issues appear on YouTube and are often reposted by Belsat, has been convicted 11 times and fined over $3,000 since April 2015.[122] The campaign paused during the presidential campaign in fall 2015, possibly in an effort to appease the international community, but new charges were brought beginning in January 2016.[123]

The Belarusian Association of Journalists (BAJ) has condemned the government's persecution of freelancers. It has pointed out that the legal provision under which the freelancers are being charged is applicable to media organizations, not to individual journalists. Furthermore, the prosecution of freelancers violates both Belarus' constitution and its international obligations.[124] The OSCE and other international organizations defending freedom of expression have denounced the campaign. In December 2015, the UN Human Rights Committee agreed for the first time to consider a complaint regarding a 2014 fine for violating Article 22.9.[125]

BAJ has appealed repeatedly to the authorities to codify the status of freelancer in the Media Law, but the Parliament rejected its proposals. In early August 2015, President Lukashenka publicly acknowledged the punishments against journalists as inappropriate and promised to resolve the problem.[126] In a promising development, draft reforms to the Administrative Code, which include a proposal to remove the prosecution of journalists under Article 22.9, were published on the website of the Ministry of Interior in January 2016.[127] On February 5, the Homel district court dismissed a

119 See, ЗАКОН РЕСПУБЛИКИ БЕЛАРУСЬ 5 января 2015 (Law of the Republic of Belarus, January 5, 2015) г. № 241-З, http://bit.ly/1PmNK7T.

120 For a list of the cases, see "Fines to Journalists for Violating Article 22.9 of the Administrative Code," *BAJ*, https://baj.by/en/analytics/fines-journalists-violating-article-229-administrative-code-chart-updated, accessed August 19, 2016.

121 Syarhey Karalevich, "Freelance journalist in Vitsyebsk region sentenced to fine for cooperation with foreign media outlets without accreditation," *BelaPAN*, July 29, 2015, http://en.belapan.com/archive/2015/07/29/en_17440729m.

122 "Freelance Journalist Zhukouski: 'Stupidity which became the norm'" (in Belarusian), *Radio Liberty*, February 1, 2016, http://www.svaboda.org/content/article/27522875.html.

123 Tatiana Korovenkova, "Tightening the Screws on Belarus' Media Sphere," *Naviny*, February 1, 2016, http://naviny.by/rubrics/society/2016/02/01/ic_articles_116_190871.

124 "BAJ protests against prosecution of journalists for contribution to foreign mass media," *Eurobelarus*, September 30, 2014, http://bit.ly/1G9XPlT.

125 Uladzimir Laptsevich, "UN Human Rights Committee to consider Belarusian freelance journalist's complaint over fine" *BelaPAN*, February 3, 2016, http://en.belapan.by/archive/2016/02/03/en_21460203H.

126 Alyaksey Alyaksandraw, "Two freelance journalists in Hrodna sentenced to fines for working for foreign media outlet without accreditation," *BelaPAN*, August 19, 2015, http://en.belapan.by/archive/2015/08/19/en_16430819.

127 Ministry of Internal Affairs, "Let's improve the law together: citizens are invited for an open discussion," January 12, 2016, http://mvd.gov.by/main.aspx?guid=303683.

charge against another freelancer, Larysa Shchyrakova, who had been convicted three times under Article 22.9. This was the fi st example in which an administrative case against a freelance journalist was halted.[128] On February 25, however, the Zhlobin district court imposed another fine on Kastus Zhukouski for allegedly violating the same article.

In January 2016, Belarusian authorities detained 26-year-old blogger Eduard Palychs, also known under his pseudonym Jhon Silver, the creator of the anti-government website 1863x.com, known for its sharp political commentary. Authorities charged Palychs with inciting racial, national, or religious hatred as well as distributing pornographic material based on content published on his website, charges which experts said were baseless.[129] He faces up to fi e years of imprisonment.[130] Palychs had been previously detained by police and confined o a psychiatric hospital in 2015. After this incident, he had tried fleeing o Ukraine, but was apprehended in Russia and extradited to Belarus. On October 14, 2016, his closed trial began in Minsk. Belarusian and international human rights groups consider him a political prisoner.[131]

In recent years, the government has begun using materials obtained from online sources as "evidence" to punish individuals for alleged offline ffenses. On August 11, 2015, four young men were detained over graffiti with political con ent on a concrete fence in Minsk, including a message in Belarusian stating that "Belarus must be Belarusian." After the authorities searched computers confi - cated from the activists' homes, the men were charged with using the internet to distribute "extremist" information, promote violence, and incite ethnic hatred. The "graffiti case" became the most ce - ebrated political trial of the last year due to a broad civic campaign spanning the country. The joint efforts of human rights defenders, civic activists, and independent journalists may have contributed to relatively mild sentences. The charges of extremism were ultimately dropped; one defendant was cleared of all charges and the others were fined ins ead of jailed.[132] Civil society groups organized an online fundraising campaign that is expected to cover the cost of the fines.[133]

Surveillance, Privacy, and Anonymity

Belarus employs systematic, sophisticated surveillance to monitor its citizens and control critical expression online.[134] All telecommunications operators are obliged to install real-time surveillance equipment, which makes it possible to monitor all types of transmitted information (voice, mobile text message and internet traffic) and obtain other types f related data (user history, account balance, and other details) without judicial oversight. Mobile phone companies are required to turn over personal data of their customers at the government's request. As of January 2016, all ISPs must

128 "Conveyor of persecution of freelance journalists was stopped in Soviet district court in Gomel" (in Belarusian), *Radio Liberty*, February 5, 2016, http://www.svaboda.mobi/a/27533644.html.

129 Reporters Without Borders, "Belarus: RSF urges withdrawal of baseless charges against detained blogger," October 12, 2016, https://rsf.org/en/news/rsf-urges-withdrawal-baseless-charges-against-detained-blogger.

130 Vadzim Smok, "John Silver: A New Political Prisoner in Belarus?", *BelarusDigest*, July 12, 2016

131 "Eduard Palchys is a political prisoner. Joint statement by human rights groups," *Viasna*, October 5, 2016, http://spring96.org/en/news/85127; Reporters Without Borders "Belarus: RSF calls for release of blogger held for past six months," July 29, 2016, https://rsf.org/en/news/belarus-rsf-calls-release-blogger-held-past-six-months.

132 "Activists Involved in 'Graffiti Case' ace Final Charge," December 11, 2015, *Viasna Human Rights Center*, http://spring96.org/en/news/81598.

133 Franak Viachorka, "Regarding the payment of the Graffitists' fines, in o days they collected more than $1,000," *Radio Liberty*, February 3, 2016, http://www.svaboda.org/content/article/27530261.html.

134 "Insights into Internet Freedom in Central Asia: Belarus," *Digital Defenders Partnership*, 2013, https://www.digitaldefenders.org/belarus.

retain information about their customers browsing history for one year. As a result, law enforcement agencies have access to the private browsing history of all web users in Belarus.[135]

Since 2010, the government has been utilizing the Russian-developed intercept technology SORM (System of Operative Investigative Measures) and allocating resources for online surveillance technologies.[136] SORM enables government surveillance directly via the provider. Since late 2011, deep packet inspection (DPI) technology has been available for network packet inspection and fil ering according to content.[137] The Belarusian government also uses Semantic Archive, software developed in Russia that monitors open data such as media archives, online sources, blogs, and social networks.[138] It also employs viruses, malware, and spying software to conduct cyber surveillance.[139] Since at least 2010, the Belarusian authorities apparently have employed mobile telephone surveillance measures.[140]

In July 2015 internal documents leaked from the Italy-based spyware fi m Hacking Team indicated that that the Belarusian government has been interested in the fi m's products since 2011. Hacking Team had presented its Remote Control System (Galileo and DaVinci) spyware, which targets computers and smartphones, to officials f om the Operational and Analytical Center, which oversees Belarus' internet, and the Belarusian Ministry of Internal Affairs, in 2014. The documents indicated Belarusian interest, but do not confi m that the government purchased the system.[141]

Chinese and Western fi ms have reportedly supplied equipment and software that would allow the state to expand its surveillance of citizens.[142] During the past year, the Belarusian government has been increasing its acquisition of equipment to monitor and control the internet. In May 2015, the government engaged a Chinese fi m to provide hardware and software for monitoring and blocking content online, and the equipment was reportedly installed ahead of the October 2015 presidential election. According to one expert, the new equipment is able to carry out a deeper analysis of internet traffic o determine which websites are undesirable for visitors, and can track user actions, sites visited, materials read, and programs connected.[143] Another report indicated that the government had installed new equipment to track anonymizer and proxy tools so that it could prevent their use to access banned websites.[144]

Beltelecom launched a tender in 2015 to purchase the hardware and software needed to identify

135 Alyaksey Areshka, "Internet service providers required to keep records of customers' visits to websites," *BelaPAN*, March 15, 2015, http://bit.ly/1LSCE3M.

136 Ministry of Communications and Informaization (MPT), "Measures on implementation of the National program of accelerated development of information and communication technologies for 2011-2015" [in Russian] http://bit.ly/1RftClJ.

137 Mikhail Doroshevich and Marina Sokolova, "Internet Development and Usage," ed. Anatoly Pankovsky and Valeria Kostyugova, *Belarusian Yearbook 2012*, 2013, 174, http://bit.ly/1hJ9XhL.

138 Andrei Soldatov and Irina Borogan, "Russia's Surveillance State," World Policy Institute, Fall 2013, http://bit.ly/1cZerr4.

139 "Insights into Internet freedom in Central Asia: Belarus," Digital Defenders Partnership 2013, accessed March 24, 2015, http://bit.ly/1OJ7ocQ.

140 Stanislav Budnitski, "Big Brother in Eurasia: Surveillance goes digital," *Digital.Report*, November 13, 2014, http://bit.ly/1Rfu5nU.

141 "OAC interested in DaVinci spyware," *Charter 97*, July 16, 2015, https://charter97.org/en/news/2015/7/16/160052; "Belarus Wanted To Use USB Sticks to Infect Devices and Collect Data," *OCCRP*, July 15, 2015, https://www.occrp.org/en/daily/4161-belarus-wanted-to-use-usb-sticks-to-infect-devices-and-collect-data; "Hacking Team," WikiLeaks, https://wikileaks.org/hackingteam/emails/emailid/541235;

142 Andrei Aliaksandrau, "Belarus: Pulling the Plug," 16-17.

143 Galina Petrovskaya, "The Belarusian segment of the internet: under the hood of the state" (in Russian), *Deutsche Welle*, September 24, 2015, http://bit.ly/2fuDknz.

144 "A system for tracking anonymizers has been launched in Belarus," (in Russian), *Providers.by*, December 10, 2015, http://providers.by/2015/12/news/v-belarusi-zarabotala-sistema-poiska-anonimajzerov.

outgoing voice traffic, including oIP, associated with a particular internet user. The company was seeking to use the system to bill its customers for Skype calls.[145] In March 2016, the government's Investigative Committee announced a tender for purchasing equipment that will provide access to data on smartphones compatible with all popular mobile operating systems. The tender said equipment should provide access to contacts, content of communications, audiovisual material, hidden or erased data on mobile devices, and assist in ascertaining user access codes, among other capabilities.[146]

In Belarus, there is no judicial or independent oversight of internet or ICT surveillance. ISPs are required to make remote access to their databases available on demand to government bodies carrying out investigations. There is widespread belief that the internet traffic, ext messages, and voice calls of opposition activists are routinely monitored. One expert notes that while the government continues to significantly ex and surveillance over the internet, few Belarusians realize the extent of this surveillance and the threat it poses to internet users.[147] One study called the Lukashenka government "a pioneer and leader in counter-revolutionary, including ICT-based, tactics among all the post-Soviet states."[148]

Given the government's increasing control over the internet, Belarusians are using proxy servers and other methods to circumvent restrictions and surveillance. However, during the past year, Tor use in the country declined from over 10,000 to almost 6,000 users.[149] This could be due to several factors, including the government's February 2015 ban of anonymity and circumvention tools, and the decrease in repression in the wake of the authorities' new détente with the West. Under the February 2015 ban on circumvention tools, the authorities can block not only anonymizers and Tor, but also other security tools like the Opera and Yandex browsers that allow access to almost any website in traffic comp ession mode.[150] At the time of this report, however, Tor is accessible and VPN use remains very popular.[151]

Since 2007, internet cafes are required to keep a year-long history of the domain names accessed by users and inform law enforcement bodies of suspected legal violations.[152] Internet cafes are also required to photograph or film use s.[153] Restaurants, hotels, and other entities are obliged to register guests before providing them with wireless access, whether free or paid.[154] Belarusian citizens must present their passports and register when buying a SIM card and obtaining a mobile phone number.

145 "Beltelecom buys equipment to monitor Skype calls," *Charter 97*, June 5, 2015, http://charter97.org/en/news/2015/6/5/154349.

146 "Investigative Committee wants to purchase smartphone 'ripper'," *42.TUT.BY*, March 16, 2016, http://42.TUT.BY/488688.

147 Jerome Taylor, "Government of Belarus using 'new tools' to silence dissent on internet, says Index on Censorship report," *The Independent*, January 4, 2013, http://ind.pn/1QATQPw. Since a majority of Belarus' internet traffic asses through Russia, which also employs SORM, it is also presumably spied on by that country's security services, which have close relations with their Belarusian counterparts.

148 Volodymyr Lysenko and Kevin Desouza, "The Use of Information and Communication Technologies by Protesters and the Authorities in the Attempts at Colour Revolutions in Belarus 2001–2010, Europe-Asia Studies, vol. 67, issue 4, 2015, http://www.tandfonline.com/doi/full/10.1080/09668136.2015.1031642.

149 Tor Project, "TorMetrics – Direct users by country," accessed August 23, 2016, https://metrics.torproject.org/userstats-relay-country.html?start=2015-06-01&end=2016-05-31&country=by&events=off.

150 "Belaru Bans Tor and Other Anonymizers," *E-Belarus*, February 26, 2015, http://www.e-belarus.org/news/201502261.html.

151 Douglas Crawford, "VPN and Tor banned in Belarus," *BestVPN*, March 4, 2015, http://bit.ly/1M6UYZA.

152 "Council of Ministers of the Republic of Belarus. Regulations on computer clubs and internet cafe functioning" [in Russian], *Pravo.by*, April 29, 2010, http://pravo.by/webnpa/text.asp?start=1&RN=C20700175.

153 Alyaksey Areshka, "Authorities scrap passport requirement for Internet cafes' visitors," *BelaPAN*, December 27, 2012, http://bit.ly/1Mubh0t.

154 Including the user's name, surname, type of ID, ID number, and name of the state body which issued the ID, as per Art. 6, Regulation on computer clubs and internet café functioning, http://bit.ly/1jIgoTB.

Belarus remains the only post-Soviet state with no proper legislation regulating the privacy of personal data. Belarus has not joined the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[155] In general, independent experts conclude that "Belarusian legislation does not provide a satisfactory basis for the proper balance between freedom and security online."[156]

Intimidation and Violence

As the Belarusian government sought international recognition for the October 2015 presidential election in an attempt to normalize relations with the EU, there were fewer recorded instances of extralegal intimidation and harassment of online activists and journalists.

However, family members of online activists continued to report intimidation and harassment. Eduard Palycha, the creator of the website 1863x.com, said his wife was threatened, pressured, and interrogated throughout his imprisonment (see Prosecutions and Detentions for Online Activities).[157] A girlfriend of one of the suspects in the "graffiti case" was lu ed to his apartment during his detention by a police officer who intimida ed and interrogated her. Psychological pressure was exerted on a pregnant girlfriend of another graffitist and online activist. An agg essive search of the apartment of the third suspect was conducted in presence of his one-year-old son and wife, who was also subjected to psychological pressure.[158] In the course of the graffiti case investigation, unknown people twice entered the apartments of one of the suspect's parents.[159]

Technical Attacks

Technical attacks have not been widely experienced in Belarus, but the government occasionally employs them against independent websites, often coinciding with important political events, such as elections, national holidays, or street protests. This past year demonstrated a new pattern, as certain news websites experienced repeated distributed denial-of-service attacks (DDoS) attacks. While Belarusian criminal law prohibits these types of technical attacks, law enforcement agencies rarely pursue such cases; when they do, the investigation is a mere formality.

Less than a week before the October 2015 presidential election, the independent websites BelaPAN.by and Naviny.by were hit by severe DDoS attacks against their Belarus-based servers. The former is the site of the country's only independent news agency, and many other outlets depend on it for news and information. The latter is also one of Belarus' most popular online newspapers. The technical attacks occurred the day after the outlets reported that students were forced to take part in a "Prayer for Belarus" event attended by President Lukashenka and his heir-apparent son ahead of the

155 Elena Spasiuk, "Belarusians will be checked by database," [in Russian] *Belorusskye Novosti*, July 24, 2013, http://bit.ly/1Oz6VLH.

156 Marina Sokolova, "Freedom and Security Online in Belarus: Window for Opportunities," Lawtrend, (presentation, May 2014) http://bit.ly/1Oz72a5.

157 Mikola Bugaj, "Creator of 1863x.com Website Claims that He Was Arrested and Investigated under Criminal Charges," *Nasha Niva*, November 5, 2015, http://nn.by/?c=ar&i=159400.

158 "Accused in 'graffiti case': During the Ar est We Were Threatened That We Would Never Get Out of Jail," *Spring 96*, September 4, 2015, http://spring96.org/en/news/79711.

159 "Suspects in 'graffiti case': e Face Six Years in Prison," *Spring 96*, September 25, 2015, http://spring96.org/en/news/80120.

presidential election.[160] Naviny.by also published caricatures of Lukashenka. The DDoS attacks continued for three days.[161] Throughout the attacks, BelaPAN continued to publish news on its Facebook page.

BelaPAN described the incident as "an example of the brutal pressure on the independent media and the violation of the constitutional principles of freedom of speech and freedom of the press."[162] The Belarusian Association of Journalists stated that it viewed the incident as an attempt to punish BelaPAN and Naviny.by for performing their professional duties.[163]

On February 15, 2016, BelaPAN's website was once again inaccessible due to another DDoS attack. The attack coincided with the meeting of the EU Council in Brussels, at which the issue of the removal of sanctions against Belarus was discussed. The website was able to resume its work the next day.[164]

Official ebsites have also been subject to technical attacks. The website of Belarus' Santa Claus hacked in summer 2015. Instead of materials about Santa's working hours, location, and contact information, the website displayed a black screen and a message from the hacker "Nassim Patchika" stating that "Muslims are not terrorists." The Algerian hacker is known for hacking different websites to remind their administrators about safety issues.[165]

160 Juras Karmenau, "Belarusian media claim gov't attack on their websites," *The Big Story, AP*, October 5, 2015, http://bigstory.ap.org/article/15ee42cef9934b2284503e55f38edf1d/belarusian-media-claim-govt-attack-their-websites; Alyaksey Alyaksandraw, "Authorities are blocking BelaPAN's websites to punish journalists for doing their job, Belarusian Association of Journalists says," *BelaPAN*, October 5, 2015, http://en.belapan.by/archive/2015/10/05/en_18261005H.

161 "BelaPAN informs about DDoS-attack," *Salidarnast*, *Gazetaby.com*, October 3, 2015, http://gazetaby.com/cont/art.php?sn_nid=102497.

162 "BelaPAN's statement in connection with DDoS-attacks against the company's websites," *Gazetaby*, October 5, 2015, http://gazetaby.com/cont/art.php?sn_nid=102497.

163 "BAJ statement on technical attacks against BelaPAN's websites," *Belarusian Association of Journalists*, October 5, 2015, http://baj.by/be/content/zayava-ga-bazh-z-nagody-ataki-na-sayty-belapan.

164 "Access to BelaPAN's website was blocked," Belarusian Association of Journalists, *BAJ*, February 16, 2016, http://baj.by/be/content/dostup-da-sayta-belapan-byu-zablakavany.

165 "Muslim hacker hacked the website of Ded Moroz in Belarus," *BBC*, December 25, 2015, http://www.bbc.com/russian/society/2015/12/151225_belarus_santa_hacked.

Freedom House

Brazil

	2015	2016
Internet Freedom Status	**Free**	**Partly Free**
Obstacles to Access (0-25)	7	8
Limits on Content (0-35)	6	7
Violations of User Rights (0-40)	16	17
TOTAL* (0-100)	**29**	**32**

* 0=most free, 100=least free

Population:	**207.8 million**
Internet Penetration 2015 (ITU):	**59 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2016 Status:	**Partly Free**

Key Developments: June 2015 – May 2016

- Popular communication application WhatsApp was temporarily blocked on two occasions during this period, in December 2015 and May 2016, after Facebook, which owns the encrypted messaging service, was unable to comply with requests to turn over data pertaining to users under criminal investigation. While higher courts quickly overturned these orders, they disproportionally impacted users across Brazil (See **Blocking and Filtering**).
- Some of the largest internet service providers in Brazil announced that they would introduce data caps for fi ed broadband, prompting widespread outrage and several bills in Congress to limit practices that are deemed to be unfair to consumers (See **ICT Market**).
- A report by a Parliamentary Investigation Commission proposing a series of cybercrime bills caused significant acklash among civil society and scholars (see Legal Environment).
- Since the adoption of the so-called "Constitution for the Internet" in April 2014, secondary legislation enacted in May 2016 further refined rules for net neutrality and security measures regarding connection logs stored by providers (see **Legal Environment**).

Introduction

Brazil's internet freedom environment declined during this period, as decisions by regional judges to temporarily block WhatsApp disproportionally affected users across the country.

Hailed as a civil rights framework for the internet, Brazil's Marco Civil Law (Marco Civil da Internet) contains key provisions governing net neutrality and ensuring strong privacy protections. In May 2016, right before the beginning of impeachment procedures that suspended President Dilma Rousseff from office, a dec ee regulating the Marco Civil further clarified rules conce ning the scope of application of net neutrality, as well as security measures to be adopted by providers for collecting and storing connection logs. However, despite boasting some of the most progressive and comprehensive legislation on digital rights, internet freedom in Brazil remains constrained by violence against independent bloggers, criminal defamation laws, restrictions on anonymity, and restrictive limits on content related to elections.

Several orders to block WhatsApp have especially raised concerns about an ongoing judicial trend within the country, and draw attention to unforeseen effects of Marco Civil enforcement. Both temporary blocking orders in December 2015 and May 2016 were linked to ongoing requests to turn over information as part of criminal investigations by the police. WhatsApp has repeatedly argued that it cannot provide information it does not have, especially because it encrypts messages and does not store them on its servers. While both decisions were quickly overturned by higher courts, digital rights advocates have criticized this trend as a disproportionate misinterpretation of the Marco Civil, which includes a sanction of "temporary suspension of activities" for providers that violate Brazilian law. Brazilian authorities have repeatedly clashed with WhatsApp over access to user data, even leading to the arrest of the Latin American Vice President of Facebook, which owns WhatsApp, in March 2016.

Concern also grew that Congress may pass laws that could change key aspects of the Marco Civil. In March 2016, a report by a Parliamentary Inquiry Commission proposed a package of cybercrime bills which threatened to undermine several privacy rights in favor of wider powers for criminal investigators, and erode the Marco Civil's judicial notice and takedown system. While several of the initial points were dropped after significant acklash from civil society and activists, the final p oposals approved by the commission in early May continued to generate debate among digital rights activists.

On the other hand, while internet penetration rates have been increasing modestly, social media and its potential for mobilization has taken center stage in Brazil. Issues that have garnered particular interest in discussions on social media over the past year range from concerns surrounding the Zika epidemic and its public health consequences, especially in the lead-up to the 2016 Rio Olympics,[1] to polarized debates surrounding the political and economic situation. Online discontent over corruption scandals are often taken to the streets, as protests reached record levels in March 2016.[2]

1 "Brazil will make Olympics safe from Zika virus: WHO official" *Reuters*, February 23, 2016, http://reut.rs/1UlXYHp.

2 "Record Brazil protests put Rousseff's future in doubt," *Reuters*, March 14, 2016, http://reut.rs/1TY0c0Q.

Obstacles to Access

Although internet and mobile penetration rates have increased steadily in Brazil, significant regional disparities in access persist. Three of the largest ISPs in Brazil caused uproar when they announced data caps for fixed broadband by 2017, and several bills proposed to limit such practices. Millions of users were also affected when the messaging service WhatsApp—the most popular communication app in Brazil – was blocked on two occasions during this period of coverage.

Availability and Ease of Access

Despite economic growth in recent years, Brazil's access rates remain below average compared to many North American and European countries. The International Telecommunications Union (ITU) estimates that Brazil's internet penetration rate reached 59 percent in 2015, compared to 55 percent in 2014 and 51 percent in 2013.[3] According to the Center of Studies on Information and Communication Technologies (CETIC), some 50 percent of households did not have access to the internet as of March 2015, an improvement from 60 percent in 2013.[4] Various obstacles continue to prevent many households from accessing the internet, such as high prices—a problem that extends to fi ed broadband, wireless, and 3G and 4G technologies—and persistent social inequalities. A significant digital divide and disparities in infrastructure are evident between various geographical regions, as well as between urban and rural areas.

According to the Brazilian Institute for Geography and Statistics, 31 million households had internet access in 2015, accounting for 49 percent of the population. Of these, 98 percent connected via broadband and only 2 percent had dial-up connections.[5] Data from the National Telecommunications Agency (ANATEL) shows a fi ed-broadband subscription penetration of around 12 percent at the beginning of 2016.[6] By the end of 2015, Akamai measured Brazil's average internet connection speed at 4.1 Mbps, up from 3.4 Mbps in the fi st quarter of 2015.[7]

Although household access is one of the most common means of connection for those with slightly higher incomes, LAN Houses (public paid access centers) remain relevant to digital inclusion in Brazil, particularly in the country's impoverished northern regions.[8] Legislative initiatives such as the bill on "Centers for Digital Inclusion" consider LAN Houses as "public interest facilities," in line with existing internet access strategies implemented by the Ministry of Telecommunications in the past years.[9] While national wireless networks are still small compared to other countries, ANATEL registered over one million hotspots in Brazil as of July 2015.[10]

3 International Telecommunications Union (ITU), "Percentage of Individuals using the Internet, 2000-2015," accessed August 11, 2016, http://bit.ly/2c3GSwk.

4 Center of Excellence in Information and Communication Technologies (CETIC), "Proporção de domicílios com Internet" [Percentage of Households with Internet Access], October 2014-March 2015, accessed March 21, 2016, http://bit.ly/2c0Km3Q; See also: CETIC, "No Brasil, 60% das casas ainda não têm internet" [In Brazil, 60 percent of households still do not have internet], July 1, 2013, http://bit.ly/1jbuXiH.

5 Empresa Brasil de Comunicação, "Acesso à internet chega a 49,4% da população brasileira" [Internet access reaches 49.4 percent of the Brazilian population], April 29, 2015, http://bit.ly/1GIh19q.

6 Teleco Inteligência em Comunicação, "Banda Larga Fixa no Brasil" [Fixed broadband in Brazil], January 2016, accessed March 21, 2016, http://bit.ly/2e2cT90.

7 Akamai, State of the Internet, Q4, 2015 Report, accessed August 11, 2016, http://akamai.me/2b5MgzU.

8 CGI.Br, "ICT Households and Enterprises 2013 - Survey on the use of Information and Communication Technologies in Brazil," 2014, http://bit.ly/1cRt7jV.

9 Bill 28/2011, http://bit.ly/1OxjBE8.

10 Teleco, "Hot-spots Wi-Fi no Brasil" [Wi-Fi hotspots in Brazil], January 2016, accessed March 20, 2016, http://bit.ly/2dLKJAo.

Mobile penetration has grown significantly o er the last few years and mobile broadband connections have quickly become a dominant means for Brazilians to access the Internet.[11] Overall, mobile penetration rates increased from 88 percent in 2009 to 126 percent (or around 259 million phone subscriptions) by the end of 2015. However, the number of subscriptions has decreased over the past year, falling from 281 million (or 139 percent) in 2014, according to ITU data.[12] This drop has been attributed to Brazil's economic crisis and stricter credit policies imposed by operators.[13]

The supply of smartphones with 4G services has significantly inc eased since its introduction in April 2013, but high prices and limited network still constitute challenges. As of May 2016, nearly 135 million users (approximately 48 percent) had 3G services.[14] According to the consultancy company Teleco, Brazil had 36.5 million active 4G subscriptions by May 2016, representing an increase of approximately 208 percent compared to the same period as of May 2015.[15] Such advanced internet services, however, are heavily concentrated in wealthy urban centers such as São Paulo.[16]

Brazil's federal government has been implementing a number of internet expansion and improvement programs since 2010, including the National Broadband Plan (Plano Nacional de Banda Larga or PNBL).[17] According to statistics from the Brazilian Telecommunications Association, broadband connections increased by 308 percent between October 2014 and October 2015.[18] The government estimates that 94 million individuals gained broadband access since the adoption of PNBL in 2010.[19] But specialists have criticized these figu es; after almost four years, only 1.8 million (7.9 percent) of the 23 million fi ed broadband subscriptions were contracted through PNBL. PNBL covered only 0.6 per cent (800,000) of the total 128.5 million individuals who accessed mobile internet.[20]

A Special Taxation Regime (REPNBL)[21] has sought to complement the PNBL by encouraging investment in existing telecommunications networks to expand broadband and mobile internet capabilities and offer internet access to the population at equitable prices, coverage and quality.[22] Under this initiative the Ministry of Communications and mobile companies have launched projects in 2015 to improve high-speed internet access in rural areas of the country.[23] In February 2013, Decree

11 "Banda ancha móvil en Latinoamérica alcanzó 32% de penetración en 2014" [Mobile broadband penetration in Latin America reached 32 percent in 2014], *Prensario Internacional*, February 3, 2015, http://bit.ly/1NUcQL2; See also: Mediatelecom Agencia, "Banda Ancha Móvil de Brasil Crece Tres Veces Más Rápido Que El Promedio Mundial" [Mobile Broadband grows three times more than the global average], *AE Techno*, May 29, 2015, http://bit.ly/1V9IfNP.

12 ITU, "Mobile-Cellular Subscriptions 2009-2015," accessed March 20, 2016, http://bit.ly/1LOr3mK.

13 "Brazil loses mobile subscribers for sixth month in a row," *Telecompaper*, January 13, 2016, http://bit.ly/2c5NqL4.

14 Teleco, "Estatísticas de Celulares no Brasil," [Statistics on Mobile Phones in Brazil], accessed August 11, 2016, http://bit.ly/1w6LIAI.

15 Teleco, "4G: 4ª Geração de Celulares no Brasil" [Fourth Generation of Cellphones in Brazil], January 2016, accessed March 20, 2016, http://bit.ly/2ddg2RO.

16 "Cidade de SP é o 5˚maior mercado da América do Sul, diz Fecomerico" [São Paolo is the Fifth Largest Market in South America, Says Fecomercio], *O Globo*, January 1, 2014, http://glo.bo/1JqlYzg.

17 Ministry of Communications, "Programa Nacional de Banda Larga" [National Broadband Plan], News release, May 25, 2015, http://bit.ly/UJ4JY6; See also: "Em 2018, 70% dos brasileiros terão acesso à banda larga" [In 2018, 70 percent of Brazilians will have access to broadband], *Portal Brasil*, October 22, 2015, http://bit.ly/2bPJzpi.

18 Associação Brasileira de Telecomunicações, "Banda larga 4G cresce 308% em 12 meses, diz Telebrasil" [4G Broadband Connections increased 308 percent over 12 months, according to Telebrasil], December 7, 2015, http://bit.ly/2bA1ivr.

19 "Em 2018, 70% dos brasileiros terão acesso à banda larga" [In 2018, 70 percent of Brazilians will have access to broadband], *Portal Brasil*, October 22, 2015, http://bit.ly/2bPJzpi.

20 Luciana Bruno, "Programa de banda larga se aproxima do fim cheio de c íticas," [Broadband program nears end with criticism], *Exame*, September 30, 2014, http://abr.ai/1QyPXdC.

21 Law 12,715 of September 17, 2012, http://bit.ly/2c61xA3.

22 Ministério das Comunicações, "REPNBL –Início," News release, March 11, 2013, http://bit.ly/1PtY0bv.

23 Luís Osvaldo Grossmann, "REPNBL aprova R$ 526,4 milhões em projetos de 4G em 450 MHz, " [REPNBL approves R$ 526.4 million in 4G projects], *Universo Online,* July 13, 2015, http://bit.ly/1WjakiS.

7.981/2013 established tax incentives for the ICT sector by exempting certain categories of smartphones from taxation, namely those produced with national content, Wi-Fi connectivity, email access, and open source code for developers.[24]

Restrictions on Connectivity

The government does not place limits on bandwidth, nor does it impose control over telecommunications infrastructure. There have been no reported instances of the government cutting off internet connectivity during protests or social unrest. However, millions of users were temporarily unable to access messaging service WhatsApp after its parent company Facebook did not comply with information requests as part of criminal investigations (see Blocking and Filtering).

Most of the backbone infrastructure for the internet is privately owned in Brazil. In 1998, the state-owned company Embratel, which was responsible for building the internet backbone, was privatized and acquired by the U.S. company MCI; it was later acquired by the Mexican telecom América Móvil in 2003. Over the past decade, private backbone infrastructure, such as that of Embratel, GVT and Oi, has expanded in Brazil. With the PNBL, however, Brazil is expected to expand government-owned infrastructure—including underutilized fibe -optics—to allow for low-cost connections. The significant increase in wired broadband subscriptions from 2010 to 2013 is at least somewhat attributable to the expansion of the state-owned backbone. Since the PNBL was initiated, over 612 Brazilian municipalities, which contain around 40 percent of the population, received service from the state-owned Telebras network.[25]

Internationally, undersea cables connect to Brazil from North America and Europe. Brazil has announced plans to create new undersea cable connections with South Africa and the Caribbean, as well as Portugal. Some of the impetus for building these connections is related to a desire to avoid reliance on U.S. infrastructure after revelations of pervasive U.S. spying on Brazilians in 2013.[26]

In 2004, the Brazilian Internet Steering Committee (CGI.br) launched an initiative called PTT Metro to create internet exchange points (IXPs) across Brazil, starting with their fi st IXP in São Paulo. As of April 2013, there were 22 IXPs in operation, covering 16 of Brazil's 26 states.[27] Currently, Brazil has at least 25 IXPs installed in the country.[28]

ICT Market

Although there are no significant legal or economic arriers for companies competing in the ISP, mobile, or digital technology sectors, the Brazilian ICT market is highly concentrated. As of May 2016, three large private companies—Oi, Claro and Vivo (Telefônica Brasil)—represented over 84 percent of the country's broadband market.[29] In January 2014, the Brazilian competition authority approved

24 Decree 7.921, February 15, 2013, http://bit.ly/1MqgJnH.

25 "Brazil's Programa Nacional de Banda Larga," *Tech in Brazil*, October 17, 2014, http://bit.ly/1Vb2cyi.

26 Anna Edgerton and Jordan Robertson, "Brazil-to-Portugal Cable Shapes Up as Anti-NSA Case Study," *Bloomberg Business*, October 30, 2014, http://bloom.bg/1gOGiDz.

27 Internet Society, "New Study Reveals How Internet Exchange Points Spur Internet Growth in Latin America," December 3, 2013, http://bit.ly/1Lx6mjr.

28 Latin America and Caribbean Network Information Center, "Internet Exchange Points en América Latina y Caribe," http://bit.ly/1V9O79Q.

29 Teleco, "Seção: Banda Larga—Market Share de Banda Larga no Brasil," [Section: Broadband—Market Share of Broadband in Brazil], accessed March 2016, http://bit.ly/1ix3MhE.

the merger of Oi and Portugal Telecom into CorpCo. This merger was completed in 2015 and ranked CorpCo as the leading telecommunication company in Portuguese-speaking countries worldwide.[30] Also in 2014, the acquisition of Vivendi's GVT by Telefônica Brasil resulted in a merger of two of the country's larger broadband services in 2016 – GVT and Vivo – further contributing to market share concentration.[31]

By mid-March 2016, Vivo, Claro and Oi announced that fi ed broadband internet would operate under a limited data cap business model by the beginning of 2017, similar to measures adopted for mobile internet access.[32] This announcement caused widespread uproar among users, politicians and internet-dependent businesses,[33] since broadband internet in Brazil has been consistently regarded as costly and of low quality.[34] ANATEL's then-president João Rezende addressed the controversy by supporting the decision and blaming users for high usage of bandwidth. However, ANATEL subsequently prohibited all major ISPs from adopting such measures for 90 days until they provided detailed motives. Several bills also proposed to limit such practices that are deemed to be unfair to consumers,[35] including one legislative proposal from a petition that gathered over 20,000 signatures within two weeks.[36]

According to the most recent data regarding Brazil's mobile market in May 2016, four large private companies—Vivo, TIM, Claro, and Oi—held 96 percent of the market.[37] Such high market concentration could make it very difficult for other p oviders such as Algar and Nextel to compete in the mobile sector.[38] Despite such concentration, Brazil has the largest smartphone market in Latin America.[39]

Regulatory Bodies

Two regulatory agencies oversee Brazilian ICTs: the Brazilian Agency of Telecommunications (ANATEL) and the Administrative Council for Economic Defense (CADE), an antitrust agency that is focused on reviewing mergers and anticompetitive practices in telecommunications markets. Additionally, in 1995 the government created the Brazilian Internet Steering Committee (CGI.br), a multi-stakeholder independent organization in charge of coordinating and integrating all internet service initiatives in Brazil, as well as promoting technical quality, innovation, and the dissemination of services. Provisions in Marco Civil mandate that the government consult with CGI.br, and in various instances directly involve the Committee, in the policy-making and implementation of Marco Civil processes.[40]

30 "Brazil competition watchdog approves Oi, Portugal Telecom merger," *Reuters*, January 14, 2014, http://reut.rs/1Ov29ys.

31 "Anatel aprova compra da GVT pela Vivo (e o que isso muda)" [Anatel approves purchase of GVT by Vivo, and what this changes], *Technoblog*, September 2014, http://bit.ly/2bQCbVX.

32 Gabriel Luiz, "Empresas querem vender Internet fixa como acote de dados" [Companies want to sell fi ed internet with data package], *G1,* March 19, 2016, http://glo.bo/2c813JC.

33 Angelica Mari, "Brazilians protest against fi ed broadband data cap," *ZDNet*, April 13, 2016, http://zd.net/2c4dCGR.

34 Helton Gomes e Thiago Reis, "Velocidade da banda larga no Brasil varia entre taxas de Líbia e Japão" [Broadband speed in Brazil varies between rates in Libya and Japan], *G1,* May 13, 2015, http://glo.bo/2bBP5JW.

35 Kimberly Anastácio, "Parlamentares apresentam projetos de lei contra franquia de dados" [Parliamentarians present bills against data caps], Instituto Beta para Internet e Democracia, June 1, 2016, http://bit.ly/2cbuydP.

36 Edilson Rodrigues, "Após sugestão popular, proibição do limite para Internet pode virar lei" [After popular suggestion, ban on limits for internet could turn into law], *IG Tecnologia*, April 20, 2016, http://bit.ly/2c4ibRL.

37 Teleco, "Telefonia Celular—Operadoras de Celular" [Cellular Telephony—Cellular Operators, June 2010], accessed March 21, 2016, http://bit.ly/1ix42gx.

38 Teleco, "Operadoras de Celular –Jan/16" [Celular Operators –Jan/16], accessed March 21, 2016, http://bit.ly/1cfEPkY.

39 EMarketer, "Latin America Is Home to a Robust Mobile Market," September 16, 2015, http://bit.ly/1KpE75q.

40 Marco Civil, Art. 24, II.

ANATEL is administratively and financially independent, and not hiera chically subordinate to any government agency. Its decisions can only be appealed in courts. From the Ministry of Communications, ANATEL has inherited the powers of granting, regulating, and supervising telecommunications in Brazil, as well as much of its technical expertise and other material assets. While both ANATEL and CGI.br are entrusted with ensuring the free, fair, and independent operation of ICTs, the General Telecommunications Act also empowers CADE to issue decisions on matters such as price setting and collusion.[41] In May 2012, the new Brazilian Antitrust Act (Law No. 12.529 of November 30, 2011) came into force, introducing a pre-merger control regime in Brazil. Under this act, mergers must have pre-approval by CADE before they can proceed. The act also expands CADE's substantive enforcement power regarding cartel and unilateral business practices that affect competition as well as consumer rights and benefits [42]

CGI.br is formed by elected members from government, the private sector, academia, and nongovernmental organizations. CGI.br's contributions include comprehensive and reliable annual reports on internet use in Brazil, funding for internet governance-related research, and the promotion of conferences such as the annual Brazilian Internet Governance Forum, and the international Net Mundial conference, which was organized in Brazil in 2014.[43] In June 2009, CGI.br declared the "Principles for the Governance and Use of the Internet," which include the goals of online freedom, privacy, human rights, and net neutrality as a base for the Brazilian information society.[44] Many of these principles were adopted into Brazilian law through the Marco Civil in 2014.

Limits on Content

Several orders to block WhatsApp have raised concerns about an ongoing judicial trend within the country. While content removal requests filed before local courts continue to pose significant challenges to social media companies in Brazil, a notice and takedown provision in Brazil's Marco Civil Law has clarified intermediary liability. Brazilians' use of social media tools for civic action and activism continues to increase, particularly in the wake of the intense protests against and in favor of Dilma Rousseff's government and anti-corruption demonstrations that took place through 2015 and early 2016.

Blocking and Filtering

In keeping with the country's push to modernize and expand access to ICTs, Brazil's digital information landscape remains largely unrestricted. There are no proven indications that Brazilian authorities are fil ering messages or engaging in widespread blocking online. Brazilians freely gather and disseminate information via the internet and mobile phone technologies. They have access to a wide array of national and international news sources, blogs, social networking platforms, and citizen journalism, the latter of which has proliferated over the past year.

Social networks, communication apps, and video-sharing websites such as Facebook, Twitter, and

41 Law 9.472/1997; See also: Maria Cecília Andrade, Ubiratan Mattos, and Pedro C. E. Vicentini, "Reforms in Brazilian Telecommunications Regulations and their Impact on Sector Competition," *The Antitrust Review of the Americas 2009* (London: Global Competition Review, 2009), http://bit.ly/2bBsz5C.

42 Vinicius Marques de Carvalho, "Brazil: CADE," *The Antitrust Review of the Americas 2014* (London: Global Competition Review, 2014), http://bit.ly/1LG4xjL.

43 For the outcomes of Net Mundial 2014, see: CGI, "Cadernos CGI.br | Declaração Multissetorial do NETmundial," January 28, 2015, http://bit.ly/1R0BsA9.

44 CGI.br, "Principles for the Governance and Use of the Internet," January 28, 2015, http://bit.ly/2bREEnM.

YouTube are—for the most part—freely accessible and widely used in Brazil. On two occasions during this coverage period, however, telecom companies were ordered to temporarily block the popular communication tool WhatsApp after failure to comply with information requests in criminal investigations.

- On December 16, 2015, a lower court in the state of São Paulo ordered wireless carriers to shut down WhatsApp for 48 hours, because the company did not cooperate with a criminal investigation. The decision was overturned 12 hours later through a temporary injunction issued by the Court of Justice in the state of São Paolo, following an appeal by the company.[45]

- On May 2, 2016, a judge in Sergipe state ordered operators to block WhatsApp for 72 hours.[46] Similarly, the decision was linked to WhatsApp's failure to comply with a court order to access users' messages for the purpose of a criminal investigation linked to drug trafficking in the city f Lagarto. Earlier in March, the same judge had ordered the arrest of Facebook's Vice-President in Latin America, Diego Dzodan, as a means of coercing the company into obeying its request (See "Prosecutions and Detentions for Online Activities"). A different judge from the state court cancelled the ruling the next day, following an appeal by WhatsApp's lawyers.[47]

- In a more recent instance on July 19, 2016,[48] a judge ordered providers to block WhatsApp for an indefini e period of time, again for not turning over requested information sought in the course of a criminal investigation. The Brazilian Supreme Court overturned the measure later that day through a preliminary injunction, stating that "the suspension of the service apparently violates the basic principle of freedom of expression and communication, enshrined in the Constitution, as well as prevailing legislation on the matter."[49]

Another order was issued prior to this period, in February 2015, but it was suspended and the application was not blocked.[50] The decisions to block the app were based on Marco Civil's statutory provisions, notably Article 12 which provides for the "temporary suspension of activities" of connection providers and internet application providers that violate Brazilian law, including the right to privacy, the protection of personal data, and the secrecy of private communications. Digital rights specialists have argued that these decisions were not only disproportionate, but also constituted a misinterpretation of the law, notably because it does not specifically mention the suspension f applications or services.[51]

45 Rafael Barifouse, Fernando Duarte, Guilherme Barrucho, "Por que o bloqueio do WhatsApp não vingou –e como isso afetará a briga entre empresas de internet e Justiça" [Why the blocking of WhatsApp did not succeed – and how this will affect the fight bet een internet companies and Justice], *BBC Brasil,* December 17, 2015, http://bbc.in/1mbcOmp.

46 "WhatsApp Ordered Blocked Again in Brazil Over Data Dispute," *Bloomberg*, May 2, 2016, http://bloom.bg/1rsCA8y; See also: "Tribunal de Justiça de Sergipe emite nota sobre bloqueio do WhatsApp" [Court of Sergipe issues note on blocking of WhatsApp], *G1,* May 2, 2016, http://glo.bo/2dXjbd1.

47 "WhatsApp block in Brazil overturned after court appeal and user complaints," *The Guardian*, May 3, 2016, http://bit.ly/2c6yhJ4.

48 This event occurred outside the period of coverage of this report.

49 "Brazil Supreme Court overturns judge's ruling blocking WhatsApp," *EFE*, July 20, 2016, http://bit.ly/2c6v38J.

50 "Juiz do Piauí determina suspensão do WhatsApp no Brasil," [Judge in Piaui decides to suspend WhatsApp in Brazil], *Folha de S. Paulo*, February 25, 2015, http://bit.ly/2bA4aIF.

51 "Justiça Bloqueia WhatsApp por 72 horas" [Justice blocks WhatsApp for 72 hours], *Jota*, May 2, 2016, http://bit.ly/2bPquiA; See also: Polido, Fabrício B.P, "Levando a sério o Marco Civil da Internet no Brasil: premissas para o repensar das instituições e a justiça na fronteira das tecnologias" [Taking the Marco Civil seriously in Brazil: premises for rethinking institutions and justice on the frontier of technology], IRIS, August 1, 2016, http://bit.ly/2c6yiNr.

On the other hand, these temporary shutdowns have added fuel to the public debate around law enforcement's ability to access tech companies' encrypted data. WhatsApp has repeatedly argued that "we cannot provide information we do not have," because it encrypts messages locally and does not store them on its servers. Especially since expanding end-to-end encryption for all users' communications in April 2016, WhatsApp has insisted that such requests to turn over information are technically impossible.[52] While millions of users were affected by these decisions, WhatsApp's main competitor, Telegram, gained over seven million new users from Brazil within 24 hours in May 2016,[53] in turn highlighting the significant repercussions for businesses within the country.

Content Removal

While the enactment of Marco Civil has been hailed as a progressive landmark for internet governance, certain legal provisions criminalizing defamation and blasphemy and restricting speech around elections continue to put some constraints on internet freedom online. Brazil's controversial Electoral Act of 1997 has faced intense scrutiny particularly because its broad terms harbor the potential to constrain freedom of expression both online and offline, as it continues to limit certain content deemed to be injurious to candidates during electoral periods. An amendment to the law in 2013 created new and specific restrictions to online content concerning candidates and political parties.[54]

These restrictions on content resulted in the state issuing hundreds of content-removal requests in late-2014 and early-2015. After the electoral period ended in Brazil, companies reported a considerable reduction in content removal requests, highlighting the Electoral Law's impact on state-initiated censorship in Brazil. Removal requests issued to Twitter almost halved in July to December 2015 compared to the previous year. From July to December 2015, Twitter received 15 removal requests from Brazilian courts. The company withheld a total of 107 tweets and 1 account from view in Brazil.[55] But with municipal elections scheduled for October 2016, such requests threaten to proliferate again.

Lawsuits have also led Brazilian courts to ban some individuals from posting online in certain cases.[56] Blogger Marcelo Auler was requested to remove several articles published on his website between November 2015 and April 2016, after they were found to contain accusations that harmed the reputation of police officers involved in overseeing investigations into the "car wash" (Lava Jato) corruption scandal. He was also prohibited from publishing future reports that "could be interpreted as offensive to the officers."[57] The rulings of the federal courts of state of Paraná have been strongly criticized for establishing a "prior censorship" measure constraining any future content published by the blogger.[58]

Brazilian law also limits certain online content through cybercrime legislation. The "Azeredo Act" was

52 Jan Koum (CEO and co-founder of WhatsApp), Facebook post, May 2, 2016, http://bit.ly/2bzZ8zf.

53 Telegram Messenger, Twitter post, May 3, 2016, 1:32 pm, http://bit.ly/2c31pT6.

54 Restrictions include liability of servers with regard to early online campaigning; unsubscribe mechanisms for electoral advertising; elevation of fines due to violations of online electoral conduct; and the criminalization of hiring people in order to perform online bashing of candidates. See: Law 12.891 of 2013, http://bit.ly/1my5W1I.

55 Twitter, "Removal requests," *Transparency Report*, July-December 2015, http://bit.ly/2dLMHk2.

56 See for example: Paula Martins, "Protest Letter to UN-Ricardo Fraga's Case," Article 19, April 22, 2014, http://bit.ly/1VcR6ci.

57 Committee to Protect Journalists, "Court orders Brazilian blogger to delete posts," June 2, 2016, http://bit.ly/2bFW9H7.

58 "Operação Censura" [Operation Censorship] *Folha de São Paulo*, June 2, 2016, http://bit.ly/2dMJmVI.

enacted in November 2012 after major changes to its original, highly controversial proposal.[59] In its final fo m, it establishes the creation of specialized teams and sectors structured by the judicial police to fight against cybe crimes and to take down racist content (other defamatory content is not directly covered by the act). In the case of cybercrimes and racist content, takedowns require a judicial notice, but can be issued before police investigations have begun.[60]

Intermediary liability issues have been settled by a case law established by the Brazilian Superior Court of Justice (STJ) and by statutory provisions enacted by Marco Civil in 2014, which establishes that internet providers shall not be held liable for civil damages resulting from content created by third parties, and that application providers will only be held liable for civil damages resulting from content generated by third parties should they refuse to follow a court order requesting specific removal of said content.[61] In recent years, case law was slowly built around a similar understanding, with the Brazilian STJ ruling towards a judicial notice-and-takedown model.[62] Exceptions were made for copyright infringement and "revenge porn," such as dissemination of sexually explicit photos or videos without the consent of the individual appearing in them. In cases pertaining to revenge porn, a court order is not required for content removal, and the user's notification alone is enough o make the intermediary liable should it refuse to make the content unavailable in a short time.[63]

Between late 2015 and early 2016, courts rejected several requests pertaining to intermediary liability and fil ering of content. In both cases, intermediaries were requested to monitor and fil er certain keywords and content deemed to be economically harmful to specific en erprises, such as bad reviews or massive social gatherings in shopping malls organized through social media. Courts argued against such requests, based on constitutional rights to freedom of expression and on Article 19 of the Marco Civil,[64] as well as freedom of expression and access to information established by Articles 2, 3 and 4 of the Law.[65]

On the other hand, the STJ ruled in March 2015 that news providers are liable for failing to preventively control offensive posts by their users. Judges held that, unlike technology companies such as Google and Microsoft, news portals have a duty to ensure that their platforms are not employed to disseminate defamatory content or violations of the privacy and intimacy of third parties, since their primary activity is providing accurate information to the public.[66] Although there were no reported

59 Law 12.735 of November 30, 2012, http://bit.ly/1sUwjhz.

60 Rafaella Torres, "Aprovação de Leis sobre Crimes Cibernéticos"[Approval of Cybercrime Laws], *A2K Brazil* (blog), January 17, 2013, http://bit.ly/1QAGF0L.

61 See Law 12.965 (Marco Civil da Internet), Art. 18: The provider of connection to internet shall not be liable for civil damages resulting from content generated by third parties. Art. 19: In order to ensure freedom of expression and prevent censorship, the provider of internet applications can only be subject to civil liability for damages resulting from content generated by third parties if, after a specific cou t order, it does not take any steps to, within the framework of their service and within time stated in the order, make unavailable the content that was identified as being unlawful, unless othe wise provided by law.

62 The case law evolved to a notice and takedown model, which means internet providers and content providers were requested to remove the alleged infringing or offensive material within 24 hours upon judicial order. See for instance STJ, *Educacional/Yahoo*, REsp 1.338.214/MT, decision as of November 13, 2013; STJ, *Sassaki/Google*, Resp 1.338.214/MT, decision as of December 12, 2012.

63 Pereira de Souza, Carlos Affonso, "Responsabilidade civil dos provedores de acesso e de aplicações de Internet: Evolução jurisprudencial e os impactos da Lei Nº 12.965," IN: Lemos, Leite, Marco Civil da Internet, Atlas, 2014.

64 Court of Justice of the State of Mato Grosso do Sul, Civil Appeal Nº0816829-25.2014.8.12.0001, decision as of January 26, 2016.

65 Court of Justice of the Federal District. Interlocutory Appeal Nº 20150020218878AGI (0022263-35.2015.8.07.0000), decision as of November 25, 2015.

66 Brazilian Superior Court of Justice (STJ), Appeal to the Superior Court No. 1352053 / AL (March 24, 2014), http://bit.ly/1MP9esA.

charges against media organizations based on this precedent, the ruling may encourage online newspapers and other media to preemptively delete their comments sections to avoid liability.

Although ISPs are not responsible for prescreening content, the STJ consolidated a number of precedents establishing that intermediaries must comply with court-issued notice and takedown requests within 24 hours.[67] Accordingly, in a June 2014 case, the court issued a decision ordering Google to compensate a user of the former Orkut social network (previously owned by Google) for moral damages, since the company did not immediately comply with an order to remove defamatory content related to false accounts in her name.[68] Although two bills to create a so-called "right to be forgotten" were proposed in Brazil's Congress, by which search engines would be required to remove links to personal data upon requests by users, legislative proposals had yet to be brought up for debate.[69]

Media, Diversity, and Content Manipulation

As of January 2016, over 99 million Brazilians had active Facebook accounts and 88 million were using the social network via mobile technology.[70] Blogs and social networking platforms have become important instruments for citizen journalists and others to access information, defend civil rights, and express political points of view. Brazilians can read news from national and international sources, without government restriction. Within such a diverse media landscape, some content providers are neutral and others show bias towards or against the government.

Although self-censorship is less pervasive in Brazil than in some neighboring countries, the ongoing use of threats, intimidation, and violence against online journalists and independent bloggers in certain areas of the country has contributed to pockets of self-censorship (see Intimidation and Violence).[71]

New blogs in Brazil have no significant difficulty in maintaining themse es online. The Brazilian government has a past history of collecting high taxes on any service, thus bringing the costs of internet and host providing services slightly higher than the international average.[72] There are no sanctions for not following a specific edi orial orientation. According to Article 19 of Marco Civil, website owners can only be held liable for content generated by third parties if, after specific judicial o der, they do not comply with the requested measures in a timely manner.[73]

Ever since the approval of the Marco Civil, the principle of Network Neutrality has been incorporated

67 Brazilian Superior Court of Justice (STJ), Appeals to the Superior Court No. 1501187 / RJ (December 16, 2014), 1337990 / SP (August 21 2014); Interlocutory Appeals No. 484995 / RJ, 1349961 / MG (September 16, 2014), 305681 / RJ (September 4, 2009), http://bit.ly/1NQa7Tg.

68 Appeal to the Superior Court of Justice No. 1337990 / SP (August 21, 2014), http://bit.ly/1NQa7Tg.

69 Senado Federal, "Conselho de Comunicação Social defende sigilo da fonte jornalística," News release, September 14, 2009, http://bit.ly/1iO7y71; See also: Instituto de Tecnologia e Sociedade, "Direito ao esquecimento: o mundo todo precise esquecer?" *Brasil Post* (blog), August 8, 2015, http://bit.ly/1Hofb7Y; See also the Proposed Bills: Câmara dos Deputados, Projeto de Lei 7881/2014, http://bit.ly/1QAItH8; and Câmara dos Deputados, Projeto de Lei 215/2015, http://bit.ly/1JjdKNY.

70 Melissa Cruz, "Facebook revela dados do Brasil na CPBR9 e WhatsApp 'vira ZapZap'" [Facebook reveals Brazil data at CPBR9], *Techtudo*, January 28, 2016, http://glo.bo/1WiPBx5.

71 "Violência contra jornalistas aumentou em 2015, diz relatório da Fenaj" [Violence against journalist increased in 2015, says Fenaj report], *Folha de S. Paolo*, January 21, 2016, http://bit.ly/2bRvZgB.

72 "For shared plans, national corporate hosting prices averages between US$ 4.85 to US$ 8.9 per month, for the beginners' plan. It is possible to reduce costs by choosing a longer plan, though. Amongst the most economic plans are HostGator hosting, at US$ 2.85/month for the triennial plan, UOL Host, at US$2.82/month for the annual plan" (currency conversion and translation by the author). See: "Cuanto custa ter um site?" [How Much does a site cost?], August 28, 2015, http://bit.ly/1XfVZW3.

73 Law 10.406, January 10, 2002, Art.932, V, http://bit.ly/1drzx5j.

into Brazilian law. Enacted in May 2016, a new decree regulating the Marco Civil solidified the rules that prohibit the discrimination or degradation of traffic for comme cial purposes while permitting it for emergency and public calamity situations.[74] Zero-rating and Facebook's Free Basics program[75] are thus considered to be barred by this new legislation, and any notice of violation of said principle by companies may be investigated and sanctioned.[76] However, zero-rating is still a common practice among larger mobile internet companies.[77]

Digital Activism

Social media platforms such as Facebook and Twitter continue to play a central role in civic activism in Brazil. Following a historically tight presidential election in 2014, general frustration over the economy and a massive corruption scandal involving the state-run oil company has contributed to widespread discontent with the government since late 2014. Catalyzed by social media, massive protests in early 2015 brought millions of citizens to the streets to express their political positions, both for and against the government in office.

New protests brewed with the development of a criminal investigation involving the former president Luiz Inácio "Lula" da Silva and the suspension of President Dilma Rousseff from office. In Ma ch 2016, Brazil had one of its largest demonstrations, attracting over six million citizens to city streets all over the country, asking for Rousseff's impeachment.[78] All major groups involved in the protests, such as "Movimento Brasil Livre" and "Vem Pra Rua," had very active profiles on social media, which have been crucial to the wide publicity around the demonstrations. On the other hand, the movement in favor of President Rousseff was also supported by social media platforms, with demonstrations all around the country.[79]

Citizen activism, however, is not merely limited to organizing street protests. Citizens increasingly engage with formal government platforms to express opinions and shape the design and implementation of legislation. For example, the regulation phase of Marco Civil has been marked by high levels of public consultation and democratic participation online—elements that were also present during the drafting of the original legislation. The Ministry of Justice launched the second phase of a public consultation in January 2016 to assess views from citizens, academics, businesses and civil society organizations, concerning the fi st draft regulation of the Marco Civil. The platform garnered more than 1,500 comments and contributions within 30 days, with roughly 10,000 visits in total. During the fi st phase of the debate the platform received more than 60,000 visits and close to 1,200 comments.[80]

74 Decree 8.771, May 11, 2016, http://bit.ly/2c7Iqqv.

75 Internet.org changed its name to Free Basics in September 2015.

76 Pedro Vilela, "O que muda com o decreto de regulamentação do Marco Civil?" [What changes with the decree regulating Marco Civil?], Instituto de Referência em Internet e Sociedade, May 13, 2016, http://bit.ly/2bLHR39.

77 Rafael Bucco, "América Móvil reavalia oferta de zero-rating no Brasil," [America Movil reevaluates zero-rating in Brazil], *Telesíntese*, August 2, 2016, http://bit.ly/2crx2sB.

78 For an interactive map of the protests, see: "Map of demonstrations against Dilma, 13/03," Globo.com, accessed May 30, 2016, http://bit.ly/1Rf6RTK.

79 Simon Romero, "Protesters Across Brazil Call for President Dilma Rousseff's Ouster," *The New York Times*, March 13, 2016, http://nyti.ms/1rPLsoO.

80 "Começa 2ª fase da Consulta Pública do Decreto do Marco Civil da Internet," [Second phase of the public consultation on the Marco Civil decree begins], *Jota,* January 30, 2016, http://bit.ly/1R5VCvd; See also: Ministry of Justice, "Debate sobre o decreto do Marco Civil da Internet finaliza com mais de 1.500 comentários" [Debate on Marco Civil Decree ends with more than 1,500 comments], March 3, 2016, http://bit.ly/2crE3tz.

Brazil is also a founding member of the Open Government Partnership—a global effort to increase transparency and accountability—and, as part of this effort, has significantly imp oved standards of access to public information in recent years, establishing a system whereby citizens are entitled to request information through an electronic system.[81]

Violations of User Rights

Brazil's Marco Civil Law established a framework for internet users' rights, but other legal provisions—such as criminal defamation laws and those restricting certain speech during elections—contribute to a legal environment where individuals can face prosecutions for what they write online. High levels of violence in Brazil's urban centers, coupled with impunity for many crimes, have contributed to one of the highest rates of violence against journalists in the region. In addition to attacks on print and broadcast journalists, at least two bloggers were killed between June 2015 and May 2016.

Legal Environment

Although Brazil adopted some of the most progressive legislation in the world related to internet governance with the enactment of Marco Civil, several competing legal provisions, such as laws criminalizing defamation and blasphemy and restricting speech around elections, continue to threaten users' rights online (see Content Removal).

The Brazilian Federal Constitution forbids anonymity but protects freedom of the press and freedom of speech, including cultural and religious expression.[82] Brazil made noteworthy progress in establishing a foundation for internet user rights with the passage of the Marco Civil Law, a so-called "Constitution for the Internet," signed into law in April 2014.[83] The groundbreaking legislation establishes the right to freedom of expression online, offers detailed privacy protections pertaining to personal data, guarantees net neutrality, and promises to uphold the participatory nature of the internet. On May 11, 2016, during her last hours in office befo e the impeachment process that suspended her from power, Dilma Rousseff signed into law the decree regulating the Marco Civil law.[84] The decree contains specific rules egarding net neutrality (see Media, Diversity, and Content Manipulation) and data protection measures (see Surveillance, Privacy, and Anonymity).

Nevertheless, Brazil continued to see instances of local officials bringing cha ges of defamation—which is a crime punishable by six months to two years in prison or a fine acco ding to the penal code—against bloggers and online journalists.[85] In October 2014, Article 19, a civil society organization, launched a campaign in Brazil to press for the decriminalization of defamation.[86]

Brazil has a long history of laws that combat discriminatory speech. Although people are rarely charged or imprisoned for racist or discriminatory speech, Brazilian law establishes penalties ranging from two to fi e years in prison for practicing or inciting discrimination based on race, ethnicity or

81 Open Government Partnership, "Brazil," accessed October 10, 2016, http://bit.ly/2d8fzoH.

82 Constituição Federal de 1988, [Federal Constitution of 1988], English translation: http://bit.ly/1iOdLz.

83 Law 12.965, April 23, 2014, http://bit.ly/1kxaoKm; See also English version by Carolina Rossini, distributed by CGI.Br at the end of Net Mundial event: http://bit.ly/1jerSOK.

84 Decree 8.771, May 11, 2016, http://bit.ly/2c7Iqqv.

85 Decree 2848/40, Penal Code, Art. 331, http://bit.ly/1OV4Vwj.

86 Article 19, "Brazil: Article 19 launches campaign to decriminalize defamation," Press release, October 29, 2014, http://bit.ly/1FwsNnz.

religion in the media or in other publications.[87] The "Azeredo Law," passed in November 2012, extended these penalties to online speech.[88] The Criminal Code further outlines punishment for vilifying or mocking religion, with penalties ranging from one month to one year in prison, although it is unclear whether these penalties have been applied online. In June 2015, representatives introduced a legislative initiative to Congress that seeks to increase the penalty for vilifying religion to four to eight years in prison.[89]

In April 2013, a Brazilian cybercrime law commonly referred to as the "Carolina Dieckmann Law" came into force. Nicknamed after actress Carolina Dieckmann, this legislation took center stage after nude photos of her were distributed online in early 2012.[90] The law criminalizes breaches of digital privacy such as computer intrusion, the "installation of vulnerabilities," and editing, obtaining, or deleting information—including credit card numbers—without authorization. The distribution, sale, production, or offer of programs or devices meant to facilitate these actions, or to interrupt ICT services, are also categorized as crimes. Associated punishments vary from fines o up to fi e years imprisonment.

In March 2016, significant criticism also sur ounded the approval of a report by a Parliamentary Inquiry Commission, which proposed a series of bills related to cybercrimes. The bills included changes to the original text of the Marco Civil, and were seen by civil rights activists as a threat to freedom of expression, privacy and several other digital rights.[91] On May 4, 2016, the Parliamentary Commission adopted the final eport with 17 votes in favor and six against.[92] While some of the initial proposals were dropped after significant acklash from civil society and activists, several of the six remaining bills continued to raise concerns among digital rights activists, including a proposal that would enable courts to order the blocking of websites and applications hosted outside the country that are primarily dedicated to crimes punishable with a minimum sentence of two years imprisonment (although the final ext clarified that instant messaging apps such as WhatsApp ould not be subject to blocking). Another proposal included broadening the scope of the computer intrusion crime under the "Carolina Dieckmann Law," which would punish any form of unauthorized access into a third-party device.[93]

Prosecutions and Detentions for Online Activities

Prosecutions for defamation continue to pose a threat to freedom of expression online in Brazil. In April 2014, the blogger Paulo Henrique Amorim was convicted of defamation for insulting Merval Pereira, a journalist for *O Globo*, whom he called a "bandit journalist." Although originally convicted to serve jail time, Amorim's jail sentence was commuted in favor of a fine f ten times the minimum

87 Law 9.459, May 13, 1997, Art. 20, http://bit.ly/2dYnwN3.

88 Law 12.735, November 30, 2012, Art.1, http://bit.ly/2d8flO .

89 Fernando Diniz, "Após Parada Gay, "Cristofobia" pode virar crime hediondo," [After Gay Parade, 'Christphobia' could become a heinous crime], *Terra*, June 8, 2015, http://bit.ly/1cIAVDW.

90 "After 13 Years, Brazil approves two cybercrime laws at once," *Linha Defensiva*, November 7, 2012, http://bit.ly/1NWuC04.

91 Andrew Fishman, "Propostas da CPI dos Crimes Ciberneticos ameaçam a Internet livre para 200 milhões de pessoas," [Cybercrime proposals threaten free internet for 200 million people], *The Intercept*, April 26, 2016, http://bit.ly/1SIrFAB.

92 Câmara dos Deputados, [Chamber of Deputies], "Conheça as propostas do Relatório Final da CPICIBER," [See the proposals of the final eport by CPICIBER], accessed May 9, 2016, http://bit.ly/2dLfiG .

93 José Antonio Miracle, "Relatório final da CPI dos Crimes Cibe néticos gera discussão," [Final report generates discussion], May 13, 2016, http://bit.ly/2e9MUgk; see also: Coletivo Intervozes, "CPI de crimes cibernéticos aprova relatório que ataca liberdade na internet," [Commission approves report that attacks freedom online], *Carta Capital,* May 6, 2016, http://bit.ly/2dl03V3.

salary to be paid to a public or private social impact institution. Amorim's lawyer stated that her client would appeal the decision.[94] More recently in July 2015, blogger Paulo Cezar de Andrade Prado was arrested after the president of a local soccer club filed a complaint against him. During the investigation, police reportedly found that he had not served a previous criminal defamation conviction for criticizing a lawyer in a blog post and calling him incompetent. As a result, he was sent to jail for four months.[95]

In the midst of ongoing tensions between WhatsApp and Brazilian law enforcement, Facebook's Vice-President in Latin America, Diego Dzodan, was arrested and briefly detained on Ma ch 1, 2016. A judge in the state of Sergipe issued the order, after the company did not comply with multiple requests to hand over WhatsApp user data linked to an organized crime and drug trafficking case. The judge had imposed fines f around US$ 12,500 and then US$250,000 to Facebook, which stated that its use encryption on the app's messages made compliance with the order virtually impossible. As Dzodan later defended, "The way that information is encrypted from one cellphone to another, there is no information stored that could be handed over to authorities."[96] The detention did not last long, as a higher instance judge ordered Dzodan's release the following day.[97] In May 2016, however, the same judge involved in this case ordered the blocking of WhatsApp for 72 hours (see Blocking and Filtering).

Surveillance, Privacy, and Anonymity

The Brazilian Constitution explicitly forbids anonymity.[98] Although in practice, anonymous speech online is common, judges have occasionally referred to the constitution as a basis for limiting certain instances of anonymous speech. Other judges, however, have upheld anonymous speech on the grounds that it is important for free expression and privacy, ruling that anonymous posts online are protected as long as it is possible to technically trace the speech through IP addresses. The Brazilian Superior Court of Justice (STJ) has held that identification th ough IP address is a "reasonably effective means for identification" and cor esponds to "average diligence" expected from internet providers.[99]

Several legal provisions also place restrictions on anonymity in Brazil. Real-name registration is required for individuals or legal entities in order to purchase mobile phones or to access private internet connections, although the use of pseudonyms in discussion forums across the web is quite common. Lawmakers have urged further restrictions on anonymity with regard to public access points such as LAN houses, suggesting that internet communications should be recorded in order to prevent cybercrimes. Several pieces of legislation of this kind already exist in São Paulo[100] and Rio

94 "Paulo Henrique Amorim é condenado por injúria a jornalista," [P. H. Amorim is condemned for insulting a journalist], *Folha de São Paulo*, April 29, 2014, http://bit.ly/1OV6sSR.

95 Committee to Protect Journalists, "CPJ calls on authorities to release imprisoned Brazilian blogger," September 15, 2015, http://bit.ly/2dl7mfm.

96 Reuters, "Facebook executive says Brazil jail stint won't slow company's growth," *The Guardian,* March 5, 2016, http://bit.ly/2fLn1qT.

97 "Polícia prende vice-presidente do Facebook na América Latina em SP" [Police arrests vice-president of Facebook in Latin America], *G1*, March 1, 2016, http://glo.bo/1TOtuyl.

98 Constituição Federal de 1988, art. 5, http://bit.ly/1FieR0R.

99 See Brazilian Superior Court of Justice Appeals to the Superior Court of Justice No. 1192208-MG, REsp 1186616-MG and REsp 1300161-RS.

100 Law 12228/06, http://bit.ly/1NvRBjT.

de Janeiro,[101] and a bill under debate in the Senate would require LAN houses to register all users and keep a directory of individual identification for an unspecified amount f time.[102] The Marco Civil requires internet service providers such as LAN houses to confidentially s ore connection records in a safe, controlled environment, for at least one year following the provision of the service.[103] Perhaps the most restrictive legislative proposal during this coverage period was introduced in July 2015, seeking to amend Marco Civil to require users to register their real-name and national registration number to post on social media or blogs.[104] Although the project was rejected in December 2015, it serves as an example of the significant ensions surrounding anonymity in Brazil.

Facebook's Government Requests Report states that between July and December 2015, the company received 1,655 requests for data related to 2,673 separate accounts and produced data for 41 percent of these requests.[105] Brazil consistently figu es among the list of countries that send the most requests for user data to Google and Twitter, following the United States and Japan.

Marco Civil Law treats privacy and data protection as fundamental rights, bans the disclosure of users' personal data to third parties—with the exception of police and judicial authorities—and requires providers to make privacy policies and terms of use clear and understandable.[106] Digital rights activists had raised some concerns about Marco Civil's data retention mandate, which imposes obligations on internet connection providers to keep records of theirs users' connection logs for 12 months, and for application providers to keep records of access for 6 months.[107] Regulations decreed on May 11, 2016 further clarified security measu es to be taken by providers regarding log-keeping, including how authorities must request users' data from intermediaries, the level of technical security said intermediaries must adopt to safeguard logs from being leaked, and other identification and security procedures to be undertaken by the professionals responsible for handling said data, such as the obligation for individual identification and for the use f two-factor authentication.[108]

In addition to the Marco Civil and the recent decree passed on May 11, a Privacy and Data Protection Bill is at an earlier stage of development. It aims to establish comprehensive data protection legislation with clear user rights regarding both government and private sector collection and use of data, and intermediary liability regarding the collection, storage and treatment of personal data. Like similar legislation overseas, such as the EU Data Protection Directive,[109] the bill calls for the establishment of a national Data Protection Authority. Unlike many data protection laws in other countries, however, this law specifically mentions in ernet data protection alongside more general provisions for personal data.[110] The latest draft for the bill was prepared following the debate on the enactment of Marco Civil, and after ten months of public consultation promoted through an interactive and

101 Rio de Janeiro Municipal Decree 36.207, September 12, 2012, http://bit.ly/1WB0trP.

102 Bill 28/2011, http://bit.ly/1OxjBE8.

103 Marco Civil da Internet, Art. 13, http://bit.ly/1kxaoKm.

104 Bill 1879/2015, http://bit.ly/1MBSghD; See also: "Fim do anonimato: projeto de lei quer exigir CPF para comentar em blogs e redes sociais," [End of anonymity: legal project seeks to require CPF in order], *Technoblog*, http://bit.ly/1MWF9Vh.

105 "Brazil Requests for Data," Facebook Government Requests Report, July-December 2015, http://bit.ly/2esMAMD.

106 Law No. 12.965, Government of Brazil, April 23, 2014. English version by Carolina Rossini, distributed by CGI.Br at the end of Net Mundial event, available at http://bit.ly/1jerSOK

107 Coding Rights and Instituto Beta para Internet e a Democracia, "Nota Técnica: Retenção de Registros de Conexão e Aplicações," [Technical note: Retention of connection and application logs], accessed October 12, 2016, http://bit.ly/2egPy7C.

108 Decree 8.771, May 11, 2016, http://bit.ly/2c7Iqqv; See also: Artigo 19, "Regulamentação do Marco Civil da Internet é um avanço," [Regulation of Marco Civil is a breakthrough], May 20, 2016, http://bit.ly/2dYbhjf.

109 Directive 95/46/EC, 24 October 1995, http://bit.ly/1Oxk8py.

110 Ministério da Justiça, "Anteprojeto de Lei para a Proteção de Dados Pessoais" [Legal Proposal for the Protection of Personal Data], accessed March 25, 2016, http://bit.ly/1PQ0LpT.

open platform created by the Brazilian Ministry of Justice, which received over 1.3 million contributions from a variety of civil society sectors.[111] On May 13, 2016 the draft bill was sent to Congress and has undergone discussion within several commissions.[112]

The Brazilian government also seems to be increasing its capacity for surveillance, including national production of surveillance equipment. The country's defense budget forecast a US$10 billion expansion before 2020, partly investing in technology such as drones. The government, which has invested US$900 million dollars in security equipment, mostly because of the World Cup of 2014, hopes to continue using such equipment for widespread surveillance for the 2016 Olympic and Paralympic Games and beyond.[113]

Intimidation and Violence

Threats, intimidation, and violence against online journalists and bloggers still constitute a major restriction on freedom of expression and human rights in Brazil. At least two bloggers and three other journalists were killed during the coverage period,[114] and many other journalists and online activists reported harassment, threats, censorship, and physical assault.

Most of the murder victims were reportedly targeted for covering local corruption-related scandals. On November 13, 2015 blogger Ítalo Eduardo Diniz Barros was murdered as he walked on a major road of his town, Governador Nunes Freira, in the state of Maranhão. Diniz was a press officer for the town mayor and had been blogging about scandals and wrongdoings by other local politicians, and his acquaintances reported that he had been receiving death threats since 2012.[115] On April 9, 2016, Manoel Messias Pereira, the owner of news portal sediverte.com, was also shot dead in the state of Maranhão. More recently, on July 24, 2016, João Miranda do Carmo, a crime reporter who owned local news website SAD Sem Censura, was shot outside his home in the state of Goiás. He had reported threats linked to his reporting.[116]

Brazil has kept the 11th position on the Committee to Protect Journalists' Impunity Index, which tracks countries where journalists are murdered and killers run free. In a meeting with a CPJ delegation in 2014, President Dilma Rousseff committed to support legislative initiatives to federalize the competence for judging crimes against freedom of expression and to adopt a "zero tolerance" policy.[117] Since then, the conviction in 2015 of the murderers of José Roberto Ornelas de Lemos, the administrative director of the daily *Hora H,* has been considered a benchmark for justice and human rights. Lemos was shot at least 41 times in 2013 after writing about the spread of militias allegedly led by corrupt police office s in the suburb of Nova Iguaçu. In November 2015, police arrested six

111 Pedro Peduzzi, "MJ finaliza no a versão de anteprojeto sobre proteção de dados na internet" [Ministry of Justice finalizes new version of internet data protection bill], *Agencia Brasil,* October 19, 2015, http://bit.ly/1OHUcX6.

112 Bill 5276/16, accessed August 16, 2016, http://bit.ly/1TujEke.

113 Lorien Olive and Orlando Guzman, "The scary history and future of Brazil's booming drone market," *Fusion,* August 24, 2015, http://fus.in/1h8T5RF; See also: Joao Paolo Vicente, "Como as Olimpíadas ajudaram o Brasil a aumentar seu aparato de vigilância social," [How the Olympics helped Brazil to increase its social surveillance apparatus], *Motherboard,* July 27, 2016, http://bit.ly/2a6WkdW; Artigo 19, "Da Cibersegurança à Ciberguerra – o desenvolvimento de políticas de vigilância no Brasil" [From cybersecurity to cyberwar: the development of surveillance policies in Brazil], March 10, 2016, http://bit.ly/2d89KI7.

114 Reporters Without Borders, Journalists Killed 2015-2016, http://bit.ly/2dXzwMD; See also: Committee to Protect Journalists, "Journalists Killed in Brazil," http://bit.ly/1LN0btX.

115 Committee to Protect Journalists, "Ítalo Eduardo Diniz Barros," November 13, 2015, http://bit.ly/1Uq4sX8.

116 Reporters Without Borders, "Website owner is third journalist murdered in Brazil in 2016," July 26, 2016, http://bit.ly/2bCgkXx.

117 Committee to Protect Journalists, "Getting Away With Murder," October 8, 2015, http://bit.ly/1G1HEGQ.

people accused of running a militia believed to be directly linked to Lemos' murder. The arrests also resulted in the creation of a new homicide division in the city.[118] However, most condemnations still only target the direct perpetrators of these crimes, allowing their planners to escape justice.

Harassment during political coverage is also a serious concern in Brazil. Online bloggers and journalists who work in poor or rural areas and are not linked to major urban media outlets may face more harassment because they lack visibility and support. Under such circumstances, authorities feel little pressure to solve attacks on the provincial press. Unsolved attacks on journalists may in turn dissuade local reporters from investigating crime and corruption in their regions.[119]

Technical Attacks

Although the government has made efforts to strengthen cybersecurity, Brazil remains the top source and target of cyberattacks in Latin America.[120] While their peers elsewhere usually concentrate on trans-border, global attacks, Brazilian hackers favor local operations, relying on a perception of impunity and on an expansive basis of potential victims.[121] They mostly use surface web, forums, social networks and apps to facilitate their activities, and share know-how, ranging from malware development to phishing, banking fraud activities and botnets. Attacks seemed to escalate during the coverage period, as national hackers have been developing underground connections with more experienced criminals, especially in Russia and Eastern Europe.[122]

In September 2015, *Reporter Brasil*, a nonprofit association f journalists, reported cyberattacks to its platform and website. A series of investigative reports on the fight against fo ced labor and complaints against major companies in the food industry were altered or deleted.[123]

The financial sec or was the main target for hackers, followed by the chemical, manufacturing and mining industries.[124] A report published by the Brazilian Banking Federation in December 2015 found that, despite an investment of some US$500 million to fight cybe crime, banks have borne an equal amount of electronic fraud-related losses.[125] Traditional attacks related to phishing and malicious downloads run in tandem with more specific vulnerabilities such as pe nicious extensions or plug-ins for Google Chrome and Mozilla Firefox, the most popular internet browsers in Brazil.[126] Mobile phones, tablets, wearables and smart home appliances have also grown as a common target for offenders, since users tend to be more reckless in providing protective tools for such products.

118 Andrew Downie, "Amid rising violence in Brazil, convictions in journalists' murders are cause for optimism," Committee to Protect Journalists, February 29, 2016, http://bit.ly/1MHdHtS .

119 John Otis, "Bloggers Targeted as Murders Spike in Brazil," Committee to Protect Journalists, February 2013, http://bit.ly/1LzzPt0.

120 "Brasil é o terceiro país que mais realiza ataques cibernéticos no mundo," [Brazil is the third country that carries out the most cyberattacks in the world], August 19, 2015, http://bit.ly/1YwiDrV.

121 "Beaches, carnivals and cybercrime: Kaspersky Lab shares insights on Brazilian cyber underground," *Kaspersky Lab*, November 11, 2015, http://bit.ly/1MBkjdj.

122 Christian Plumb, "Latam cyberattacks rise as Peru, Brazil hackers link up with Russians," *Reuters,* August 28, 2015, http://reut.rs/1RyqAOl.

123 "Reporter Brasil sofre pesado ataque digital" [Reporter Brasil suffers heavy digital attack], *Reporter Brasil*, September 19, 2015, http://bit.ly/1gGZB1n.

124 "Ascending the Ranks: The Brazilian Cybercriminal Underground in 2015," *Trend Micro,* January 12, 2016, http://bit.ly/1o5txbh.

125 Claudia Tozetto, "Cibercrime faz bancos perderem R$ 1,8 bilhão," [Cybercrime makes banks lose R$1.8 billion], *O Estado de São Paulo,* December 21, 2015, http://bit.ly/1PjGmKh.

126 "Largest Cybercrime Threats in Brazil," *Tech in Brazil,* April 8, 2015, http://bit.ly/1py3z1l.

The National Agency of Telecommunications (ANATEL), Brazil's main regulatory body for the telecommunication sector, suffered a major DDoS attack at the end of April 2016, remaining offline for over 24 hours. The attack followed the announcement by major ISPs that they would introduce data caps for fi ed broadband, causing major uproar among all sectors of Brazilian society.[127]

Brazilian authorities have made some efforts to increase cybersecurity and invest more resources in overcoming current obstacles. Since 2008, Brazil has engaged in a multi-stakeholder debate to develop its cybersecurity agenda, which resulted in the opening of a National Cyber Defense Command, and a National School for Cyber Defense aimed at preparing military personnel for the use of cyber tools on national defense.[128]

127 Olhar Digital, "Anatel sofre ataque hacker e tem serviços online derrubados" [Anatel suffers hacking attack and online services are brought down], *Olhar Digital*, April 22, 2016, http://bit.ly/2cdjPz9.

128 Andrea Barreto, "Brazilian Armed Forces Strengthen the Nation's Cybersecurity Defense," *Diálogo Digital Military Magazine, April 14, 2015,* http://bit.ly/1FinqJ7; See also: "EB - Defesa Cibernética entra em nova fase" [Cyber defense enters new phase], Defesanet, July 24, 2015, http://bit.ly/1o5CtNX.

Freedom House

Cambodia

	2015	2016
Internet Freedom Status	Partly Free	Partly Free
Obstacles to Access (0-25)	14	15
Limits on Content (0-35)	15	15
Violations of User Rights (0-40)	19	22
TOTAL* (0-100)	**48**	**52**

* 0=most free, 100=least free

Population:	**15.6 million**
Internet Penetration 2015 (ITU):	**19 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- The telecommunications law passed in November 2015 increased the government's au-thority over the industry and granted officials o erbroad surveillance powers (see **Legal Environment**).
- In March 2016, a court sentenced 25-year-old student Kong Raya to 18 months in prison for posting a comment against Hun Sen's "cheap regime" on Facebook (see **Prosecutions and Detentions for Online Activities**).
- Opposition leader Sam Rainsy, Senator Hong Sok Hour, and at least two supporters face criminal charges for posting allegedly inaccurate historical documents on Facebook in 2015 (see **Prosecutions and Detentions for Online Activities**).
- Prime Minister Hun Sen publicly embraced social media, launched his own app, and amended a traffic law a ter Facebook users complained of new safety requirements (see **Digital Activism**).

Introduction

Internet freedom declined following a number of arrests for online speech and the passage of a problematic telecommunications law with inadequate protections for user privacy.

Even so, the internet continues to be the nation's freest medium for sharing information. The number of internet and smartphone users continued to rise during the coverage period of this report.

The telecommunications law strengthens official po ers over telecommunications networks through the infrastructure and the regulator, and granted officials access o telecommunications company data without oversight, posing a threat to the privacy of individual users.[1] A cybercrime law fi st announced in 2012 underwent some revision, but a second draft leaked in 2015 retained vague language that could be abused to suppress free expression.

Hun Sen urged government officials o use Facebook and social media to engage with citizens,[2] and even launched his own application to keep users up to date with his news.[3] At the same time, he threatened Facebook critics and reminded internet users that the government is monitoring their activity. Several arrests and criminal charges were documented in relation to legitimate online speech, marking a disturbing new trend that threatens to increase self-censorship.

Obstacles to Access

Increasing smartphone penetration in both urban and rural areas has allowed greater access to the internet across Cambodia. As in past years, access remained lower in rural areas than in urban areas, while data indicated individuals with education are more likely to have smartphones and to use the internet.

Availability and Ease of Access

Mobile phone penetration was almost 100 percent in 2015;[4] the International Telecommunication Union estimated internet penetration at 20 percent.[5] Advancements in internet technology have made the web more accessible in Cambodia. The average download speed was 9.04 Mbps in 2015,[6] up from 5.8 Mbps in 2014 but well below the global average of 18.2 Mbps.[7] Average monthly subscription rates were between US$ 10 and US$ 20, depending on the connection speed, compared to a GDP per capita of US$ 86 per month.[8]

1 Mech Dara and Kuch Naren, 'Draft Telecoms Law Gives Gov't Broad Spying Powers,' *The Cambodia Daily,* November 27, 2015, http://bit.ly/1NRKBrc.

2 Phorn Bopha, 'Hun Sen Urges Party Members To Connect With Cambodians Online,' *Voice of America,* January 12, 2016, http://bit.ly/1QEFIIZ.

3 Khuon Narim, 'Keeping Up With Hun Sen? There a New App for that,' *The Cambodia Daily,* January 6, 2016, http://bit.ly/20s8QTA.

4 Kimchhoy Phong and Javier Sola, 'Mobile Phones and Internet in Cambodia 2015,' The Asia Foundation, November 30, 2015, http://bit.ly/1NlsZ9T.

5 Telecommunications Regulator of Cambodia, 'Internet Subscribers,' http://bit.ly/1mfBlqa; International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1cblxxY.

6 'Philippines ranks 21st of 22 Asian countries in Internet download speeds,' May 19, 2015, http://bit.ly/1N8bOvn.

7 Joshua Wilwohl, "Internet Speeds in Cambodia Faster Than Others in Region" *The Cambodia Daily,* May 6, 2014, http://bit.ly/1Q1emrW.

8 United Nations Development Programme, "About Cambodia", http://www.undp.org/content/cambodia/en/home/countryinfo/

At the end of 2015, the Open Institute reported that 52 percent of the population in urban areas own smartphones, a significant inc ease from the previous year's 39 percent, while 34 percent of the rural population own a smartphone, an increase from 21 percent.[9] Overall, smartphone penetration is now at 39.5 percent, and phones represent the only means of internet access for many users. Indeed, 29 percent of mobile subscribers report accessing the internet on their phones.[10] The Open Institute also found that the likelihood of smartphone ownership increased with an individual's level of education. Just 15 percent of individuals with no formal education owned a smartphone, compared to 82 percent among those with university education.[11]

Support for Khmer language applications on mobile phones has made it easier for Cambodians to connect. Among Cambodians aged 15 to 65, 63 percent had at least one phone with support for Khmer script, and 33 percent of users reported having read Khmer script on their own phones. Overall, there has been a 23 percent increase in the number of users with phones that support Khmer script, allowing individuals more access to the news as well as a great ability to communicate throughout Cambodia.[12] Men were slightly more likely to own such a device though, as 59 percent of women reported that their devices could support Khmer script, versus 68 percent of men.[13]

Restrictions on Connectivity

Internet usage has been constrained by poor infrastructure. The absence of an extensive landline network inhibits greater internet penetration, since the fi ed landlines which broadband internet services depend on are often unavailable in rural areas. ISPs develop their own infrastructure, and three have announced plans to construct submarine fibe -optic internet cables to connect to high-speed international connections (with one of those projects commissioned by the government). To date, however, none of the three have been completed.[14]

Insufficient electricit , often resulting in nationwide blackouts, imposes additional constraints on computer and internet use. Connections can also be extremely slow, especially in remote areas.

Three operators provide a backbone network in Cambodia totaling 26,411 km: Telecom Cambodia, Viettel (Cambodia) Pte. Ltd., and Cambodia Fiber Optica Cable Network.[15] These operators interconnect with smaller networks, allowing exchanges of information through Wi-Fi, LAN lines, or other means. Telecom Cambodia operates under the Ministry of Posts and Telecommunications of Cambodia (MPTC) and the Ministry of Finance.[16]

With the exception of one short-lived attempt by the NEC to ban SMS nationwide in advance of a

9 Kimchhoy Phong and Javier Sola, "Mobile Phones and Internet in Cambodia 2015," The Asia Foundation, November 30, 2015, http://bit.ly/1NlsZ9T.

10 Phong and Sola, "Mobile Phones and Internet in Cambodia 2015."

11 Phong and Sola, "Mobile Phones and Internet in Cambodia 2015."

12 Phong and Sola, "Mobile Phones and Internet in Cambodia 2015."

13 Phong and Sola, "Mobile Phones and Internet in Cambodia 2015."

14 Simon Henderson, "Internet Firm Inks Fiber Optic Deal, "*The Cambodia Daily,* June 13, 2014, http://bit.ly/1QoqOD9.

15 Ministry of Posts and Telecommunications, "September 2015 Fact Sheet."

16 World Bank, "Cambodia Services Trade: Performance and Regulatory Framework Assessment," July 2014, http://bit.ly/2errMWc 28-29

2007 election under a law prohibiting campaigning immediately before a vote,[17] no government shutdowns of internet or mobile access have been documented in Cambodia.

However, the telecommunications law passed during the coverage period of this report extended government control of the industry in ways which could facilitate service interruptions in the future. Under Article 7, the MPTC or other relevant ministries will have the authority to order telecommunications providers to "take necessary measures" in undefined ci cumstances of "force majeure." The law separately established an enforcement body of "telecommunications inspection officials" o police offenses under the law, with the authority to call in support from the armed forces.[18] These officials "hold po er to temporarily suspend telecoms fi ms' services and suspend or fi e their staff," according to local NGO LICADHO.[19]

ICT Market

The telecommunications market remains competitive since it opened to private investment in 2006.[20] In 2016, the Telecommunications Regulator of Cambodia reported 31 ISPs operating in Cambodia, and 7 mobile service providers, a decrease since 2014 following some consolidation.[21]

The telecommunications law passed during the coverage period of this report was intended to clarify and improve development and regulation of the sector, but critics said it introduced troubling penalties for constructing or operating telecommunications without a license, including fines and prison sentences of up to three years. Article 110 requires all telecommunications operators to reapply for licenses within a year of the law coming into effect.[22]

Regulatory Bodies

The Telecommunications Regulator of Cambodia (TRC) is the main regulatory body in Cambodia. Established by royal decree on September 20, 2012, the TRC is required to foster "regulations, policies, standards, instructions, and circulars to provide solutions to existing and future problems," as well as to set goals to develop the ICT market "out from the centrally and directly [sic] control of government" to "rely on the existence of multi-operators, multi-services and the opening of free and fair competition market."[23]

On November 30, 2015, the National Assembly passed a telecommunications law, the fi st of its kind in Cambodia, which significantly unde mined the body's stated goal of reducing centralized state control. The law, which the TRC worked with the MPTC to draft, established the ministry's ultimate authority over the regulator, and failed to introduce transparency or appeal procedures to ensure that decisions about licensing and other issues under its remit are fair.[24]

17 Norbert Klein, "Civil Society Organizations Said That The National Election Committee Caused Fear To The Citizen Who Are The Electorate," *Cambodia Mirror*, April 1, 2007, http://bit.ly/2eNDdmj

18 LICADHO, "Cambodia's Law on Telecommunications: A Legal Analysis," briefing, Ma ch 2016, https://www.licadho-cambodia.org/reports.php?perm=214.

19 LICADHO, "Cambodia's Law on Telecommunications: A Legal Analysis," briefing, Ma ch 2016.

20 World Bank, "Cambodia Services Trade: Performance and Regulatory Framework Assessment," July 2014, 30.

21 Telecommunication Regulator of Cambodia, "Licenses," http://bit.ly/1TmPxM9.

22 LICADHO, "Cambodia's Law on Telecommunications: A Legal Analysis," briefing, Ma ch 2016.

23 Telecommunication Regulator of Cambodia, "Background," http://bit.ly/1XukaPb.

24 'Law on Telecommunications,' *Sithi Portal, February 17, 2017,* http://bit.ly/1XwQ2CC.

Limits on Content

With the passage of the telecommunications law and ongoing discussions about a pending cybercrime law, the Cambodian government is slowly instating legal limits on what users are allowed to post on the internet. In lieu of these laws, however, the government has made public threats and arrests against those who post negative online comments about government officials, leading to increased self-censorship. However, users continue to actively engage on social media and the internet has become the second most important source for citizens seeking news, after television.

Blocking and Filtering

Websites showing pornography or sexually explicit images are subject to blocking in Cambodia on moral grounds. Politically motivated blocking has not yet been systematically applied, although it has been observed on a case by case basis. Blogs blocked for supporting the political opposition, such as *KI Media* and *Khmerization*, were available through at least some ISPs during the coverage period, indicating that censorship orders are unevenly executed.

Implementation of censorship is nontransparent, apparently based on informal communications between government officials and se vice providers, which provide no avenue for appeal. In 2011, for example, then-Minister of Posts and Telecommunication So Khun asked mobile phone operators to "cooperate" in blocking websites "that affect Khmer morality and tradition and the government," according to *The Phnom Penh Post,* citing internal MPTC minutes.[25]

Social media platforms such as YouTube, Facebook, and Twitter, were freely available in 2015 and 2016, and provided a platform for significant go ernment engagement (see Media, Diversity, and Content Manipulation).

Content Removal

The extent of content removal remains difficult o assess, as the process is unofficial and nontran - parent. In January 2016, a Facebook account was deactivated after posting doctored versions of Prime Minister Hun Sen's holiday photos.[26] Officials implied the owner f the account, based outside Cambodia, was affilia ed with the political opposition.[27]

Media, Diversity, and Content Manipulation

The internet has quickly become one of the main sources of news and information for Cambodian citizens. Both independent and government-controlled media organizations have a strong online presence in Cambodia, providing access to news, photographs, and videos that are easily shareable on social media platforms. Content on non government-controlled news outlets are not regulated and are able to provide unbiased information to citizens and foreigners. In an Open Institute study, 25 percent of respondents listed either Facebook or the internet as their most important source of

25 Thomas Miller, "Ministry Denies Blocking Website," *Phnom Penh Post,* February 16, 2011, http://www.phnompenhpost.com/national/ministry-denies-blocking-website.

26 Vong Sokheng, 'Fake family photos upset PM,' *The Phnom Penh Post,* January 1, 2016, http://bit.ly/1nF6uEf.

27 Bun, Sengkong, 'Facebook Photoshopper dual national: ministry', *The Phnom Penh Post,* January 18, 2016, *http://bit.ly/24hvccl*

news, second only to television at 32 percent.[28] In addition, 29 percent of individuals cited obtaining information about events in Cambodia as a factor in their decision to join Facebook.

In September 2015, the cabinet of Prime Minister Hun Sen confi med that he was an avid Facebook user, after years of denying that the *"Samdech Hun Sen, Cambodian Prime Minister"* page was his official acebook account. It is unclear why the prime minister did not previously acknowledge the page, although confi mation came shortly after the account reached over one million 'likes'. After his page's fans passed three million in March 2016, a post on his page read: "I would like to thank my national compatriots and youths in the country and overseas who support my Facebook page… Facebook has brought me closer with people and allowed me to listen and receive more requests from them."[29] The same month, *The Phnom Penh Post* alleged that only 20 percent of the page's 'likes' in February and March 2016 came from within the country, with the rest reportedly coming from paid 'click farms' abroad.[30]

The prime minister's belief that the internet has brought him closer to the Cambodian people has even driven him to create his own mobile application and encourage social media use amongst civil servants.[31] While government engagement on social media can be positive, it has also raised questions about government regulation and manipulation of content. While citizens' feedback on such platforms can lead to positive change, the Royal Government of Cambodia has also begun to be very vocal, cautioning users about what they post.[32]

In December 2015, after holiday photos of Prime Minister Hun Sen and his wife doctored to cause offense appeared on Facebook, Hun Sen threatened social media users with possible prosecution, announcing that "all actions that ruin my honor and my family's honor, as a prime minister of a country, those must be responsible before the law."[33] On December 28, during a graduation speech given at the Royal University of Law and Economics in Phnom Penh, Hun Sen warned that Facebook users who criticize government policy on sensitive issues, or resort to personal insults, could be traced in a matter of hours. He also referenced the conviction of university student Kong Raya (see Prosecutions and Detentions for Online Activities), saying, "the color revolutionaries were arrested immediately."[34] On February 10, 2016, in response to a factsheet on digital rights released by local NGO the Cambodian Center for Human Rights (CCHR), government spokesperson Phay Siphan reiterated that the government has a duty to arrest citizens if they "disrespect" Hun Sen.[35]

Other warnings targeted the main opposition Cambodia National Rescue Party (CNRP), leading CNRP Deputy President Kem Sokha to urge youth members of the party to exercise caution with

28 Kimchhoy Phong and Javier Sola, "Mobile Phones and Internet in Cambodia 2015," The Asia Foundation, November 30, 2015, http://bit.ly/1NlsZ9T.

29 Daniel Nass and Shaun Turton, 'Only 20 per cent of PM's recent Facebook 'likes' from Cambodia,' *The Phnom Penh Post,* March 9, 2016, http://bit.ly/1M5DMlT.

30 Nass and Turton, 'Only 20 per cent of PM's recent Facebook 'likes' from Cambodia.'

31 Joshua Wilwohl, 'Follow The Leader: Cambodians…Making Big Waves on Social Media," *Forbes,* February 4, 2016, http://onforb.es/1QvMUSd.

32 Pech Sotheary, 'Hun Sen Warns Facebook users that he's watching,' *The Phnom Penh Post,* December 29, 2015, http://bit.ly/1PuX6OC.

33 Kuch Naren, "Doctored Image of First Lady Draws OM's Ire," January 1, 2016, http://bit.ly/1olfyzf.

34 Pech Sotheary, 'Hun Sen warns Facebook users that he's watching,' *The Phnom Penh Post*, 15 December 2015. Available at: http://bit.ly/1PuX6OC.

35 Pech Sotheary, "NGO notes uptick in gov't 'threats' against online posters," *The Phnom Penh Post*, February 10, 2016, http://www.phnompenhpost.com/national/ngo-notes-uptick-govt-threats-against-online-posters.

their social media use. "We should not play the game they're drawing for us… especially on Facebook," he told supporters.[36]

These warnings, particularly when uttered by the prime minister, have already led to an increase in self-censorship and threaten to infringe further upon online freedoms in years to come. In an online survey conducted by CCHR, internet users were asked to rate the freedom of expression they exercise on social media, from 0 or none at all, to 10, meaning full freedom. The average score from 403 responses was 4.83, demonstrating a troubling culture of self-censorship among Cambodia's nascent online community.

Digital Activism

The government's increased engagement on Facebook and social media has entailed both positive and negative outcomes. Internet users were responsible for a quick change to a Land Traffic Law put in place on January 1, 2016. The law tightened road safety guidelines, and many individuals were pulled over and cited on the fi st day.[37] After many expressed anger on social media, the prime minister amended the law a week after it was put into effect, in what observers described as a regressive, though populist, move.[38] The amendments removed requirements for motorbike drivers with smaller engines to get a license. Though a remarkable instance of the government changing the law in direct response to social media activism, critics were concerned by the prime minister's willingness to change laws on his own initiative, rather than via an official legislati e process.

Digital activism is not always so effective. In May 2016, members of the indigenous Pu Nong communities in eastern Mondulkiri province posted photos of themselves on Facebook holding placards demanding the release of jailed human rights activists.[39] Local police questioned villagers about whether the act had been coordinated by civil society groups.

Violations of User Rights

Freedom of expression is guaranteed under Cambodia's constitution. Yet the 2010 penal code has been used to threaten and arrest bloggers, social media users, and journalists. The new telecommunications law paves the way for increasing government intrusion into digital privacy. Despite objections from civil society, the law retains certain alarming provisions contained in a draft leaked in 2014, including one allowing government surveillance of communications without a warrant. Additionally, MPTC will have the power to direct private providers to hand over data, systems and equipment. A pending cybercrime law could potentially further stifle user rights.

Legal Environment

Article 41 of the Constitution of the Kingdom of Cambodia guarantees freedom of expression and

36 Mech Dara and Alex Willemyns, 'Sokha warns youth against provocative use of Facebook' *The Cambodia Daily*, 4 December 2015. Available at: http://bit.ly/20mhB1m.

37 Kuch Naren and Taylor O'Connelle, 'Consulting Facebook, PM Changes Traffic Laws' *The Cambodia* Daily, January 8, 2016, http://bit.ly/1o92GMz.

38 Naren and O'Connelle, 'Consulting Facebook, PM Changes Traffic Laws'

39 Brooks Boliek, 'Cambodian Government Attempts to Silence Dissent as Legal War Rages', *Radio Free Asia,* 17 May 2016, Available at: http://bit.ly/1Uw536N.

the press.[40] These rights are further protected under Article 31, where the Universal Declaration on Human Rights (UDHR)[41] and the International Covenant on Civil and Political Rights (ICCPR) are recognized as forming part of national law.[42] Article 19 of both the UDHR and ICCPR guarantee a universal right to freedom of expression. However, this right is threatened under the Criminal Code of the Kingdom of Cambodia due to the vagueness of certain provisions.[43] Individuals can be arrested for disturbing public order or affecting the dignity of individuals and public officials, which is o erly subjective.[44]

On November 30, 2015, the National Assembly formally adopted a new draft of the Telecommunications Law, "formulated with the purpose of defending the rightful benefits f all parties concerned," including telecom operators, users, and the government.[45] The law came into effect on December 17, 2015, having been promulgated by King Norodom Sihamoni following a rushed legislative process that lacked transparency and consultation. The law increases government control over the sector and threatens the rights to privacy and freedom of expression (see, Surveillance, Privacy, and Anonymity). Using telecommunications to plan criminal activity or damage property carries a possible prison sentence of up to six months and fines f up to KHR 40 million (US$ 8,800) under Articles 93–96. Article 80 punishes the "establishment, installation and utilization of equipment in the telecommunications sector" with 7 to 15 years in prison "if these acts lead to national insecurity." Critics feared the heavy penalties attached to this vaguely defined clause could be abused o prosecute legitimate activity.

In 2012, the government announced its intention to adopt Cambodia's fi st cybercrime law to regulate online content and to prevent the "ill-willed" from spreading false information.[46] Attempts by civil society to acquire a copy of the draft law from the government were met with vague, noncommittal answers. The draft was then leaked in April 2014, though the government refused to release an official ersion. Some of the most problematic provisions under Article 28 sought to prohibit content deemed to "generate insecurity," damage "moral and cultural values," including defamation and slander, or undermine "the integrity of any governmental agencies." Article 35 threatened to dissolve legal entities, like civil society organizations, found to commit offenses under the law. Though some local news reports said the law might be scrapped, in May 2015, the Minister of Posts and Telecommunications announced that the law was still under consideration, and would include criminal sanctions for "people with bad intentions" who "criticize the government."[47]

The Ministry of Interior privately released a revised draft of the law to select NGOs in September and October 2015. The document was clearly a working draft, with some articles copied directly from the Council of Europe's Convention on Cybercrime, and some uncorrected article numbers that still corresponded to the fi st draft instead of the second. This raised questions regarding the document's

40 Article 41.

41 UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III), http://www.un.org/en/documents/udhr/.

42 Constitutional Council of the Kingdom of Cambodia, Decision No. 092/003/2007 (10 July 2007).

43 Human Rights Watch, 'Cambodia: New Penal Code Undercuts Free Speech,' December 23, 2010, http://bit.ly/1VJfUty.

44 Human Rights Watch, 'Cambodia: New Penal Code Undercuts Free Speech.'

45 Announcement by the Ministry of Posts and Telecommunications: National Assembly Adopted the Draft of Telecommunication Law http://bit.ly/1PTxahA

46 Bridget Di Certo and Kim Yuthana, 'The 'ill-willed' spark cyber law: officials , *The Phnom Penh Post*, 24 May 2012. Available at: http://bit.ly/1sW3Mvb.

47 Mech Dara, 'Cyber Law to Protect Gov't Honor, Ministry Says', *The Cambodia Daily*, 27 May 2015. Available at: http://bit.ly/1PfcTgS.

reliability and highlighted the shortcomings of leaking drafts in place of a more open and consultative legislative process.

Some troubling provisions were reported to have been removed from the second draft, including Article 28.[48]

Other provisions threatening digital rights were added. For example, Article 13(1) criminalizes obtaining confidential data even without malicious intent, meaning it could be an offence to receive it.[49] The crimes enumerated in the draft remain broadly defined, and ould introduce scope for abuse against perceived government opponents, in violation of national and international human rights guarantees. Moreover, most of the crimes are already punishable under the criminal code, rendering a new law unnecessary.

Prosecutions and Detentions for Online Activities

The coverage period of this report saw a dramatic increase in detentions for online activity. Between August 2015 and February 2016, at least seven people were arrested for posts or comments made online, and at least twenty-four were publically threatened with prosecution.[50] While some of the comments triggering prosecutions had threatened violence, other charges were clearly politically motivated, leading observers to fear that the government views criminal threats and legitimate criticism in the same category.

The conviction of 25-year-old student Kong Raya exemplifies the go ernment's stance toward negative comments.[51] Raya was charged with incitement based on a post on his personal Facebook account on August 7, 2015 that called for a "color revolution in order to change the cheap regime running Cambodian society." Observers said he was not politically influential, and Raya apologized, saying he had no intent to lead an uprising but was merely expressing his frustration with the government. On March 15, 2016, he was sentenced to 18 months in prison under Article 495 of the criminal code, "provocation to commit [a] crime."[52] Raya said he would appeal.

Other prosecutions relating to online content targeted the political opposition. On August 15, 2015, Hong Sok Hour, an opposition CNRP party senator, was detained in Prey Sar prison on charges of forgery and incitement.[53] Prime Minister Hun Sen had personally called for his arrest during a speech, which accused him of 'treasonously' posting a doctored version of a 1979 border treaty between Cambodia and Vietnam to the public Facebook page of CNRP President Sam Rainsy on August 12. The disputed border is the center of a long-running controversy, with the opposition claiming that the ruling party knowingly ceded territory to Vietnam.

Senators are immune from prosecution under the constitution, which gives them protection from

48 Shaun Turton, "Cybercrime law 2.0 nixes key provision," *The Phnom Pehn Post,* December 5, 2015, http://www.phnompenhpost.com/post-weekend/cybercrime-law-20-nixes-key-provision.

49 Cambodian Center for Human Rights, "Digital Wrongs? An Overview of the Situation of Digital Rights in Cambodia," briefing no e, February 2016, http://bit.ly/1SBxi3e. .

50 Cambodian Center for Human Rights, "Fact Sheet: Crackdown on Facebook Users Intensifies" February 2016, http://bit.ly/1TfVMBq.

51 Pech Sotheary, 'Student arrested after posting about revolution,' *The Phnom Penh Post,* August 24, 2015, http://www.phnompenhpost.com/national/student-arrested-after-posting-about-revolution.

52 Ouch Sony and Taylor O'Connell, 'Student Gets 18 Months for Call for 'Color Revolution", *The Cambodia Daily*, March 16, 2016 http://bit.ly/1SLu4uq

53 Taing Vida, 'Sok Hour defence balks at evidence demands,' *The Phnom Penh Post*, 27 November 2015. Available at: http://bit.ly/1JWYucq.

arrest except when approved by the Senate, or when caught during the commission of a criminal act. However, Sok Hour was charged with forgery of public documents, use of forged public documents, and provocation to commit crimes under Articles 629, 630, and 495 of the criminal code, which carry a maximum combined prison sentence of 17 years.[54] Sok Hour's defense team said he was unaware of any inaccuracies in his post when he made it, and that dissemination of a fake treaty does not amount to a criminal act. The Phnom Penh Municipal Court and the Court of Appeal rejected Sok Hour's requests for bail. Sok Hour appealed those decisions on health grounds, but the Supreme Court upheld the Court of Appeal's decision on March 4, 2016,[55] and he was still in prison in June 2016.

Police also issued arrest warrants for Sathya Sambath and Ung Chong Leang, the administrators of the Sam Rainsy Facebook page, on charges of conspiring to fake public documents, using fake documents, and incitement to cause serious social chaos.[56] The two men left the country, and Hun Sen has called for the men to return from their self-imposed exile and confess to the alleged conspiracy.[57]

Court officials also alleged that Sam Rainsy was an accomplice o the post, since it was made on his Facebook page, and demanded his appearance in court for questioning.[58] Rainsy separately went overseas after the Phnom Penh Municipal Court issued a warrant for his arrest on November 13, 2015. That warrant was in relation to charges of defamation and incitement that date back to 2008, but were announced less than 24 hours after Prime Minister Hun Sen threatened Rainsy with legal action via a video posted on Facebook.[59] On November 26, the European Parliament approved a resolution urging the Cambodian government to revoke the warrant and "drop all charges issued against opposition leader Sam Rainsy and CNRP members of the National Assembly and Senate," including CNRP activists and organisers.[60] Sam Rainsy was provisionally charged as an accomplice to forgery and incitement in Sok Hour's case on December 9, after he failed to appear in court.[61]

The Cambodia-Vietnam border was the focus of another prosecution during the coverage period. On November 20, 2015, police in Svay Rieng province arrested CNRP activist Sok Sam Ean on charges of incitement to commit a crime for posting on Facebook an image of a public document that suggested Cambodian territory had been lost. The document, the birth certifica e of an individual named Nhem Chhoeun dating from November 2004, listed the place of birth as Svay Rieng, Vietnam.[62] A CNRP city councilor, Norng Sarith, was also arrested and charged with forging the certifica e. Local police chief Pin Pirom said Sam Ean used his real name on Facebook, enabling him to be found within half an hour.

54 Taing Vida, 'Sok Hour defence balks at evidence demands,' *The Phnom Penh Post*, 27 November 2015. Available at: http://bit.ly/1JWYucq.

55 Kuch Naren, 'CNRP Senator Makes Case for Bail at Supreme Court,' *The Cambodia Daily*, 27 February 2016. Available at: http://bit.ly/1LUfjjs; Chhay Channyda,, 'Senator's final ail attempt shot down,' *The Phnom Penh Post*, 5 March 2016. Available at: http://goo.gl/0Jk85T.

56 May Titthara, 'Arrest Warrants Issued for Opposition Facebook Administrators' *The Khmer Times*, 1 December 2015. Available at: http://bit.ly/1PeRtpu.

57 Shaun Turton and Vong Sokheng, 'CNRP trio seek asylum' *The Phnom Penh Post*, 10 September 2015. Available at: http://bit.ly/1KD2AGw.

58 Mech Dara, 'Arrest Ordered for Rainsy Facebook,' *The Cambodian Daily*, 2 December 2015. Available at: http://bit.ly/207D1PD.

59 Phak Seangly and Shaun Turton, 'Sam Rainsy faces arrest warrant', *The Phnom Penh Post*, 14 November 2015, Available at: http://bit.ly/1XaL6GT

60 European Parliament resolution of 26 November 2015 on the political situation in Cambodia (2015/2969(RSP)) http://bit.ly/1P02K7Z

61 Khy Sovuthy and Alex Willemyns, 'Another Arrest Warrant Issued for Sam Rainsy,' *The Cambodia Daily,* 06 January 2016. Available at: http://bit.ly/1WfM5RM.

62 Phak Seangly, 'CNRP duo jailed for birth certifica e 'lies", *The Phnom Penh Post*, 21 November 2015. Available at: http://bit.ly/1W4FB8b.

Some of the comments subject to prosecution during the coverage period included violent threats. On September 28, 2015, student Tao Savoeun was arrested after threatening on Facebook to bomb his own graduation ceremony.[63] He later said he was expressing frustration that the ceremony had been repeatedly postponed, and did not intend to cause harm. He was charged with issuing a death threat under Article 233 of the criminal code and sentenced to 15 months of imprisonment, but released after one month following a written apology. In a contrasting case involving the Cambodia-Vietnam border, police arrested 27-year old construction worker Phorng Seyha on September 5, 2015 for a Facebook post threatening to kill Dr. Sok Touch, a scholar recruited by the government to do Cambodia-Vietnam border research.[64] Despite issuing a formal apology letter to Sok Touch, Phorng Seyha was held until February 2016, when he was sentenced to 18 months in prison, subsequently reduced to 6 months, and a fine f KHR 1 million (US$250).[65]

Surveillance, Privacy, and Anonymity

Surveillance of citizens' digital activity has not been technologically advanced in Cambodia, but the telecommunications law approved during the coverage period includes several provisions that undermine security and privacy.[66] Article 97 criminalizes eavesdropping by private individuals, but permits secret surveillance with approval from an undefined "legitima e authority." The law includes no legal or procedural safeguards, and as such, appears to authorize undeclared monitoring of "any private speech via telecommunications," according to one analysis.[67]

Article 6 requires that, "All telecommunications operators and persons involved with the telecommunications sector shall provide to the Ministry of Post and Telecommunications the telecommunications information and communication technology service data." There is no requirement for a judicial warrant or other safeguard, and the law places no limits on how long data can be stored.[68]

The TRC had previously ordered mobile phone operators and ISPs to cooperate with police in 2014,[69] and it is believed that this law will strengthen the legal grounds for overreaching government surveillance.

In 2012, a circular from the Ministry of Interior and the MPTC ordered internet cafes to install surveillance cameras, and phone shops and telecommunications operators to register subscribers' identification documents on the asis that these measures would "better promote protection of national security, safety and social order."[70] In addition, the circular required used data to be stored by the operators for six days so that designated officials can use the info mation for investigations of offenses related to "issues of national security, safety, and social order."

63 Mech Dara, 'Graduate Convicted for Bomb Threat; Sentence Cut, *The Cambodia Daily*, 26 October 2015, http://bit.ly/1Q4n8tS.

64 Aun Pheap, 'Man Arrested Over Threat to Kill Border Researcher,' *The Cambodia Daily*, September 7, 2015, http://bit.ly/1Rn0ywp

65 Lay Samean, "Man jailed 6 months for threats on Sok Touch," *Phnom Penh Post,* February 25, 2016, http://www.phnompenhpost.com/national/man-jailed-6-months-threats-sok-touch.

66 'Law on Telecommunications,' *Sithi Portal, February 17, 2017,* http://bit.ly/1XwQ2CC.

67 LICADHO, "Cambodia's Law on Telecommunications: A Legal Analysis," briefing, Ma ch 2016, https://www.licadho-cambodia.org/reports.php?perm=214.

68 LICADHO, "Cambodia's Law on Telecommunications: A Legal Analysis," briefing, Ma ch 2016, https://www.licadho-cambodia.org/reports.php?perm=214.

69 Matt Blomberg, Joshua Wilwohl and Phann Ana, 'Police Inspected Telecom Firms' Routers, Records', *The Cambodia Daily*, December 9, 2014, http://bit.ly/1G8OIgY.

70 John Weeks, "Cambodia's Default Internet Law – Draft Translation," *Jinja.Apsara*, July 5, 2012, http://bit.ly/1K8dFsu.

Intimidation and Violence

The internet is often used as a medium for threats and intimidation, such as the death threat issued against Sok Touch on Facebook for his work for the government mapping the Cambodia-Vietnam border (see Prosecutions and Detentions for Online Activity). However, there were no incidents of physical violence in retribution for online activity documented during the coverage period of this report.

Technical Attacks

In mid-January 2016, a group of hackers called Cyber TeamRox hacked into several websites, including those operated by the Cambodian Navy, Aeon Microfinance and the A tisans' Association of Cambodia. Defense Ministry spokesman Chhum Socheath confi med that the hackers were able to access data through the Navy's website, but said the content was not sensitive.[71] The team declared war on the government and the hacking was done in an "effort to secure justice the people [sic]."[72]

In 2014, two members of Anonymous, the online collective that has claimed responsibility for hacking many government websites, saw their sentences were reduced after they agreed to work for the Ministry of the Interior.[73]

There have been no publicized problems with government agents hacking or hijacking opposition or civil society websites in Cambodia.

71 Mech Dara and Daniel de Carteret, 'Slew of websites hacked,' *The Phnom Penh Post,* January 12, 2016, http://bit.ly/1R5xbMB.
72 May Titthara, 'Gov't to Hacker: Info Technology is Crucial to Peace,' *The Khmer Times,* January 12, 2016, http://bit.ly/20Xjdo0.
73 Titthara, 'Gov't to Hacker.'

Freedom House

Canada

	2015	2016
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	3	3
Limits on Content (0-35)	4	4
Violations of User Rights (0-40)	9	9
TOTAL* (0-100)	**16**	**16**

* 0=most free, 100=least free

Population:	**35.9 million**
Internet Penetration 2015 (ITU):	**88 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2016 Status:	**Free**

Key Developments: June 2015 – May 2016

- In July 2015, the Canadian Radio-television and Telecommunications Commission (CRTC) ruled that the largest telecommunications providers must provide wholesale access to their new fibe -optic internet infrastructure to smaller ISPs, a decision which could increase availability and ease of access to high-speed internet (see **Availability and Ease of Access**).
- The Supreme Court of Canada will hear Google's appeal in a major case with global implications, where Google was required to remove certain search engine results worldwide for a trademark-infringing company (see **Content Removal**).
- In June 2015, Bill C-51, the Anti-Terrorism Act with wide-ranging privacy implications, became law. Although the new Liberal government has promised to repeal some of the more problematic elements and introduce parliamentary oversight of intelligence agencies, reforms had not yet materialized during this period (see **Surveillance, Privacy, and Anonymity**).

Introduction

Canada's internet freedom environment continued to be generally free of government restrictions, although privacy-related concerns reemerged with new anti-terrorism legislation in June 2015.

Internet access in Canada is reliable and affordable for a majority of the population and is generally free of government restrictions. Canadians enjoy strong protections for freedom of expression, as well as a well-developed set of rules regulating intermediary liability in cases of copyright infringement.

Two major events loomed large over Canada in the past year. In October 2015, Canadians elected a new federal (national) government. The Liberal Party won a majority, after Canada had been ruled by the Conservative Party since 2006. The Liberals promised to look into some of the more onerous elements of certain laws affecting internet freedom passed under the Conservatives, such as Bill C-51, the Anti-Terrorism Act. However, the Liberal Party platform was short on details on substantive changes to internet and digital policy, and its effects, if any, will most likely not be felt in the short term. Their fi st budget did not assuage concerns of little movement on this front.[1]

The second event was the signing of the Trans-Pacific artnership (TPP) Agreement in February 2016. While ostensibly a trade agreement, the TPP includes several chapters that would likely have an impact on internet freedom in Canada - notably Telecommunications, Electronic Commerce, and Intellectual Property. However, the TPP has yet to be ratified domesticall , meaning any influence on Canadian internet freedom is merely speculation at this point. Furthermore, there is considerable divergence of opinion amongst respected expert commentators as to the actual potential effects of the TPP on the internet and digital spheres in Canada.[2]

Obstacles to Access

There are very few infrastructural or regulatory obstacles to internet access in Canada. Internet and mobile phone penetration rates continue to grow, although there are still geographic disparities related to internet access, reliability, and cost that especially affect more rural and remote areas.

Availability and Ease of Access

According to the International Telecommunication Union, the internet penetration rate in Canada reached 88 percent in 2015, compared to 87 percent in 2014 and 80 percent in 2009.[3] Canada had a mobile phone penetration rate of over 81 percent in 2015.[4] Mobile carriers have deployed a number of newer technologies to provide mobile broadband service, including HSPA+ and LTE.

1 See e.g. Michael Geist, "Budget 2016: Is It The End of a Canadian Digital Strategy?," March 23, 2016, http://bit.ly/1Sr8LxE.

2 Compare e.g. Barry Sookman, "TPP, copyright, e-commerce and digital policy: a reply to Michael Geist," December 15, 2015, http://bit.ly/1T6doiZ, and Michael Geist, "The Trouble With the TPP, Day 50: The Case Against Ratifying the Trans Pacific Partnership," March 14, 2016, http://bit.ly/1T6do2l.

3 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," accessed October 10, 2016, http://bit.ly/1cblxxY.

4 International Telecommunication Union, "Mobile-cellular telephone subscriptions, 2000-2015" accessed October 10, 2016, http://bit.ly/1cblxxY.

Broadband service of at least 5 megabits per second (Mbps) is available to 96 percent of Canadian households through a variety of technologies including fi ed and wireless, according to the *Communications Monitoring Report 2015,* published by the Canadian Radio-television and Telecommunications Commission (CRTC), an independent public regulator.[5]

Aiming to provide quality and accessible communications services, the CRTC has set a target to provide 100 percent of Canadian households with access to internet connectivity and broadband speeds of at least 5 Mbps by the end of 2016.[6] The government department of Innovation, Science and Economic Development Canada has set a target for broadband subscriptions at 80 percent of the population by the end of March 2017.[7] The CRTC indicates that 77 percent of households already subscribe to broadband services with internet speeds of 5 Mbps or more, so the government's target would appear easily attainable and well below what could theoretically be achieved.[8]

The potential for increased availability and ease of access to ultra high-speed internet was greatly increased this year thanks to a landmark policy decision put forward by the CRTC in July 2015.[9] In the policy, the CRTC required the largest internet and telecommunications providers in Canada to provide wholesale access to their emerging high-speed fibe -optic networks to smaller, independent providers of internet services. This should increase competition and reduce prices for consumers, at least in urban centers. The largest telecom player, Bell, appealed the policy,[10] but this appeal was denied.[11]

Perhaps the most important obstacle to availability and ease of access in Canada is geography. Canada is overwhelmingly urban, with 81 percent of the population living in urban areas.[12] Furthermore, approximately 75 percent of the population lives within 160 kilometres of the border with the United States.[13] While providing "reliable and affordable telecommunications services of high quality" to rural areas is enshrined in Canadian law,[14] from a practical perspective this has not translated to available and affordable high-speed internet services in rural areas, and especially in Canada's vast northern territories, which are underserved by infrastructure generally, and telecommunications services in particular.

According to CRTC's 2015 report, household broadband availability, in the form of 5-9.99 Mbps services, was 100 percent in urban areas yet only 86 percent in rural areas. The 86 percent figu e includes 11 percent where availability was only via wireless services (HSPA+ and LTE), which are gen-

5 Canadian Radio-television and Telecommunications Commission, *"Communications Monitoring Report 2015," October 2015,* accessed March 22, 2016, http://bit.ly/1WIBcsd.

6 Canadian Radio-television and Telecommunications Commission, "*Report on Plans and Priorities for 2016-2017,*" accessed March 22, 2016, http://bit.ly/1Mo0awn.

7 Innovation, Science and Economic Development Canada, "*2016-17 Estimates-Report on Plans and Priorities,*" accessed March 22, 2016, http://bit.ly/1VK9Xip.

8 Canadian Radio-television and Telecommunications Commission, "*Communications Monitoring Report 2015," October 2015,* accessed March 22, 2016, http://bit.ly/1WIBcsd.

9 *CRTC Telecom Regulatory Policy 2015-326*, July 22, 2015, http://www.crtc.gc.ca/eng/archive/2015/2015-326.htm.

10 See e.g. William Sandiford, "Bell playing politics with your Internet bill by appealing CRTC ruling," *The Globe and Mail*, October 30, 2015, http://bit.ly/1RbiIQA.

11 Aleksandra Sagan, "Bell's appeal against sharing Internet infrastructure denied by federal cabinet," *Toronto Sun*, May 11, 2016, http://bit.ly/1Wuwpht.

12 From the 2011 census. See Statistics Canada data at http://bit.ly/1pHhdjd, accessed March 22, 2016.

13 National Geographic "Canada Facts", accessed March 22, 2016, http://on.natgeo.com/1pHhpPv.

14 See the *Telecommunications Act*, S.C. 1993, c.38, section 7(b), http://bit.ly/1ZpuSrg.

erally more expensive, especially as data usage rates increase. Faster speeds, such as 25-29.9 Mbps, are only available in 29 percent of rural households, compared to 99 percent of urban households.[15]

The new Liberal government has recognized this issue, and has pledged CDN$500 million over fi e years for a new program to "extend and enhance broadband service in rural and remote communities."[16] As yet, however, the government has provided no details, nor targets or definitions f broadband service. Perhaps more promising is the CRTC, which launched the so-called #TalkBroadband – a comprehensive review of basic telecommunications services with a focus on internet services.[17] Part of the focus of the review was to examine the urban-rural divide, especially as it relates to costs, which may lead to significant policy changes down the oad. The review culminated in public hearings in April 2016. The results of the second phase of the review, a major study of Canadians' opinions about their broadband service, indicated that rural internet users experienced a range of issues with access, reliability, and cost.[18]

While internet access is widely available in Canada (to varying degrees as already described), there is a gap in access related to income: the highest income bracket has a penetration rate of nearly 95 percent, while the penetration rate within the lowest income bracket is closer to 63 percent.[19] Internet connectivity is widely available in public spaces such as cafés, shopping malls and libraries, generally free of charge. There is a wide range of content available in both of Canada's official languages (English and French) as well as many other languages.

Restrictions on Connectivity

There are no government restrictions on bandwidth, although the major access providers generally offer services that have caps on bandwidth that result in increased fees for users who exceed the limit. The government has not centralized the telecommunications infrastructure in Canada. However, given the vertical integration of the Canadian marketplace, the telecom infrastructure is controlled by a small number of companies, which in theory could facilitate greater control of content and the implementation of surveillance technologies.

ICT Market

To operate as a Canadian telecommunications carrier, a company must meet the requirements in section 16 of the Telecommunications Act. In 2014, Canadian telecommunications revenues amounted to $45.9 billion, up from $44.8 billion the previous year, a 2.1 percent growth. The fi e largest companies (Bell Canada, MTS Inc./Allstream Inc., Rogers, Shaw, and TELUS) captured more than 84 percent of total revenues. This number has remained steady over the last several years.[20]

15 Canadian Radio-television and Telecommunications Commission, *"Communications Monitoring Report 2015," October 2015,* accessed March 22, 2016, http://bit.ly/1WIBcsd.

16 See "Growing the Middle Class", federal government budget document, March 22, 2016, at page 106, http://bit.ly/1UXygJ5 (PDF).

17 See *Telecom Notice of Consultation CRTC 2015-134*, April 9, 2015 at http://bit.ly/1RDqW6h.

18 EKOS Research Associates Inc., "Let's Talk Broadband Findings Report," March 18, 2016, http://bit.ly/1M0lkB0.

19 Statistics Canada, "Canadian Internet use by age group and household income for Canada, provinces, and metropolitan areas," CANSIM, Table 358-0152, accessed September 17, 2014, http://bit.ly/1GQi7M1.

20 Canadian Radio-television and Telecommunications Commission, "Communications Monitoring Report 2015," October 2015, accessed March 22, 2016, http://bit.ly/1WIBcsd.

Canadians have a choice of wireless internet providers, all of which are privately owned. There are at least three providers to choose from in all markets, although which providers may vary region to region. Restrictions on foreign investment establish some controls, though Canada has seen some foreign companies enter the marketplace in recent years. The provision of access services is subject to regulation with rules on tower sharing, domestic roaming agreements, and a consumer regulator to address consumer concerns.

For wireless services, three companies dominate the market: Bell, Telus, and Rogers. Those same companies are also leaders in the provision of wired internet services (whether via phone lines or cable), along with Shaw, Cogeco, and Vidéotron. While Canadians generally do enjoy a choice of wired internet providers, again this choice will vary from region to region, and often there is only one choice per technology type, leading to a public perception that there is not much choice and that prices are kept artificially high. The *Let's Talk Broadband Findings Report* from March 2016 indicated that only one in three Canadians is satisfied with the cost f their home internet service.[21]

Regulatory Bodies

The Canadian Radio-television and Telecommunications Commission (CRTC), the regulatory body that oversees the communications industry, operates largely independently from the government. The government appoints the CRTC chair and commissioners without public consultation. The government also has, in some cases, provided guidance on their policy expectations regarding telecommunication regulations. Moreover, CRTC decisions can be appealed to the courts, or a government review can be requested. The government has overturned CRTC decisions and directed it to reconsider the issue in the past, but this has been rare.

CRTC's regulatory powers extend to *access* of the internet in Canada, but not to *content* of the internet in Canada; this is commonly called the New Media Exemption. The CRTC's position to not regulate internet content dates back to 1999 and has been reinforced numerous times since then,[22] including by the Supreme Court of Canada.[23] This is in contrast to other industries, specifically ele- vision, where the CRTC does exert some control over content, most notably by requiring a minimum amount of Canadian content by Canadian broadcasters.

Limits on Content

The Canadian government does not generally block websites or filter online content. Illegal content may be removed by legal action taken through the court system.[24] YouTube, Facebook, Twitter, and international blog-hosting services are freely available.

Blocking and Filtering

The government does not generally block or fil er online content, though there are a few legal

21 EKOS Research Associates, "Let's Talk Broadband Findings Report," March 18, 2016, accessed October 10, 2016, http://bit.ly/2d7AIuv.

22 See most recently *Broadcasting Regulatory Policy CRTC 2015-355 and Broadcasting Order CRTC 2015-356*, August 6, 2015, http://bit.ly/22HBQx9.

23 Reference re Broadcasting Act, 2012 SCC 4, http://bit.ly/22HDXRm.

24 OpenNet Initiative, "United States and Canada Overview," accessed September 19, 2014, http://bit.ly/1RTmw7q.

mechanisms that may lead to the blocking or removal of online content in Canada. Canada's largest ISPs participate in Project Cleanfeed Canada, an initiative that allows ISPs to block access to child pornography images that are hosted outside of Canada (as opposed to content hosted within Canada, which is subject to removal).[25] Accessing child pornography is illegal in Canada under section 163.1(4.1) of the criminal code,[26] as well as under international human rights standards. The initiative is targeted at international sites that the Canadian government does not have the jurisdiction to shut down.

In April 2015, the government of Quebec announced plans in its budget to require ISPs to block access to online gambling sites. The list of blocked sites will be developed by Loto-Québec, a government agency. This is expected to act as a revenue-enhancing measure for the government by directing gamblers to the state government's own Loto-Québec-run online gaming site, Espacejeux. On May 18, 2016, the law went into effect.[27] The law is likely to face a legal challenge, both on free speech and jurisdictional grounds, since the federal government has exclusive jurisdiction over telecommunications regulation. It may also violate net neutrality principles, and ISPs are concerned over the potential costs and a complicated implementation.[28]

Canada's tough anti-spam law, which regulates commercial electronic messages ("CEMs"), has been in effect since July 1, 2014. The law prescribes certain content requirements in electronic messages (such as unsubscribe mechanisms and contact information) and restricts sending such messages without appropriate consent. There have been several enforcement actions involving the law in the past year, including against some of Canada's largest corporations. In June 2015, Porter Airlines agreed to pay of fine f $150,000 for an absent or improper unsubscribe link or button, and in November 2015 Rogers Media agreed to pay a fine f $200,000 for a malfunctioning unsubscribe mechanism. Rogers Media is a division of Rogers Communications, one of Canada's principal suppliers of telecommunications services, including internet services. In a speech to a major marketing industry group in March 2016, CRTC Chairman Jean-Pierre Blais warned that the rules in the anti-spam law "aren't going anywhere."[29]

Content Removal

With respect to removal of content due to copyright infringement, in 2004 the Supreme Court of Canada ruled that ISPs are not liable for violations committed by their subscribers.[30] Canadian copyright law features a notice-and-notice provision in effect since January 2015, which, unlike a notice-and-takedown system, does not make intermediaries legally liable for removing content upon notification by the copyright owne . Rather, copyright owners are permitted to send notific - tions alleging infringement to ISPs. The providers are then required to forward the notifications o the implicated subscriber. Any further legal action is the responsibility of the copyright owner, and it is incumbent upon the person who uploaded the infringing content to remove it following a legal

25 Cybertip!ca, "Cleanfeed Canada," accessed September 19, 2014, http://bit.ly/1jy5ws4.

26 *Criminal Code,* RSC 1985 c C-46 s 163.1(4.1).

27 Michael Geist, "Government-Mandated Website Blocking Comes to Canada as Quebec's Bill 74 Takes Effect", May 26, 2016, http://bit.ly/22r74ET.

28 Sean Craig and Damon van der Linde, "Internet service providers, First Nations gird for fight o er Quebec's gambling law", June 1, 2016, http://bit.ly/29EXzAm.

29 "Jean Pierre Blais to the Canadian Marketing Association", March 22, 2016, text available at http://bit.ly/1SgLHix.

30 Society of Composers, Authors and Music Publishers of Canada v Canadian Assn of Internet Providers, [2004] SCC, 2 SCR 427.

decision. No content is removed from the internet without a court order, and the internet provider does not disclose subscriber information without court approval. ISPs qualify for a legal safe harbor if they comply with the notice-and-notice requirements.

Despite the good intentions, the notice-and-notice system has been subject to some misuse. Several U.S.-based anti-piracy fi ms, including Rightscorp and CEG-TEK, have used the system to send notifications o subscribers that misstate Canadian law, citing U.S. damage awards and the possibility that their internet access will be terminated, in order to sow fear among Canadians so that they pay a settlement fee.[31] The author of this report, an attorney specializing in internet and technology law, has personally been contacted by dozens of panicked Canadians who have received such notices, the overwhelming majority from CEG-TEK.

Media companies have used the courts to shut down websites that redistribute their content in violation of copyright laws. In February 2016, two major media companies, Bell and TVA, used a court order in Quebec to seize equipment and shut down a website that was streaming their sports programming over the internet without permission.[32]

In February 2016, the Supreme Court of Canada ("SCC") granted leave to appeal from the judgment of the British Columbia Court of Appeal ("BCCA") in *Equustek Solutions Inc. v. Jack*, a closely-watched case involving a court order requiring Google to remove websites that infringed on the plaintiffs' trademark from its global index. Rather than ordering the company to remove certain links from the search results available through Google.ca, the BCCA upheld the lower court's decision that intentionally targeted the entire database, requiring the company to ensure that no one, anywhere in the world, could see the search results. The SCC hearing is tentatively scheduled for November of 2016,[33] and commentators, experts and free speech advocates in Canada and around the world will be watching with interest.[34]

Defamation claims may also result in the removal of content, as content hosts fear potential liability as a publisher of the defamatory content. Unlike legal protections against liability for copyright infringement by its users, platforms may face liability for alleged defamation once alerted to the publication. A court may also order the removal of the content. The Supreme Court of Canada has held that merely linking to defamatory content on the internet is not defamation in and of itself; it would only be defamation if it actually repeats the defamatory content, so simple links would not be removed.[35]

In Quebec, Canada's French-speaking province, websites that are commercial in nature are required by law to be in French,[36] although they can be in other languages as well. Violators may receive a warning from a government agency ordering the website be in French, and then be subject to fines if they do not comply. Some website operators may choose to take down their websites rather than face the expense of translation or the fines. National or in ernational operators of websites who do

31 Jeremy Malcolm, "Canada Must Fix Rightsholder Abuse of its Copyright Notice System," *Deeplinks Blog,* Electronic Frontier Foundation, April 23, 2015, http://bit.ly/29hzJGZ.

32 Lise Millette, "Saisies de matériel lié au piratage des chaînes spécialisées de Bell et TVA", February 5, 2016, http://bit.ly/21RqTmS.

33 See SCC case information at http://bit.ly/1UWRrUA.

34 Sebastien Beck-Watt, "Is Google "Feeling Lucky" at the Supreme Court?", *IP Osgoode*, November 14, 2015, http://bit.ly/1RECVxp.

35 Crookes v. Newton, 2011 SCC 47, http://bit.ly/1SrcV8P.

36 See the *Charter of the French Language*, c. C-11, article 52, http://bit.ly/1Srh2Sm.

business in Quebec (who would then be subject to the law) may block Quebec residents' access to their websites rather than comply.[37]

Media, Diversity, and Content Manipulation

The online environment in Canada is relatively diverse, and internet users have access to a wide range of news, content, and opinions. There does not appear to be widespread self-censorship in Canadian online publications, and there is no evidence of government manipulation of online content. Some sites are affilia ed with a particular partisan interest, but there are representative sites from all sides of the political spectrum available online. All major media organizations feature extensive websites with articles, audio, and video. The public broadcaster maintains a very comprehensive website that includes news articles and streamed video programming. Paywalls have become increasingly popular among newspaper organizations, but there remains considerable choice (including alternate, independent media) that is freely available.

To date, economic constraints such as net neutrality concerns have not been a significant fac or in the success or failure of online media outlets and platforms in Canada, though the debate over net neutrality continues. The future of net neutrality in Canada remains unclear, as the new Liberal government's policies are silent on the subject. However, the CRTC Chairman has often expressed support for net neutrality.

Digital Activism

Social media and communication applications have been widely used in Canada for the mobilization of political and social movements. Online digital activism played a significant ole in the Liberal government's promise to repeal the problematic aspects of Bill C-51 (see "Surveillance, Privacy, and Anonymity"), and online activism was prominent during the federal election generally. Much online activism targeted at the ICT sector is spearheaded by a popular non-partisan, non-profit o ganization called Open Media, which advocates for three pillars of internet rights – free expression, access, and privacy.[38]

Violations of User Rights

Despite having a generally positive record for freedom of expression, Canada has taken some regressive steps in recent years, driven by court decisions that weakened confidentiality for journalists' sources, and the introduction of several bills that could have negative implications for the protection of internet users' data. However, user rights as they relate to the government and its data have improved in the past year, with the new Liberal government's commitment to open data and access to government information a central tenet of their election platform,[39] contrasting with the previous Conservative government's more restrictive approach regarding access to information.

Legal Environment

37 Elysia Bryan-Baynes, "Quebec language police target English retail websites," November 13, 2014, http://bit.ly/1SrI50Y.
38 See https://openmedia.org/.
39 Liberal Party Platform, accessed March 27, 2016, https://www.liberal.ca/realchange/.

The Canadian Constitution includes strong protections for freedom of speech and freedom of the press. Freedom of speech in Canada is protected as a "fundamental freedom" by section 2 of the Canadian Charter of Rights and Freedoms. Under the Charter, one's freedom of expression is "subject only to such reasonable limits prescribed by law as can be demonstrably justified in a f ee and democratic society."[40] These laws and protections apply to all forms of speech, whether online or offline

Hate speech, along with advocating genocide, uttering threats and defamatory libel, are also regulated under the Canadian criminal code.[41] Punishment for defamatory libel, advocating genocide and uttering threats may include imprisonment for up to fi e years, and up to two years for hate speech. Human rights complaints regarding potentially defamatory statements could also be decided through the mechanisms provided by provincial human rights laws and the Canadian Human Rights Act ("CHRA");[42] however the controversial provision of the CHRA prohibiting hate speech (s. 13), which was perceived by many as being too broad and thus potentially limiting legitimate free speech, is currently not in force.

There are no specific online estrictions on sensitive topics. Anti-spam legislation, enacted in July 2014, requires opt-in consent to send commercial electronic messages. Critics of the legislation have argued that it is overly broad and seeks to overregulate commercial speech.

Prosecutions and Detentions for Online Activities

Individuals were not arrested or prosecuted for online activities during the coverage period.

Citizens can be subject to legal sanction for possessing, accessing or even distributing child pornography if they post images of it on the internet.[43] Generally, writers, commentators, and bloggers are not subject to legal sanction for content that they post on the internet. Internet users are free to discuss any political or social issues without concern for prosecution, with the exception of the hate speech provisions discussed above.

Surveillance, Privacy, and Anonymity

After a busy period for legislation and court cases involving surveillance and privacy in 2014 and mid-2015, the environment remained largely unchanged in 2016. While some argue that the signing of the Trans-Pacific artnership (TPP) Agreement has major implications for privacy,[44] the concerns remain speculation with the TPP not yet in effect.

Bill C-51, the Anti-Terrorism Act that passed in June 2015, has major privacy implications. The bill permits information-sharing across government agencies for an incredibly wide range of purposes, many of which have nothing to do with terrorism. The bill was opposed by all Canadian privacy commissioners but ultimately passed and became law. However, the newly-elected Liberal government

40 Constitution Act, Canadian Charter of Rights and Freedoms, 1982, http://bit.ly/1cijVUc.

41 R.S.C 1985 c C-46, http://bit.ly/22YUNYE.

42 R.S.C., 1985, c. H-6, http://bit.ly/1qjY3zS.

43 Kevin Bissett, "Douglas Hugh Stewart, New Brunswick Man, Gets 5 Years In Prison For Millions Of Child Porn Images," *Huffington Post*, November 14, 2011, accessed September 19, 2014, http://huff.to/1ZSBgZq.

44 See e.g. Michael Geist, "The Trouble with the TPP, Day 11: Weak Privacy Standards," January 18, 2016, http://bit.ly/1M01EgC.

has vowed to "repeal the problematic elements of Bill C-51,"[45] even though the Liberals supported the bill when it was originally passed. While the Liberals have not provided an exhaustive list of the "problematic elements" they would repeal, they would at the very least seek to ensure any Canadian Security Intelligence Service (CSIS) warrants respect the Canadian Charter of Rights and Freedoms, and to narrow certain overly broad definitions in the bill. The Liberals also p omised a Parliamentary Committee to oversee national security activities covered under the bill and introduced Bill C-22 in June 2016 to achieve that goal.[46]

In June 2015 the government passed Bill S-4, the Digital Privacy Act, which modified the ersonal Information Protection and Electronic Documents Act (PIPEDA), Canada's private sector privacy law.[47] The bill expanded the scope for companies to make voluntary warrantless disclosures of personal information under certain circumstances, by allowing for such disclosures to any organization, not just law enforcement. The bill also established new mandatory security breach disclosure requirements (although these provisions are not yet in force) and enhanced the meaning of consent within PIPEDA.

In a potentially disturbing development for Canadians' privacy, it was revealed in January 2016 that metadata had been shared with Canada's "Five Eyes" international partners (the U.S., U.K, Australia and New Zealand) without necessarily having been anonymized. In response, the Communications Security Establishment, Canada's electronic spy agency, stopped sharing certain metadata with those countries, until appropriate protections are in place.[48]

The ability of Canadians to seek legal redress against foreign internet companies for privacy violations diminished significantly in the ast year. In June 2015, the British Columbia Court of Appeals held that residents of British Columbia could not bring a class action suit against Facebook for violation of certain privacy rights, because a forum selection clause in Facebook's Terms of Use was enforceable and not trumped by the province's Privacy Act.[49] The Supreme Court of Canada granted leave to appeal,[50] with a hearing scheduled for November 2016.

From the previous year, the most notable privacy case was the Supreme Court of Canada's *R. v. Spencer* decision, released in June 2014.[51] In a unanimous decision written by Justice Thomas Cromwell, the court issued a strong endorsement of internet privacy, emphasizing the importance of privacy regarding subscriber information, the right to anonymity, and the need for police to obtain a warrant for subscriber information except in exigent circumstances or under a reasonable law. In January 2016, Canada's Privacy Commissioner called on the government to confi m these "Spencer principles," in light of complaints from law enforcement officials that the decision has made their job impossible.[52]

45 Liberal Party platform on Bill C-51, accessed March 26, 2016, http://www.liberal.ca/realchange/bill-c-51/; See also: Jim Bronskill, "Justin Trudeau's promised overhaul of C-51 tops incoming security to-do list," *CBC.ca*, November 3, 2015, http://bit.ly/1M09lTL.

46 See "Government of Canada Introduces Legislation to Establish National Security and Intelligence Committee of Parliamentarians", June 26, 2016, at http://bit.ly/2d5vLHi.

47 Personal Information Protection and Electronic Documents Act (PIPEDA), last amended on June 23, 2015, http://bit.ly/1hVRkBe.

48 "Canada's electronic spy agency stops sharing some metadata with partners," *CBC News*, January 28, 2016, http://bit.ly/2d7REWv.

49 Douez v. Facebook, Inc., 2015 BCCA 279 (CanLII), http://canlii.ca/t/gjldz.

50 See SCC case information at http://bit.ly/1TkTReF.

51 R. v. Spencer, [2014] SCC 43, http://bit.ly/1szAZgb.

52 Daniel Therrien, "Op-ed: Federal Privacy Commissioner urges caution should Parliament revisit warrantless access," January 25, 2016, http://bit.ly/2drmDZJ.

The Office of the Privacy Commissioner provides an important oversight function related to privacy of Canadians' information in the digital medium. The Privacy Commissioner of Canada, Daniel Therrien, is an officer of parliament who reports directly to the House of Commons and the Senate. The commissioner's mandate includes overseeing compliance with the Privacy Act, which covers the personal information-handling practices of federal government departments and agencies, and PIPEDA, Canada's private sector privacy law.[53]

Intimidation and Violence

There were no documented cases of violence or physical harassment of internet users in Canada for their online activities during the report period. In a highly-watched case, a Toronto man was found not guilty of criminal harassment regarding a high volume of possibly threatening Tweets targeted at two women.[54] The judge found the women's fear was not reasonable given the circumstances. However, in another case, a man was found guilty of harassing and threatening a female Member of Parliament on Twitter.[55]

In a highly-praised landmark civil case in January 2016, a man who published revenge porn against his ex-girlfriend was ordered to pay $100,000 to the victim who suffered severe emotional distress.[56] The Ontario judge clearly tried to dissuade future publishers of revenge porn, and used an expansion of the invasion of privacy tort in Canada to do so. The judge even indicated he would have ordered a larger award if possible ($100,000 was the maximum under the specific procedure used).

Technical Attacks

While there have been numerous cyberattacks and data breaches in Canada in recent years, very serious, widespread, systematic technical attacks have not been such a serious issue in Canada. A prominent cyberattack in June 2015 crashed several government websites and e-mail services. The international group Anonymous claimed responsibility, citing it as a protest against the passage of the Bill C-51 Anti-terrorism Act.[57] More recently, in March 2016, an Ottawa hospital was the victim of ransomware (a type of malware used to extort money from victims), but it is uncertain if they were specifically targeted.[58] The new Liberal government has launched a comprehensive review of cybersecurity threats[59] and increased spending for cybersecurity in their March 2016 budget to prepare for the increasing risk of technical attacks. Many experts believe Canadian citizens and business are woefully unprepared against cybercrime and hacking.[60]

53 Office of the Privacy Commissioner of Canada, "Mandate and Mission," http://bit.ly/1LlfhTx.

54 R. v. Elliott, 2016 ONCJ 35 (CanLII), http://canlii.ca/t/gn1hq.

55 Ashley Csanady, "The Twitter trial you never heard about: Toronto man found guilty of harassing Michelle Rempel," *National Post*, January 29, 2016, http://bit.ly/1M371LP.

56 Doe 464533 v N.D., 2016 ONSC 541 (CanLII), http://canlii.ca/t/gn23z.

57 Steven Chase, "Cyberattack deals crippling blow to Canadian government websites," *The Globe and Mail*, June 17, 2015, http://bit.ly/1JUAcOF.

58 Vito Pilieci, "Ottawa Hospital hit with ransomware, information on four computers locked down", *National Post*, March 13, 2016, http://bit.ly/1SuaMsO.

59 David Akin, "Trudeau government to take on cybersecurity threats", *Toronto Sun*, February 18, 2016, http://bit.ly/1SuchaE.

60 Dave Seglins, "Canada 'failing' in fight against cybe crime, hacking," *CBC.ca*, November 24, 2015, http://bit.ly/1SufVRH.

Freedom House

China

	2015	2016
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	18	18
Limits on Content (0-35)	30	30
Violations of User Rights (0-40)	40	40
TOTAL* (0-100)	**88**	**88**

* 0=most free, 100=least free

Population:	**1.371 billion**
Internet Penetration 2015 (ITU):	**50 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- A draft cybersecurity law could step up requirements for internet companies to store data in China, censor information, and shut down services for security reasons, under the auspices of the Cyberspace Administration of China (see **Legal Environment**).
- An antiterrorism law passed in December 2015 requires technology companies to cooperate with authorities to decrypt data, and introduced content restrictions that could suppress legitimate speech (see **Content Removal** and **Surveillance, Privacy, and Anonymity**).
- A criminal law amendment effective since November 2015 introduced penalties of up to seven years in prison for posting misinformation on social media (see **Legal Environment**).
- Real-name registration requirements were tightened for internet users, with unregistered mobile phone accounts closed in September 2015, and app providers instructed to register and store user data in 2016 (see **Surveillance, Privacy, and Anonymity**).
- Websites operated by the *South China Morning Post, The Economist* and *Time* magazine were among those newly blocked for reporting perceived as critical of President Xi Jinping (see **Blocking and Filtering**).

Introduction

China was the world's worst abuser of internet freedom in the 2016 *Freedom on the Net* survey for the second consecutive year. Harsh punishments for expression and a deteriorating legal environment are significantly unde mining civil society activism on the internet.

"Cyberspace sovereignty" has been a top policy strategy for the Chinese Communist Party (CCP) under its general secretary, President Xi Jinping. Over the past year, the renewed emphasis on information control took the form of laws that sought to codify existing strategies of censorship and surveillance. The National People's Congress drafted a cybersecurity law which could strengthen requirements for internet companies to censor content, shut down their services, register their users' real names, and provide security agencies with user data stored in mainland China. An antiterrorism law passed in December 2015 also introduced scope for abuse, requiring companies to provide technical support to authorities seeking to access encrypted data, and some content controls. An amendment to the criminal law separately penalized spreading alleged misinformation on social media.

Free expression and privacy were undermined through heightened pressure on companies providing internet services and content to comply with censorship orders and user data requests. Regulators introduced new rules for online news outlets, audiovisual content, and digital publishing. Service providers continued to implement real-name registration of all customers, closing down avenues for anonymous communication, and in August 2016, the registration policy was extended to apps which rely on internet connectivity to provide other services. The state even fl ated a proposal to purchase a one percent share in major Chinese internet companies like Baidu and Tencent in April 2016, another potential avenue of control. Companies who refuse to cooperate are shut out. The website of *South China Morning Post,* Hong Kong's largest English-language newspaper, *The Economist* and *Time* magazine were among those newly blocked in 2015 and 2016.

As in past years, dozens of domestic internet users were investigated for digital crimes from disseminating misinformation to promoting tools to circumvent censorship, and one Uyghur teenager was reported to have been imprisoned for life for watching banned videos on a cellphone.

Against the backdrop of stricter internet control across all platforms, digital activism has been gradually waning. While some individuals are still outspoken, observers noted a decline in the lively discussion of social causes which used to characterize popular microblogs. And in one high profile case, collective action was channeled to further policies that could be used to control information. Internet users successfully forced regulators to impose restrictions on advertising by search engines, after the death of a student who railed against Baidu for promoting an expensive and unproven medical treatment in a sponsored search result. Yet when those regulations on online advertising materialized in late 2016, they also imposed restrictions on the way search engines manage prohibited content.[1]

Obstacles to Access

China boasts the world's largest number of internet users, yet obstacles to access remain, including poor infrastructure, particularly in rural areas; a telecommunications industry dominated by state-

1 State Administration for Industry and Commerce, SAIC, 国家工商行政管理总局令, July 4, 2016, http://www.saic.gov.cn/zwgk/zyfb/zjl/xxzx/201607/t20160708_169638.html

owned enterprises; centralized control over international gateways; and sporadic, localized shutdowns of internet service to quell social unrest. Nationwide blocking, filtering, and monitoring systems delay or interrupt access to international websites.

Availability and Ease of Access

The authorities reported in January 2016 that there were 688 million internet users in China,[2] and the International Telecommunication Union estimated internet penetration at 50 percent in 2015.[3] Since 2011, internet adoption rates have slowed as the urban market approaches saturation, according to the China Internet Network Information Center (CNNIC), an administrative agency under the Ministry of Industry and Information Technology (MIIT).[4] Though the digital divide between urban and rural areas narrowed marginally in 2014, 71.6 percent of users are based in cities, according to the most recent government figu es.[5] Penetration rates significantly ary by province, from Beijing (76.5 percent) to Yunnan in the southwest (37.4 percent).[6] The CNNIC continued to report a small gender gap among internet users, with males making up 53 percent of the total.

Mobile replaced fi ed-line broadband as China's preferred means of accessing the internet for the fi st time in 2012. From December 2014 to December 2015, the mobile internet population grew from 557 million to 620 million, accounting for 90 percent of all internet users.[7]

Though demand is relatively high in rural areas and small towns, the number of internet users throughout China who were connecting through cybercafes and public computers remained relatively constant in 2015, at 17.5 percent.[8]

Costly and inefficient fixed-line broadband service has contributed to the shift toward mobile. The MIIT ordered that homes constructed within reach of public fibe -optic networks be connected via a selection of service providers from April 2013 onward.[9] A "Broadband China" government strategy issued in 2013 aimed to boost penetration to 70 percent nationwide by 2020, raise third-generation (3G) mobile internet penetration to 85 percent, and increase connection speeds to 50 Mbps in cities and 12 Mbps in rural areas, with even faster Gbps speeds promised in bigger cities.[10]

The reality is more complicated. At the end of 2015, the CNNIC reported that the average domestic fi ed-line broadband download speed across the country increased from 4.25 Mbps to 8.34 Mbps in 2014. The highest available rate was in Shanghai, which averaged 11.3 Mbps, while the lowest was in

2 China Internet Network Information Center (CNNIC),中国互联网络发展状况统计报告 [The 37th Report on the Development of the Internet in China], January 2016, http://www.cnnic.cn/hlwfzyj/hlwxzbg/201601/P020160122469130059846.pdf.

3 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1cblxxY; CNNIC reported 50.3 percent 中国互联网络发展状况统计报告.

4 CNNIC, 中国互联网络发展状况统计报告 [The 28th Report on the Development of the Internet in China], July 2011, http://bit.ly/1GadOjH.

5 CNNIC, 中国互联网络发展状况统计报告.

6 CNNIC, 中国互联网络发展状况统计报告.

7 CNNIC, 中国互联网络发展状况统计报告

8 CNNIC, 中国互联网络发展状况统计报告, [The 37th Report on the Development of the Internet in China].

9 Shen Jingting, "New residences required to provide fiber net ork connections," *China Daily*, January 9, 2013, http://bit.ly/1GaeW6R.

10 Ministry of Industry and Information Technology, 国务院关于印发"宽带中国"战略及实施方案的通知, 2013, http://bit.ly/1RFIavO.

Tibet, which averaged 6.21 Mbps.[11] By contrast, Akamai, which measures access to the global internet, registered slower average speeds of 3.7 Mbps, down from 3.8 Mbps in 2014.[12]

In Shanghai, customers of Shanghai Telecom experienced lack of bandwidth and slow connections to overseas websites in 2015. In response, the company offered customers an "International nitrogen cylinder plan" which tripled the cost of access to overseas websites, possibly to offset the cost of more affordable access to domestic content.[13]

Restrictions on Connectivity

Nine state-run operators maintain China's gateways to the global internet, giving authorities the ability to cut off cross-border information requests.[14] All service providers must subscribe via the gateway operators under MIIT oversight. In March 2016, MIIT announced a draft regulation on domain name management (*hulianwang yuming guanli banfa*). The regulation requires that all domain name holders must go through a real-name registration process, and domain names managed by overseas institutions will not be connected.[15] Foreign media worried that the measure could potentially block all foreign websites,[16] but MIIT clarified that the egulation only applies to websites with Chinese domain names.[17]

The government has shut down access to entire communications systems in response to specific events, notably imposing a 10-month internet blackout in the Xinjiang Uyghur Autonomous Region—home to 22 million people—after ethnic violence in the regional capital, Urumqi, in 2009.[18] Since then, authorities have enforced smaller-scale shutdowns, including in March 2016, when network disruptions were reported in western Sichuan province after a Tibetan woman set herself on fi e and burned to death in an act of protest against Chinese rule of Tibet.[19]

Some disconnections are more targeted. In November 2015, residents of Xinjiang reported that mobile service was temporarily shut down for those using circumvention tools, those who had not registered their connections using their real names, and those who downloaded foreign messaging software.[20]

Uyghurs, Tibetans, and others who express their opinions about Chinese rule of disputed territory are frequently targeted on the pretext that they threaten national security. For that reason, the introduction in 2015 of legal provisions that could enable network disruptions to prevent terrorism and

11 Broadband and Development Alliance, *China's broadband speed status report* [in Mandarin], http://chinabda.cn/kdfzbg/252261.shtml

12 Akamai, *State of the Internet: Q3 2015 Report*, infographics, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-state-of-the-internet-report-q3-2015.pdf; Akamai, State of the Internet: Q4 2014 Report, infographics http://akamai.me/1LGi8U4

13 Oiwan Lam, Shanghai Telecom Triples Cost of Access to Overseas Websites, August 11 2015, Global Voices, https://globalvoices.org/2015/08/11/shanghai-telecom-triples-cost-of-access-to-overseas-websites/

14 CNNIC, 中国互联网络发展状况统计报告 [The 31st Report on the Development of the Internet in China], 21.

15 域名管理新规征求意見 調整域名管理體系, http://chinese.gmw.cn/tech/2016-03/28/content_19481218.htm

16 域名须在华注册！中国拟再度收紧网管, http://bit.ly/2fh69aE.

17 工信部回应域名管理新政:不影响外企正常业务http://tech.163.com/16/0330/20/BJEBUA2T000915BF.html.

18 See Alexa Olsen, "Welcome to the Uighur Web," *Foreign Policy*, April 21, 2014, http://atfp.co/1jmJCYH.

19 Nithin Coca, "The slow creep and chilling effect of China's censorship," The Daily Dot, August 29, 2016, http://www.dailydot.com/layer8/china-tibet-xinjiang-censorship/.

20 Paul Mozur, "China cuts mobile service of Xinjiang residents evading internet filters," New York Times, November 23, 2015, http://www.nytimes.com/2015/11/24/business/international/china-cuts-mobile-service-of-xinjiang-residents-evading-internet-fil ers.html?_r=0.

protect cybersecurity was cause for concern. Article 84 of the antiterrorism law passed in December introduced fines and de entions of up to 15 days for telecommunications operators and ISP personnel who fail to "stop transmission" of terrorist or extremist content, "shut down related services," or implement "network security" measures to prevent the transmission of such content.[21] A draft cybersecurity law issued for public comment in July 2015 would also provide legal grounds for officials o instruct network operators to stop transmission to protect public security (see Content Removal and Legal Environment).

ICT Market

In 2011, an antimonopoly investigation accused state-owned China Telecom and China Unicom of abusing their market dominance to manipulate fi ed-line broadband pricing, marking the fi st use of a 2008 antimonopoly law against state enterprises.[22] The telecom giants revised their inter-network pricing structures to allow rivals to access their infrastructure,[23] and customers can now choose from among many small local, private internet service providers (ISPs).[24]

State-owned China Mobile, China Telecom, and China Unicom dominate the mobile market. In 2014, the government formally authorized the three major players to set pricing for services according to market forces, resulting in price cuts.[25] Private capital was allowed to enter the network leasing business during the coverage period. By November 2015, the MIIT had issued 42 network leasing licenses to private companies.[26] In some cities, municipal governments proposed regulations to ensure telecommunication market diversity so that residents within a single community could have a choice of telecommunications providers.[27]

Despite the gradual lifting of longstanding market control, network leasing represents only a small part of the telecommunication business. Licenses for basic telecommunications services are still monopolized by the three state-owned enterprises, and no other companies are involved in other key services such as public network infrastructure construction.[28] In May 2016, China Broadcast Network

21 Drew Foerster, American Bar Association, "China's Legislature Gears Up to Pass a Sweepingly Vague Cybersecurity Law," May 2, 2016, http://www.americanbar.org/publications/blt/2016/05/02_foerster.html; "Counter-Terrorism Law (2015)," *China Law Translate,* December 27, 2015, http://bit.ly/2eZydih.

22 Jan Holthuis, "War of the Giants—Observations on the Anti-Monopoly Investigation in China Telecom and China Unicom," HIL International Lawyers & Advisers, Legal Knowledge Portal, March 2, 2012, http://bit.ly/1Mxc8SI; "Tighter Rules for Telecom Costs," *Shanghai Daily*, April 26, 2012, http://on.china.cn/1LJDfEV.

23 Lu Hui, "China Telecom, China Unicom pledge to mend errors after anti-monopoly probe," Xinhua, December 2, 2011, http://bit.ly/1RFKEdz; "Guo Jia Guang Dian Wang Luo Gong Si Jiang Qiang Cheng Li Zhong Yi Dong Wei Can Yu Chu Zi" [State Radio and Television Networks Will Be Set Up], Sina, November 15, 2012, http://bit.ly/1GbT0bw.

24 "Chinese Internet Choked by 'Fake Broadband' Providers," *Global Times*, October 8, 2012, http://www.globaltimes.cn/content/736926.shtml.

25 Lan Xinzhen, "Full-Pricing Autonomy," *Beijing Review*, May 29, 2014, http://bit.ly/1G3MsMf; Paul Mozur and Lorraine Luk, "China to Liberalize Telecommunications Pricing," *Wall Street Journal*, May 9, 2014, http://on.wsj.com/1NFam3s. Prices were previously regulated by the government.

26 工信部支持民资进入转售业务 打破垄断发文还不够, [MIIT supports private capital entering network leasing business, more antimonopoly policy is needed] http://it.sohu.com/20151230/n432995626.shtml.

27 重庆出台电信新规 想用哪家宽带用户可自主选择, March 2, 2016 http://cq.cqnews.net/html/2016-03/02/content_36455828.htm

28 中国广电成第四大运营商 业内称其仅拿到半个牌照 , May 6, 2016, http://finance.sina.com.cn/chanjing/gsnews/2016-05-06 doc-ifxryhhi8426724.shtml

(CBN) received a license for basic telecommunications business from MIIT,[29] but since it only provides landline service, it does not represent a threat to the three dominant players.[30]

Authorities exercise tight control over cybercafes and other public access points, which are licensed by the Ministry of Culture in cooperation with other state entities.[31] In practice, control can be difficult to enforce. The Ministry of Culture reported 14,000 illegally-operated internet cafés (*hei wangba*) in operation nationwide as of 2014.[32] In November 2014, the Chinese government loosened restrictions on opening new cybercafes, lifting a 2013 requirement that they had to be run by chain stores.[33]

Regulatory Bodies

Several government and CCP agencies are responsible for internet censorship at the local and national levels, but the process has been consolidated under Xi Jinping.

The (State Internet Information Office) SIIO was c eated in May 2011 to streamline regulation of online content, punish violators, and oversee telecommunications companies.[34] On August 26, 2014, the State Council formally authorized the SIIO to regulate and supervise internet content.[35] In December 2014, it launched a new website as the Cyberspace Administration of China (CAC) and Office of the Central Leading Group for Cyberspace Affairs.[36] After the coverage period of this report, Lu Wei, who commentators referred to as China's internet czar, was unexpectedly replaced as head of the CAC by Xu Lin, a former deputy of Xi Jinping.[37]

The CAC has an organizational affiliation o the Central Internet Security and Informatization Leading Group that was formed in February 2014 to oversee cybersecurity directly under Xi Jinping, making it the highest authority on internet policy in China.[38] In December 2014, the leading group took charge of the CNNIC, which issues digital certifica es to websites.[39]

Two regulatory bodies, the State Administration of Radio, Film, and Television (SARFT) and the Gen-

29 广电国网获得基础电信业务经营许可, May 10, 2016, http://www.sarft.gov.cn/art/2016/5/10/art_114_30759.html

30 中国广电获批基础电信业务牌照 暂难撼动三大运营商, May 6, 2016, http://finance.sina.com.cn/ oll/2016-05-06/doc-ifxryhhi8423048.shtml

31 These include the Public Security Bureau and the State Administration for Industry and Commerce. "Yi Kan Jiu Mingbai Quan Cheng Tu Jie Wang Ba Pai Zhao Shen Qing Liu Cheng" [A look at an illustration of the whole course of the cybercafe license application process], Zol.com, http://bit.ly/1QmkImh.

32 Jamie Fullerton, China Has Had Enough of Its Illegal Internet Cafés, December 8 2015, http://motherboard.vice.com/read/china-has-had-enough-of-its-illegal-internet-cafs

33 Many Zuo, "China eases restrictions on number of internet cafes but adds space requirements," *South China Morning Post*, November 24, 2014, http://bit.ly/1QmlcJf.

34 "China sets up State Internet Information Office" *China Daily*, May 4, 2011, http://bit.ly/1LMdB8M. See also Freedom House, "New Agency Created to Coordinate Internet Regulation," *China Media Bulletin*, May 5, 2011, http://bit.ly/1VR5RBG.

35 Xinhua, "State Internet Information Office egulates internet: Beijing," *Want China Times,* August 30, 2014, http://bit.ly/1k2Rhvt; Government of China, 国务院关于授权国家互联网信息办公室 负责互联网信息内容管理工作的通知, press release, January 2014, http://bit.ly/1VR6yLu.

36 Office f the Central Leading Group for Cyberspace Affairs website, http://bit.ly/1OzUsFS; David Feng, "Chinese Cyber Administration Office Goes Online" *Tech Blog 86*, December 31, 2014, http://bit.ly/1LMezBS.

37 China File, "A Grim Future for Chinese Web Freedom," *Foreign Policy, July 1, 2016,* http://foreignpolicy.com/2016/07/01/a-grim-future-for-chinese-web-freedom-lu-wei-internet-china/

38 Paul Mozur, "In China, Internet Czar Is Taking a Blunt Tone," *Bits* (blog), *New York Times*, October 31, 2014, http://nyti.ms/1GELosY; Shannon Tiezzi, "Xi Jinping Leads China's New Internet Security Group," *Diplomat*, February 28, 2014, http://bit.ly/1N9FBAn.

39 "CNNIC Undergoes Personnel Changes" [in Mandarin], *Guangming Daily,* December 27, 2014, http://bit.ly/1G3Oqwa.

eral Administration for Press and Publications (GAPP), both responsible for censorship in their respective sectors, merged in 2013 to form the State Administration of Press, Publications, Radio, Film, and Television (SAPPRFT).[40] The body's tasks include monitoring internet-based television and online videos. In addition, the Central Propaganda Department oversees the ideological inclination of online content.

In March 2016, Xinhua reported the establishment of the non-profit Cyber Security Association f China to promote online security.[41] It is made up of more than 200 member technology and cybersecurity companies, research institutions, and headed by Fang Binxing, who is recognized as the developer of the Great Firewall.[42]

Limits on Content

The CCP propaganda department, government agencies, and private companies employ thousands of people to monitor, censor, and manipulate content. A range of issues are systematically censored, including independent evaluations of China's human rights record, critiques of government policy, discussions of politically and socially sensitive topics, and the authorities' treatment of ethnic minorities. Routine censorship is reinforced during politically sensitive events or in response to breaking news. During the coverage period, online entertainment and user-generated news reports were subject to heightened censorship and punishment. The heavily manipulated online environment still provides space for average citizens to express themselves or criticize the state than any other medium in China, but the frequency and the scale of digital activism were weakened over the years.

Blocking and Filtering

The Chinese government uses a sophisticated and ever-evolving censorship apparatus, incorporating both automated mechanisms and human monitors, to block and fil er material that criticizes or challenges individuals, policies, or events considered integral to the one-party system. The most censored news topics in 2015 were health and safety, economics, official w ongdoing, media censorship, the reputation of the party or officials, and civil societ .[43] During a military parade in September, an image of Winnie the Pooh in a toy car was heavily censored because the image was used as a spoof of President Xi Jinping.[44] In the aftermath of a series of deadly explosions at a container storage station at the port of Tianjin on August 12, 2015, websites and social media accounts were closed and at least two internet users were detained for posting misinformation online.[45]

Over the last several years, censors have increasingly blocked international news websites, especially those with Chinese-language websites, for their reporting on corruption and illicit wealth among

40 Romi Jain, "China keeps its telecoms sector close," *Asia Times Online*, January 29, 2014, http://bit.ly/1LMeKgL.

41 Xinhua, "China's fi st national NPO in cyber security founded," March 25, 2016, http://news.xinhuanet.com/english/2016-03/25/c_135223674.htm.

42 Austin Ramsy, "Architect of China's 'Great Firewall' Bumps Into It, "*New York Times,* April 7, 2016, http://www.nytimes.com/2016/04/07/world/asia/china-internet-great-fi ewall-fang-binxing.html.

43 Sarah Cook, "China's most censored news topics in 2015," Freedom House, January 2016, https://freedomhouse.org/article/china-media-bulletin-issue-no-111-january-2016.

44 Tessa Wong, The military parade posts China censored, BBC, 3 September 2015, http://www.bbc.com/news/world-asia-china-34137519

45 天津爆炸受害业主连日请愿 网民因造谣被行政拘留, August 17, 2015, Radio Free Asia, http://www.rfa.org/mandarin/yataibaodao/meiti/yf1-08172015100130.html

high-level officials, as ell as a range of other issues thought to challenge the government. At least 15 of 18 global news websites tracked by the nonprofit news o ganization ProPublica were inaccessible inside China as of mid-2016.[46] Websites of *The Economist* and *Time* magazines were newly blocked during the coverage period of this report, apparently in reprisal for critical coverage of Xi Jinping.[47]

In April 2016, the International Consortium of Investigative Journalists released the Panama Papers, confidential documents containing the identities f shareholders of more than 214,000 offshore companies. The documents named relatives of at least eight current or former members of China's top leaders, including Deng Jiagui, brother-in-law of Xi Jinping. Discussion of the Papers was quickly purged from Chinese websites.[48]

In March 2016, the website of *South China Morning Post*, the largest English newspaper in Hong Kong, was blocked and social media accounts affilia ed with the paper were disabled.[49] The paper has faced periodic censorship before, including during Umbrella Revolution protests that shook Hong Kong in autumn 2014.[50] The reason for the latest incident was not clear, though the paper had reported on allegations that Chinese security agents abducted Hong Kong-based booksellers to face criminal charges in China, after publishing books perceived as critical of Xi Jinping.[51] It had also published a column linking Xi's political strategy to Mao Zedong's Cultural Revolution, according to international news reports.[52] The block came a few months after the Alibaba Group, a Chinese e-commerce company, purchased media assets owned by the SCMP group, including the *South China Morning Post*, in December 2015, prompting concerns about its editorial independence.[53] In mid-2016, the site was still blocked.

The system responsible for such automated, technical blocking of foreign websites is commonly referred to as China's "Great Firewall." In some cases, whole domain names or internet protocol (IP) addresses are blocked, with users receiving an explicit message about illegal content. Other interventions are less visible. For example, observers have documented unusually slow speeds that indicate deliberate throttling, which delays the loading of targeted sites and services.[54]

Authorities also use deep packet inspection (DPI) to scan both a user's request for content and the results returned for any blacklisted keywords. Once these are detected, the technology signals both

46 Sisi Wei, "Inside the Firewall: Tracking the News that China Blocks," ProPublica, February 13, 2015, https://projects.propublica.org/fi ewall.

47 Josh Horwitz, "The Economist's website is now censored in China—and all it took was one satirical cover," *Quartz,* April 7, 2016, http://qz.com/655995/the-economists-website-is-now-censored-in-china-and-all-it-took-was-one-satirical-cover/; Emily Feng, "China Blocks Economist and Time Websites, Apparently Over Xi Jinping Articles," *New York Times,* April 9, 2016, http://www.nytimes.com/2016/04/09/world/asia/china-blocks-economist-time.html.

48 Tom Phillips, All mention of Panama Papers banned from Chinese websites, April 5, 2016, The Guardian, http://www.theguardian.com/news/2016/apr/05/all-mention-of-panama-papers-banned-from-chinese-websites

49 中国网信办回应《南华早报》中文帐号被删, March 11, 2016, BBC, http://www.bbc.com/zhongwen/simp/china/2016/03/160311_china_scmp; http://www.reuters.com/article/hongkong-china-newspaper-idUSL1N16J06R.

50 Patrick Frater, "China Extends Media Blocking as Hong Kong Protests Swell," *Variety,* 2014, http://variety.com/2014/biz/asia/china-extends-media-blocking-as-hong-kong-protests-swell-cyberwarfare-alleged-1201319136/

51 中国网信办回应《南华早报》中文帐号被删, March 11, 2016, BBC, http://www.bbc.com/zhongwen/simp/china/2016/03/160311_china_scmp.

52 Heather Timmons and Zheping Huang, "Hong Kong's SCMP is being blocked in China for cheering on Xi Jinping," March 10, 2016, http://qz.com/635915/hong-kongs-scmp-is-being-blocked-in-china-for-cheering-on-xi-jinping/

53 David Barboza, "Alibaba Buying South China Morning Post, Aiming to Influence Media" *New York Times*, December 12, 2015, http://www.nytimes.com/2015/12/12/business/dealbook/alibaba-scmp-south-china-morning-post.html?_r=0.

54 "In Tandem with Slower Economy, Chinese Internet Users Face Slower Internet This Week," *China Tech News*, November 6, 2012, http://bit.ly/1L9Pm0L.

sides of the exchange to temporarily sever the connection. Such granular control is less noticeable to users because specific ages can be blocked within otherwise approved sites, and because the interruption appears to result from a technical error.[55] Returning fake pages, or replacing the requested site with content retrieved from an unrelated IP address using a technique known as DNS poisoning, is another routine method of disrupting access to specific con ent.

In practice, fil ering varies depending on timing, technology, and geographical region. ISPs reportedly install fil ering devices differently, in the internet backbone or even in provincial-level internal networks, a development that would potentially allow interprovincial fil ering.[56]

Censorship decisions are arbitrary, opaque, and inconsistent, in part because so many individuals and processes are involved. Blacklists periodically leak online, but they are not officially published. There are no formal avenues for appeal. Criticism of censorship is itself censored.[57]

Software developers, both domestic and overseas, have created applications offering access to virtual private networks (VPNs), which encrypt the user's traffic and eroute it through a server outside the fi ewall to circumvent technical fil ering. In 2014, China boasted the largest number of VPN users in the world, nearly 93 million, according to Global Web Index.[58]

In January 2015, Chinese authorities reported an upgrade to its national fi ewall that blocked several providers of VPNs, including the U.S.-based StrongVPN and Golden Frog, which is registered in Switzerland. Officials claimed that the upgrade was meant o uphold "cyberspace sovereignty."[59] Users of the Seychelles-based service Astrill have reported connectivity problems in the past two years, and the company announced the possibility of its service being disrupted during the two political meetings. In mid-2016, users in Beijing and Shanghai reported having been unable to use Astrill since early March.[60] Separately, a 2015 amendment to the criminal law offered possible legal grounds for prosecuting circumvention tool developers.[61]

Certain web applications are totally blocked, isolating the Chinese public from a global network of user-generated content. According to GreatFire.org, an organization that monitors blocked content in China, 138 of Alexa's top 1,000 websites in the world were blocked in 2016.[62] These include YouTube, Google, Facebook, Flickr, SoundCloud, and WordPress.[63] Services operated by Google including Google Maps, Translate, Calendar, and Scholar were blocked in 2014;[64] Google Analytics, which provides audience data to website owners, remained operational, according to the London-based

55 Ben Wagner et al., "Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control,'" Global Voices Advocacy, June 25, 2009, http://bit.ly/1GbWFGq.

56 Xueyang Xu, Z. Morely Mao, and J. Alex Halderman, "Internet Censorship in China: Where Does the Filtering Occur?" *Passive and Active Measurement*, (2011): 133–142, http://pam2011.gatech.edu/papers/pam2011--Xu.pdf.

57 King, Pan, and Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression."

58 Jason Mander, "90 Million VPN users in China have accessed restricted social networks," GlobalWebIndex blog, November 24, 2014, http://bit.ly/1VR9Y0M.

59 "China blocks virtual private network use," BBC, January 26, 2015, http://bbc.in/1CrMgBJ; Jon Russell, "China Cracks Down On VPN Services After Censorship System 'Upgrade,'" *TechCrunch*, January 23, 2015, http://tcrn.ch/1BPJtUe.

60 翻不过"长城" 两会期间VPN失, June 9, 2016, 参考网，http://www.fx361.com/page/2016/0309/166807.shtml

61 Oiwan Lam, China Is Blocking Circumvention Tools With Help of Cloud Service Providers, Global Voices, January 20 2016, https://globalvoices.org/2016/01/20/china-is-blocking-circumvention-tools-with-help-of-cloud-service-providers/

62 GreatFireChina, https://en.greatfi e.org/analyzer.

63 GreatFireChina, "Censorship of Alexa Top 1000 Domains in China," https://en.greatfi e.org/search/alexa-top-1000-domains.

64 Julie Makinen, "China broadens crackdown on Google services," *Los Angeles Times,* June 13, 2014, http://lat.ms/1qQMKtO.

Guardian newspaper.[65] Other social media services like the photo-sharing platform Instagram and Viber were blocked during the 2014 Umbrella Revolution.[66] Instagram had already been removed from online Android application stores run by the Chinese services Baidu, Xiaomi, Wandonjia, Qihou360, Tencent, and 91 Wireless in July 2014.[67]

Many social media applications produce sanitized versions for the mainland Chinese market. In 2012, Evernote launched a separate service for the Chinese mainland, with modified terms of use containing a list of nine categories of "undesirable information." In January 2015, it disabled the public note feature, which had been used to share news and information about the Umbrella Revolution.[68] LinkedIn, which censors briefly blocked in 2011,[69] launched a Chinese-language version in early 2014.

Search requests that include blacklisted keywords also trigger China's censorship apparatus, producing blank or severely limited results. For example, in recent years, the number 535, signifying "May 35th," a popular way to refer to the June 4 anniversary of the Tiananmen Square crackdown, has gone missing on the Chinese internet.[70] In mid-2015, users reported being unable to make digital financial transfers if the amount contained sensitive numbers such as 6.4 yuan, 64 yuan or 89.64 yuan.[71]

Content Removal

The government has generally not been transparent about content controls, telling international reporters in 2013 that "the perception that the government has placed any restrictions on the internet is untrue."[72] Laws passed or pending during the coverage period were more explicit about restrictions implemented in the name of security which could also threaten legitimate speech.

The antiterrorism law passed in December 2015 instructed companies to delete terrorist or extremist content or "close down relevant websites" at the authorities' request, and also to implement "precautionary measures" against the transmission of such content, with possible administrative detentions for noncompliance (see Restrictions on Connectivity and Legal Environment). While international law supports restrictions on content that incites violence in some circumstances, ethnic and religious minority groups in China have been subject to rights violations on grounds that their legitimate dissent amounts to a terrorist or security threat. A draft cybersecurity law released to the public in July 2015 separately stated that the CAC or relevant departments, "where discovering information the release or transmission of which is prohibited by laws [or] administrative regulations, shall re-

65 Maria Repnikova and Timothy Libert, "Google is returning to China? It never really left," *Guardian*, September 21, 2015, http://bit.ly/1Ku8EOi.

66 "China blocked information of the Occupy Central in Hong Kong" [in Mandarin], September 30, 2014, https://pao-pao.net/article/192; Josh Chin and Eva Dou, "Hong Kong Protests Lead to Censorship on WeChat," *China Real Time Report*, *Wall Street Journal*, October 3, 2014, http://on.wsj.com/1hD6Sjq.

67 Instagram內地「被下架」, July 10, 2014, Mingpao, http://bit.ly/2fjRZUk.

68 Catherine Shu, "Evernote's Chinese Service Disables Public Note Feature," *TechCrunch*, January 5, 2014, http://tcrn.ch/1GbZozn.

69 Keith B. Richburg, "Nervous about unrest, Chinese authorities block web site, search terms," *Washington Post,* February 25, 2011, http://wapo.st/1Mps054.

70 Oiwan Lam, Why the Numbers 64, 89 and 535 Are Missing From the Chinese Internet, Global Voices, June 4, 2015, https://globalvoices.org/2015/06/04/a-special-day-when-some-numbers-are-missing-in-the-chinese-internet/

71 Tiananmen Anniversary Makes Money Transfers in China Trickier, June 3, 2015, http://www.bloomberg.com/news/articles/2015-06-03/tiananmen-anniversary-makes-money-transfers-in-china-trickier

72 Heather Timmons and Ivy Chen, "Beijing calls fears over internet crackdown 'paranoia,' briefly detains corruption-fightin blogger," *Quartz*, September 18, 2013, http://bit.ly/1PrOBDw.

quest the network operators stop transmission, employ disposition measures such as deletion, and store relevant records; for information described above that comes from outside mainland People's Republic of China, they shall notify the relevant organization to adopt technological measures and other necessary measures to block the transmission of information."[73] That law was still pending in mid-2016 (see Legal Environment).

Antipornography and antirumor campaigns are a long-standing cover for government censorship of social and political content. On June 8, 2015, the CAC announced that 100 websites and 20,000 social media accounts were shut down during an "anti-internet blackmail and paid content removal" campaign. However, legitimate accounts were also affected: Sina Weibo and Tencent Weibo accounts of human rights lawyer Liu Xiaoyuan were closed on June 4, 2015.[74] Another purge in early 2016 wiped out 580 accounts, including some operated by outspoken celebrities like businessman Ren Zhiqiang, on grounds they had "abused their own influence o attack the party and the government."[75] Ren, a former property developer, had criticized Xi Jinping's media policy to more than 30 million followers in February, and was threatened with expulsion from the party in May.[76]

Censors targeted online entertainment in the past year. In June 2015, the Ministry of Culture announced its 23rd illegal internet "culture activities" list, which focused on animation and cartoons online; eight websites were shut down.[77] In August, 120 songs were banned by the Ministry of Culture for "containing content that promotes sex, violence or crime, or harms public morality," adding them to the list of content for online portals to monitor and delete.[78] SAPPFRT targeted popular drama series after the agency's head of the television drama management division announced that they would be regulated as broadcast television shows.[79] At least six digital series were removed, two of them permanently, due to content deemed to violate the regulations, including violence, indecency, and superstition.[80] In November, SAPPFRT launched a campaign to purge television set top boxes which can receive overseas television signals through the internet, including VOA and the BBC.[81] In April 2016, the regulator required Apple to withdraw the company's iBooks and iTunes stores six months after their launch in China, according to the *New York Times*.[82]

Mobile service providers monitor text messages and delete pornographic or other "illegal" content.[83] Users report receiving blank messages in place of banned keywords, though what content is banned

73 Cybersecurity Law (Draft), translated by China Law Translate, http://chinalawtranslate.com/cybersecuritydraft/?lang=en.

74 中国专项整治网络违规 维权律师微博账户被删, June 9, Radio Free Asia, http://www.rfa.org/mandarin/Xinwen/8-06092015115226.html

75 Anne Henochowicz, "Social Media Purge Goes Far Beyond Ren Zhiqiang," *China Digital Times,* March 1, 2016, http://chinadigitaltimes.net/2016/03/social-media-purge-goes-far-beyond-ren-zhiqiang/

76 Edward Wong, "China Puts a Tycoon, Ren Zhiqiang, on Probation for Criticizing Policies," May 3, 2016, http://www.nytimes.com/2016/05/03/world/asia/china-ren-zhiqiang.html.

77 文化部關停8家違法動漫網站 首次公布動漫"黑名單, June 8, 2015, http://culture.people.com.cn/BIG5/n/2015/0608/c1013-27121959.html

78 Hu Xin, The Day the Music Died: China Blacklists 120 Songs for 'Morality' Violations, August 12 2015, http://blogs.wsj.com/chinarealtime/2015/08/12/the-day-the-music-died-china-blacklists-120-songs-for-morality-violations/

79 "太子妃"被下架 郑晓龙:网剧与电视剧审查标准应一致 January 22, 2016 http://ent.people.com.cn/n1/2016/0122/c1012-28076699.html

80 "太子妃"等热门网剧下架 传广电总局勒令删改重审, People.cn, January 21, 2016, http://media.people.com.cn/n1/2016/0121/c40606-28072084.html

81 广电总局禁令又来了，直播看不了了，电视盒子这是要死了么, Huxiu.com, http://www.huxiu.com/article/131762/1.html

82 Paul Mozur and Jane Perlez, "Apple Services Shut Down in China in Startling About-Face," *New York Times,* April 22, 2016, http://www.nytimes.com/2016/04/22/technology/apple-no-longer-immune-to-chinas-scrutiny-of-us-tech-fi ms.html?_r=0.

83 Agence France-Presse, "China Mobile Users Risk SMS Ban in Porn Crackdown," *ABS-CBN News,* January 14, 2010, http://bit.ly/1Ljww5q; Elaine Chow, "So about that sexting ban in China," *Shanghaiist,* January 20, 2012, http://bit.ly/1PemWqk.

appears to vary.[84] Instant-messaging services such as TOM-Skype and QQ include programming that downloads updated keyword blacklists regularly.[85] Other companies employ human censors to delete posts, sometimes before they appear to the public.[86] Experts say staff members receive as many as three censorship directives per day by text message, instant message, phone call, or e-mail.[87] Most come from local propaganda officials.

Media, Diversity, and Content Manipulation

Online journalists regularly practice self-censorship. Editors and reporters who post banned content, or content that is critical of the CCP, its high-ranking members, or its actions now or in the past, risk disciplinary warnings, job loss, or even criminal detention.

Authorities warned online news providers of tighter scrutiny in 2015,[88] and threatened the Sina web portal with suspension in April for failing to prevent violations.[89] In May, the agency published a list of news organizations that were "authorized to provide websites for reposting news."[90] Formerly outspoken media outlets under the Nanfang Daily Group, including *Southern Weekend*, *Southern Metro Daily*, and *21st Century Business Herald*, were overhauled in late 2015 to comply with instructions from the propaganda department in Guangdong, reducing the diversity of critical reporting published both in print and on their respective websites.[91] In February 2016, Xi Jinping visited three key state media outlets, the People's Daily, Xinhua Agency, and CCTV, and emphasized the leadership of the Party in state media.[92] In Xi's speech on media policy, he highlighted three points: putting the party fi st, controlling media of all forms, and making the party's message more appealing.[93]

Not all media remain submissive. Just weeks after Xi Jinping delivered a speech demanding absolute loyalty from the media, Caixin reported on its English-language website that the CAC ordered the removal of an interview they posted on the Chinese website on the issue of free speech.[94] However, that report was later replaced with an unrelated article.[95]

Propaganda officials also manipula e online content, instructing internet-based outlets to amplify

84 Elaine Chow, "An Alleged List of Banned SMS Terms from China Mobile and Co.," *Shanghaiist*, January 4, 2011, http://bit.ly/1MpvfcT.

85 TOM-Skype is a joint venture between Skype and Chinese wireless service TOM Online. Vernon Silver, "Cracking China's Skype Surveillance Software," *Bloomberg Business*, March 8, 2013, http://bloom.bg/1jwMz8G; Jedidah R. Crandall et al., "Chat Program Censorship and Surveillance in China: Tracking TOM-Skype and Sina UC," *First Monday* 18, no. 7 (2013), http://bit.ly/1ZAQfaq; Jeffrey Knockel, "TOM-Skype Research," http://cs.unm.edu/~jeffk/tom-skype/.

86 King, Pan, and Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression."

87 Xiao Qiang, "From 'Grass-Mud Horse' to 'Citizen': A New Generation Emerges through China's Social Media Space," (presentation, Congressional-Executive Commission on China, Washington, DC, November 17, 2011), http://1.usa.gov/19dzOZn.

88 "China's Internet Censor Increases Scrutiny on News Portals," *Bloomberg Business*, April 28, 2015, http://bloom.bg/1bPLy8l.

89 Xinhua, "Sina faces suspension over lack of censorship," *People China*, April 11, 2015, http://bit.ly/1PrQu2V.

90 "Government Tells People Who Is Authorized to Repost News Online," *Fei Chang Dao* (blog), May 2015, http://bit.ly/1K7qtPw.

91 中共南方报业传媒集团党委关于巡视整改情况的通报, http://gdjct.gd.gov.cn/xunshizhenggai2015/31829.jhtml

92 时事大家谈：习近平访三大官媒，强调官媒姓党 VOA, February 23, 2016, http://www.voachinese.com/content/VOAWeishi-IssuesandOpinions-20160222-why-xi-jinping-visited-government-news-outlets/3201386.html

93 Xi Jinping visits flagship sta e media, lays out vision for party control. China Media Bulletin Issue No. 113 March 2016 https://freedomhouse.org/article/china-media-bulletin-issue-no-113-march-2016

94 Chinese magazine challenges government over censorship, http://www.theguardian.com/world/2016/mar/08/chinese-magazine-challenges-government-censorship-organ

95 "Article About Government Censorship of Article About Politician's Complaints of "Frightening" Censorship of Article About Chilling Effects on Speech Gets Censored," *Fei Chang Dao,* March 13, 2016, http://blog.feichangdao.com/2016/03/article-about-government-censorship-of.html.

content from state media. Since 2005, propaganda units at all levels have trained and hired web commentators, known colloquially as the "50 Cent Party," to post pro-government remarks and influence online discussions.[96] These commentators also report users who have posted offending statements, target government critics with negative remarks, or deliberately muddy the facts of a particular incident.[97] Coordinated smear campaigns are used to discredit high-profile government critics.[98]

The work also extends beyond China's borders to social media apps that are actually banned for mainland users, such as Twitter. One 2014 analysis identified over 2,500 "50 Cent" users spreading misinformation on Twitter.[99] In November 2015, the People's Daily was found to have a large percentage of inactive followers, leading observers to conclude that the fake accounts were used to create a perception of popularity. More than 58 percent of the account's supporters had posted fewer than 5 times themselves.[100]

These methods are not always effective, however. Many government-paid commenters are more concerned about filling their quota than mounting a convincing argument, and web users are wary of content manipulation. Companies also pay for "astroturfing"—positive comments promoting products or services—which further erodes public trust in online content (commercial commenters are colloquially known as the "internet water army").[101]

In recent years, "spreading positive energy among society" has become a major propaganda strategy.[102] Local authorities have started to mobilize *ziganwu*, or volunteer commentators, to promote the government's image and refute negative online depictions of the party or government officials [103] While the 50 Cent Party is maintained by economic interest, *ziganwu* are mobilized by ideology. A document leaked in January 2015 revealed hundreds of thousands of "youth league online commentators" in China's higher-education institutions, tasked with swaying students against supposed Western values.[104] More recruits were being sought.[105] In May 2015, documents leaked online indicated the league had millions of recruits.[106] Nationalism and xenophobia are prominent components of Chinese cyberspace, though censorship that targets rational dissent instead of inflammatory dis-

96 David Bandurski, "Internet spin for stability enforcers," China Media Project, May 25, 2010, http://cmp.hku.hk/2010/05/25/6112/.

97 These propaganda workers are colloquially known as the 50 Cent Party due to the amount they are reportedly paid per post, though recent reports put the going rate as low as 10 cents, while some commentators may be salaried employees. See Perry Link, "Censoring the News Before It Happens," *New York Review* (blog), *New York Review of Books*, July 10, 2013, http://bit.ly/1bj1vTt; Rongbin Han, "Manufacturing Consent in Censored Cyberspace: State-Sponsored Online Commentators on Chinese Internet Forums" (paper for Annual Meeting of America Political Science Association, New Orleans, August 31–September 2, 2012), http://ssrn.com/abstract=2106461.

98 Murong Xuecun, "Beijing's Rising Smear Power," *New York Times*, September 21, 2014, http://nyti.ms/1OvsWuZ.

99 "The New Generation of Fifty-Centers on Twitter," *I YouPort*, October 9, 2014, https://iyouport.com/en/archives/676.

100 克里斯蒂安•谢泼德,中国官媒Twitter账号被疑"僵尸粉"过多, FT中文网 http://m.ftchinese.com/story/001064972

101 Rongbin Han, "Manufacturing Consent in Cyberspace: China's 'Fifty-Cent Army'," *Journal of Current Chinese Affairs* 44, no. 2 (2015): 105-134, http://bit.ly/1R9RKWK) Cheng Chen, et al, "Battling the Internet Water Army: Detection of Hidden Paid Posters," arXiv, November 18, 2011, http://arxiv.org/abs/1111.4297.

102 Oiwan Lam, Chinese Authorities Think Internet Companies Should Reward Netizens Who 'Spread Good News', Global Voices, December 11, 2015, https://globalvoices.org/2015/12/11/chinese-authorities-think-the-internet-could-use-more-positive-energy/

103 Local Chinese Authorities Use Internet Slang 'Ziganwu' in Their Propaganda Recruitments, Global Voices June 15, 2015 https://globalvoices.org/2015/06/15/local-chinese-authorities-use-internet-slang-ziganwu-in-their-propaganda-recruitment/

104 Sandra Fu, "Central Committee of Communist Youth League Issues an Announcement," *China Digital Times*, January 19, 2015, http://bit.ly/1jmXT7R.

105 Xu Yangjingjing and Simon Denyer, "Wanted: Ten million Chinese students to "civilize" the Internet," *Washington Post*, April 10, 2015, http://wapo.st/1NbD9tb.

106 How China's Online Civilization Army Turned a Youth Street Fight into a Patriotic Struggle, July 30, 2015, Global Voices, https://globalvoices.org/2015/07/30/how-chinas-online-civilization-army-turned-a-youth-street-figh -into-a-patriotic-struggle/

course arguably magnifies their im act. In extreme cases, online quarrels have resulted in real world violence.[107]

Government employees also openly engage citizens in online discussions. In March 2014, the state news agency Xinhua announced a round of internet supervision training courses for officials ac oss government institutions, including the police and the judiciary. The courses offered fi e qualific - tions from assistant to senior manager costing 6,800 yuan (US$ 1,108).[108]

Still, political discourse can be vigorous online, even about democracy and constitutional government.[109] This is partly because the leadership redefined democratic go ernance as "the Chinese Communist Party governing on behalf of the people" in 2005.[110] A certain amount of open discussion also allows officials o monitor public sentiment, debunk "enemy" ideology,[111] and conduct internal power struggles. Censors employed by Sina allowed "more room for discussions on democracy and constitutionalism because there are leaders who want to keep the debate going," according to one 2013 report.[112]

Domestic internet fi ms benefit comme cially from the blocking of foreign social media since they gain market share, but they are obliged to prevent banned content from circulating as part of their licensing requirements. Chinese company executives also enjoy political patronage.[113] About a third of mobile internet users used domestic microblogging applications like Sina Weibo and Tencent's Weixin in 2015,[114] though Weibo in particular has suffered due to censorship requirements, and its use to promote social and political causes has declined.[115] Weibo's distinct feature is the comment thread developed in response to individual posts; the threads are lost if the original post is censored, and the feature can also be shut off to prevent a given post from gaining traction.[116] During the two meetings (annual plenary sessions of the National People's Congress (NPC) and the National Committee of the Chinese People's Political Consultative Conference (CPPCC) in 2016, the comment function on many official eibo accounts was disabled by the company's account maintenance team.[117]

Sina's efforts to manage Weibo content are well documented. Staff, reportedly 150 people working

107 How China's Online Civilization Army Turned a Youth Street Fight into a Patriotic Struggle, July 30, 2015, Global Voices, https://globalvoices.org/2015/07/30/how-chinas-online-civilization-army-turned-a-youth-street-figh -into-a-patriotic-struggle/

108 Oiwan Lam, "Chinese Government is "Winning" Internet Ideology Battle," *Global Voices Advocacy*, November 8, 2013, http://bit.ly/1Ps0fy4; Alastair Sloan, "China ramps up army of "opinion monitors," Index on Censorship, March 25, 2014, http://bit.ly/1NFCrYq.

109 Xu Qianchuan, "Constitution Debate Holds Broader Reform Implications," *Caijing*, July 16, 2014, http://bit.ly/1Ps0J7p; King, Pan, and Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression"; Ashley Esarey and Xiao Qiang, "Digital Communication and Political Change in China," *International Journal of Communication* 5 (2011): 298–319, http://bit.ly/1LKgXCU. Xiao Qiang was an advisor for this report.

110 Richard McGregor, *The Party: The Secret World of China's Communist Rulers* (New York: Harper Collins, 2010), 20.

111 See "以敢于亮剑的精神确保西藏意识形态领域安全," November 1, 2013, http://bit.ly/1GGlJQC.

112 See "China must crack down on critical online speech: party journal," Reuters, September 16, 2013, http://reut.rs/1GGsphD.

113 Freedom House, "Tech Company Leaders Join Legislative, Advisory Bodies," *China Media Bulletin*, March 7, 2013, http://bit.ly/1R9T77X.

114 China Internet Network Information Center (CNNIC),中国互联网络发展状况统计报告 [The 37th Report on the Development of the Internet in China], January 2016

115 How China stopped its bloggers Angus Grigg, http://www.afr.com/technology/social-media/how-china-stopped-its-bloggers-20150701-gi34za

116 Gady Epstein, "The Great Firewall: The Art of Concealment," *Economist*, April 6, 2013, http://econ.st/145qZuP.

117 中国两会微博评论被关闭 民众不满遭"嘘声", March 7, 2016, Radio Free Asia, http://www.rfa.org/mandarin/yataibaodao/meiti/yf2-03072016102954.html

12-hour shifts,[118] delete individual posts or accounts, often within 24 hours of an offending post, but sometimes long after publication;[119] make published posts visible only to the account owner; and personally warn individual users.[120] Moreover, hundreds of terms have been automatically fil ered from Weibo search results over time.[121]

Weibo's fall from popularity began when it was punished with restrictions on some of its functions in 2012 for failing to curb "rumors."[122] In 2013, following an intensified antirumor cam aign, Weibo said 1,000 accounts had been shuttered for posting false information, out of a total 100,000 accounts that were disabled for harassment and other violations.[123] Activity on the platform dropped by an estimated 70 percent;[124] one 2014 study said that approximately 5 percent of Weibo users were still active.[125] In January 2014, the CNNIC reported that 38 percent of Weibo users had migrated to Weixin.[126] In 2015, Tencent reported a combined 500 million monthly active users for Weixin and its international equivalent.[127] Weixin users have the option to restrict updates to a closed circle of connections, and can send audio messages that bypass keyword censorship, though it is also subject to monitoring.[128]

On June 1, 2015, internet police units from local governments started a "speech inspection campaign" on major social media platforms including Weibo and Weixin. The campaigns, which built on existing practices but enlisted more police to enforce them, were intended to detect "illegal and harmful information" and "educate and warn" those who violate the law.[129] Separately, the antiterrorism law passed in December 2015 barred social media users from sharing information about acts of terror that could lead to copycat incidents, or spreading "cruel" or "inhuman" images.[130]

Regulations passed or proposed during the coverage period had the potential to further strengthen state control of companies sharing digital content:

- In June 2015, the State Council drafted "Methods of Regulating Audio and Video programming on the Internet (revised version)" (*hulianwang deng xinxi wangluo chuanbo shiting*

118 Li Hui and Megha Rajagopalan, "At Sina Weibo's censorship hub, China's Little Brothers cleanse online chatter," Reuters, September 11, 2013, http://reut.rs/1LMCa5z.

119 Keith B. Richburg, "China's 'weibo' accounts shuttered as part of internet crackdown," *Washington Post*, January 3, 2013, http://wapo.st/1ZBq82V.

120 Xiao, "From 'Grass-Mud Horse' to 'Citizen': A New Generation Emerges through China's Social Media Space."

121 "How a Weibo post gets censored: what keywords trigger the automatic review fil ers," *Blocked on Weibo* (blog), November 26, 2014, http://bit.ly/1LtbwMR; Xiao, "From 'Grass-Mud Horse' to 'Citizen': A New Generation Emerges through China's Social Media Space". See also Tao Zhu et al., "The Velocity of Censorship: High-Fidelity Detection of Microblog Post Deletions" (paper for 22nd USENIX Security Symposium, Washington, DC, August 2013), arXiv, http://bit.ly/1G4dIdx; King-wa Fu and Michael Chu, "Reality Check for the Chinese Microblog Space: A Random Approach," *PLoS ONE* 8, no. 3 (2013), http://bit.ly/1LMCP6R.

122 Xinhua, "China's major microblogs suspend comment function to 'clean up rumors,'" *People's Daily Online*, March 31, 2012, http://bit.ly/1RGh3kn.

123 "Sina shuts down weibo accounts," *China Daily,* November 14, 2013, http://bit.ly/1OvymWC.

124 Malcolm Moore, "China kills off discussion on Weibo after internet crackdown," *Telegraph,* January 30, 2014, http://bit.ly/1fDGbEW.

125 活跃度下降 新浪微博只有5%用户发内容, April 11 2014, http://tech.163.com/14/0411/16/9PIIGA13000915BF.html

126 See CNNIC, 中国互联网络发展状况统计报告, January 2014, http://bit.ly/1LMDtBB.

127 Lulu Yilun Chen, "Tencent Climbs as Ad Surge Boosts WeChat Earnings Outlook," *Bloomberg Business*, March 18, 2015, http://bloom.bg/1Ltc8Cc.

128 Alexa Oleson, "China's New Media Species, Now Endangered?" *Foreign Policy*, March 15, 2014, http://atfp.co/1OvyDsJ.

129 第二批139家网警执法账号集中上线, August 13 2015, http://media.people.com.cn/n/2015/0813/c40606-27453939.html-voices/

130 Ben Blanchard, "China passes controversial counter-terrorism law," Reuters, December 28, 2015, http://www.reuters.com/article/us-china-security-idUSKBN0UA07220151228.

jiemu guanli banfa).[131] The draft proposed that all internet content providers offering video or audio broadcasting services must have staff responsible for content censorship, or face fines of up to 30,000 RMB. In addition, the regulation restricted news broadcasting online to city-level radio and television stations, essentially banning user-generated news content. It had yet to be finalized by the end of the coverage period.

- In February 2016, the State Administration of Press, Publication, Radio, Film and Television (SAPPRFT) and the Ministry of Industry and Information Technology (MIIT), jointly issued the Online Publication Services Administrative Provisions, which came into effect on March 10, 2016. The provisions clarified restrictions on foreign investment in online publishing activities, and listed requirements for domestic companies to obtain an online publishing permit. As well as compliance with censorship, the requirements included at least eight full time editorial or publishing staff, potentially increasing the cost of sharing content online.[132]

- In April 2016, regulators sought feedback from major Chinese internet companies on a proposal that the state purchase a one percent share in major Chinese internet companies like Baidu and Tencent.[133] Observers said this could strengthen state influence over content distributed by the platforms, but details of how it might work remained unclear at the end of the coverage period.

Despite technical filtering, enforced self-censorship, and manipulation, the internet is a primary source of news and a forum for discussion, particularly among the younger generation. Chinese cyberspace is replete with online auctions, social networks, homemade music videos, a large gaming population, and spirited discussion of some social and political issues. Overtly political organizations, ethnic minorities, and persecuted religious groups remain underrepresented, though they have used the internet to disseminate banned content, and overseas media and human rights groups report sending emails to subscribers in China with news, instructions on circumvention technology, or copies of banned publications. Civil society organizations involved in charity, education, healthcare, and other social and cultural issues often have a vigorous online presence.

Users combat censorship by opening versions of the same blog on different sites and circulating banned information directly through peer-to-peer networks, which bypass central servers. Text rendered as image, audio, or video files can evade keyword sensors. Humorous neologisms, homonyms, and cryptic allusions substitute for banned keywords, forcing censors to filter seemingly innocuous vocabulary like "tiger."[134] This version of the Chinese internet does not resemble a repressed information environment so much as "a quasi-public space where the CCP's dominance is being constantly exposed, ridiculed, and criticized, often in the form of political satire, jokes, videos, songs, popular poetry, jingles, fiction, Sci-Fi, code words, mockery, and euphemisms."[135]

131 信息网络传播视听节目管理办法公开征求意见, June 12 2015, People's Daily, http://legal.people.com.cn/n/2015/0612/c42510-27143264.html

132 Hogan Lovells, "Are Foreigners Banned from Publishing on the Internet in China," May 2016, http://f.datasrvr.com/fr1/716/75489/Final_Publishing_on_Intranet.pdf

133 China Wants to Own Small Stake in Web Firms, http://www.wsj.com/articles/china-wants-to-own-small-stake-in-web-firms-1461781500; http://www.rfa.org/mandarin/yataibaodao/meiti/ql2-05212016120813.html

134 Anne Henochowicz, "Sensitive: PX Protests, Tigers, More," *China Digital Times*, April 2, 2014, http://bit.ly/1La8bAV.

135 Xiao, "From 'Grass-Mud Horse' to 'Citizen': A New Generation Emerges through China's Social Media Space."

Digital Activism

Social media platforms such as Weibo used to be a vibrant space for revealing government official wrongdoings and organize activism for different social causes. Whereas Chinese citizens traditionally trek to the seat of power to present their grievances, digital technologies can offer a way to overcome the geographic, financial, and physical challenges f such petitioning, and microblogs generated a strong sense of empowerment among many Chinese users.[136] Moreover low-level government wrongdoing, once exposed by users, has been punished, with officials f equently singled out for overspending on entertainment or designer watches, a sign of possible corruption.[137]

Against the background of stricter controls across all platforms and public punishments for outspoken internet users, however, activism has been gradually waning since 2013.[138] The word "netizen"—a translation of the Chinese *wangmin*, or citizen of the internet—conveys the legitimate sense of civic engagement associated with online exchanges, but the term was less common in China by mid-2015.[139]

Some collective action still takes place. In March 2016, human rights activists used the internet to organize demonstrations of support for workers in a Shuangya mountain coalmine in Heilongjiang, who were on strike for unpaid wages, though in mid-2016, the campaign had yet to achieve results.[140]

In April 2016, college student Wei Zexi died of a rare form of cancer after receiving questionable treatment from a hospital he found via a promoted search result in Baidu's search engine.[141] Following Wei's death, many Chinese internet users expressed disdain for Baidu's advertising business, referring to the company using a homophone for Baidu meaning "100 poisons." In response to the fury online, the CAC imposed new restrictions on the way search engines promote content in June 2016, outside the coverage period of this report. The regulations also prohibit search engines from providing links to banned content and require them to report websites carrying banned content when they learn of it.[142]

Violations of User Rights

A number of criminal laws and internet regulations ensnare users who post content deemed undesirable by the CCP. Authorities use antipornography and antirumor campaigns as a cover for suppressing politically sensitive material and voices, and charges typically used to silence offline dissent—subversion, separatism, and terrorism, as well as defamation and "creating a disturbance"—are regularly in-

136 David Barboza, "Despite Restrictions, Microblogs Catch On in China," *New York Times*, May 15, 2011, http://nyti.ms/1X1ri5y.

137 Laura Zhou, "Watch Imprint on Quake Official s Wrist Goes Viral on Internet," *South China Morning Post*, April 24, 2013, http://bit.ly/1ZBtOBT; Jonathan Kaiman, "Chinese Police Chief Suspended after Online Storm over Teenager's Detention," *Guardian,* September 24, 2013, http://bit.ly/1jxg7mB.

138 中國立法嚴格管控 部落客噤聲接受再教育 http://www.storm.mg/article/57176

139 How China stopped its bloggers Angus Grigg, http://www.afr.com/technology/social-media/how-china-stopped-its-bloggers-20150701-gi34za

140 维权人士发起联署声明支持双鸭山矿工, March 16, 2016, Radio Free Asia, http://www.rfa.org/mandarin/yataibaodao/renquanfazhi/yf1-03162016103722.html

141 China Investigates Baidu After Student's Death From Cancer, New York Times, http://www.nytimes.com/2016/05/04/world/asia/china-baidu-investigation-student-cancer.html;

142 Bloomberg News, "China Tightens Internet Rules for Baidu and Other Search Engines," June 25, 2016, https://www.bloomberg.com/news/articles/2016-06-25/china-tightens-internet-rules-for-baidu-and-other-search-engines.

voked to imprison citizens for their online activity. Netizens and activists have been detained in a series of crackdowns over the last several years that were aimed at curtailing protests and perceived threats to "social and public order." Those affected have included lawyers who utilized social media to advocate for civil society, well-known online commentators accused of spreading rumors online, and even engineers developing internet circumvention tools. A bolstered "real-name registration" system remains a threat to users' privacy and anonymity, and surveillance has increased in ethnic minority areas chafing under CCP rule. Websites, hosting services, and dissidents' email accounts are routinely attacked by hackers based in China.

Legal Environment

Article 35 of the Chinese constitution guarantees freedoms of speech, assembly, association, and publication, but such rights are subordinated to the CCP's status as the ruling power. In addition, the constitution cannot, in most cases, be invoked in courts as a legal basis for asserting rights. The judiciary is not independent and closely follows party directives, particularly in politically sensitive freedom of expression cases. China lacks specific p ess or internet laws, but government agencies issue regulations to establish censorship guidelines. Regulations—which can be highly secretive—are subject to constant change and cannot be challenged by the courts. Prosecutors exploit vague provisions in China's criminal code; laws governing printing and publications; subversion, separatism, and antiterrorism laws; and state secrets legislation to imprison citizens for online activity.

In 2013, the Supreme People's Court and the Supreme People's Procuratorate, the top prosecutorial body, issued a judicial interpretation entitled "Regarding the Interpretation of Various Laws Concerning the Handling of Cases of Using the Internet to Carry Out Defamation and Other Crimes," which formally defined online manifestations f crimes including defamation, creating disturbances, illegal commercial activities, and extortion.[143] Local officials had al eady detained online whistleblowers for criminal defamation, which carries a possible prison term of three years under "serious" circumstances.[144] But the new interpretation defined those ci cumstances to cover defamatory online content that receives more than 5,000 views or is reposted more than 500 times.[145] Online messages deemed to incite unrest or protest are also subject to criminal penalties under the interpretation.

The legal grounds for criminalizing digital activity were bolstered during the coverage period. Effective November 1, an amendment to the criminal law introduced criminal penalties up to seven years in prison for those who disseminate misinformation on social media.[146] Separately, in December 2015, an antiterrorism law increased pressure on private companies to provide the government with user data and introduced some content restrictions which could limit free expression (See Restrictions on Connectivity, Content Removal, and Surveillance, Privacy, and Anonymity).

In July 2015, the National People's Congress issued a draft cybersecurity law to consolidate the

143 Human Rights Watch, "China: Draconian Legal Interpretation Threatens Online Freedom," September 13, 2013, http://bit.ly/1ZBv0Ff; Megha Rajagopalan and Adam Rose, "China Crackdown on Online Rumors Seen as Ploy to Nail Critics," Reuters, September 18, 2013, http://reut.rs/1PeTbFX.

144 Justin Heifetz, "The 'Endless Narrative' of Criminal Defamation in China," Journalism and Media Studies Centre of the University of Hong Kong, May 10, 2011, http://coveringchina.org/2011/05/10/the-endless-narrative-of-criminal-defamation-in-china/.; Associated Press, "Chinese prosecutors decide not to charge journalists detained for online posts in 2013," *Star Tribune*, September 10, 2015, http://strib.mn/1ZBKiK6.

145 Human Rights Watch, "China: Draconian Legal Interpretation Threatens Online Freedom."

146 刑法修正案下月起正式实施 微信、微博造谣最高获刑七年, October 28, 2015, Xinhuanet, http://news.xinhuanet.com/legal/2015-10/28/c_1116970714.htm

role of the CAC, which it identified as the principle agency esponsible for implementing many of the law's provisions.[147] The draft codified existing estrictions, strengthening self-regulation and real-name registration requirements for internet companies and requiring them to assist security agencies with investigations; and permitting the government to shut down internet connections at times of public security emergencies, and implement censorship (see Content Removal).[148] Caixin's English-language news website commented that the law remains vague and gives government too much control of the internet.[149] A second draft was under consideration in June 2016 but had not been released to the public.[150]

Bloggers and activists occasionally use the law to defend their right to online expression. In December 2014, Liang Zhuqiang from Guangzhou province was detained on charge of inciting state subversion in relation to a QQ group discussing his family's misfortune during the Cultural Revolution. In June 2015, the People's Procuratorate in Guangzhou dismissed the case for lack of evidence. In December, Liang received RMB 41,090 (US$ 6,400) in state compensation for his wrongful detention.[151]

Prosecutions and Detentions for Online Activities

Reporters Without Borders documented a total of 84 netizens in Chinese jails as of September 2015.[152] As of December 2015, 49 journalists were jailed in China, 35 of them internet journalists, according to the Committee to Protect Journalists.[153]

Religious and ethnic minorities face particularly harsh treatment for online activity. In November 2015, Radio Free Asia reported that a Uyghur teenager sentenced to life imprisonment in Xinjiang had "simply watched videos on his cellphone," citing his father. He was detained with classmates at school in 2014, aged 17, for what the news report described as "internet access offences," and was unable to prove that he was a minor at the time of the trial, which may have contributed to the severity of his sentence.[154] At least one other Uyghur man was detained for watching videos on a cellphone; he was reported to have died in custody in June 2016.[155] In 2014, a court sentenced professor, writer, and Uyghur rights advocate Ilham Tohti to life imprisonment in relation to activities on a Uyghur community website he founded.[156] Separately, a court in Guangdong sentenced Liu Mouling

147 Drew Foerster, American Bar Association, "China's Legislature Gears Up to Pass a Sweepingly Vague Cybersecurity Law," May 2, 2016, http://www.americanbar.org/publications/blt/2016/05/02_foerster.html.

148 Gillian Wong, China to Get Tough on Cybersecurity, July 9 2015, The Wall Street Journal, http://www.wsj.com/articles/china-to-get-tough-on-cybersecurity-1436419416

149 Proposed Law Gives Gov't Too Much Control of Internet, Experts Say, July 30, 2015 Caixin Online, http://english.caixin.com/2015-07-30/100834587.html

150 "China moves closer to adopting controversial cybersecurity law," Reuters, June 27, 2016, http://www.reuters.com/article/us-china-cyber-lawmaking-idUSKCN0ZD1E4.

151 男子涉煽动颠覆国家政权被捕，检方因证据不足不起诉并赔偿, December 20, 2015, the Paper, http://www.thepaper.cn/newsDetail_forward_1411135_1

152 Other cases go unreported. Reporters Without Borders, "2015: Netizens Imprisoned," Press Freedom Barometer, accessed September 23, 2015, http://bit.ly/1GuFfjv.

153 2015 prison census: 199 journalists jailed worldwide, https://cpj.org/imprisoned/2015.php

154 Radio Free Asia, "Uyghur Teenager Serving Life Sentence Is Victim of China's Strike Hard Campaign: Father," November 16, 2015, http://www.rfa.org/english/news/uyghur/uyghur-teenager-serving-life-sentence-is-victim-of-chinas-strike-hard-campaign-11162015141753.html

155 Radio Free Asia, "Jailed for Watching Islamic Video, Uyghur Dies in Police Custody," June 13, 2016, http://www.rfa.org/english/news/uyghur/custody-06132016142251.html.

156 Tania Branigan, "China charges Uighur scholar Ilham Tohti with separatism," *Guardian,* July 30, 2014, http://bit.ly/1K7GmFv; Miao Deyu, "The Case against Ilham Tohti," *Guardian*, May 7, 2014, http://bit.ly/1NFIJXK; Damien Grammaticas, "China jails prominent Uighur academic Ilham Tohti for life," BBC, September 23, 2014, http://bbc.in/1uocWkg.

to 10 years in prison in September for activities in support of the banned Falun Gong spiritual group, which included accessing related websites.[157]

As in past years, police and prosecutors also targeted individuals who criticized the party or the leadership online. In one high profile example, human rights law er Pu Zhiqiang was given a suspended three-year prison sentence on December 22, 2015.[158] He was detained in Beijing on May 6, 2014, on suspicion of "picking quarrels" after he attended a May 3 seminar about the 25th anniversary of the Tiananmen Square crackdown., and later charged with creating a disturbance, inciting ethnic hatred, and separatism, based on 28 posts Pu made on Weibo between July 2012 and May 2014—the prosecution's only evidence.[159] Other cases involving criticism of the authorities were documented in 2015 and 2016:

- On June 30, 2015, Liang Qinhui from Guangzhou, who writes online under the name Jiandao, was charged for inciting subversion of the state in relation to a number of online articles criticizing the Communist Party.[160] Liang, who was fi st arrested on February 4, was sentenced to 18 months in prison on April 8, 2016.

- On April 6, 2016, Tianyou, a well-known online writer in Shenzhen, was detained for fi e days based on an article about China's fi st lady Pen Liyuan.[161] Tianyou, a former Sina Weibo user with several hundred thousand followers, had his account closed in 2014.

- On April 20, 2016, human rights defender Wang Jing from Jilin was sentenced to four years and ten months on charge of picking quarrels.[162] Wang is an independent journalist who writes articles for the overseas website *64Tianwang*.

In a more unusual development, Lefu Chen, a Shanghai network engineer, was detained for 28 days on charge of "destroying computer information systems" in June 2015.[163] Commentators said he had publicly promoted circumvention tools before his arrest.[164] Separately in April 2016, police held a Jinan resident in administrative detention for 15 days under the antiterrorism law after he used circumvention tools to download and view ISIS propaganda videos.[165]

Digital activism was also grounds for detention. Police in Inner Mongolia detained at least fi e herders for up to ten days each in March 2016 for inciting unrest on WeChat, according to the New York-based Southern Mongolian Human Rights Information Center.[166] More than 100 herders had gathered to protest mining activities they said polluted grazing lands.

157 被告人刘某玲犯利用邪教组织破坏法律实施罪一案一审刑事判决书, http://wenshu.court.gov.cn/content/content?DocID=6052790d-3882-4fec-a130-d262b38734b2

158 中國維權律師浦志強 判刑3年緩刑3年, http://news.ltn.com.tw/news/world/paper/942887

159 Chris Buckley, "Comments Used in Case Against Pu Zhiqiang Spread Online," *Sinosphere* (blog), *New York Times*, January 29, 2015, http://nyti.ms/1GGuHNN.

160 网络作家"尖刀""煽颠罪"移送法院, June 30, 2015, Radio Free Asia, http://www.rfa.org/mandarin/yataibaodao/renquanfazhi/ql1-06302015102048.html

161 曾批彭麗媛如武則天 深圳作家被拘, http://udn.com/news/story/7331/1618493

162 "保护记者委员会"谴责中国重判记者王晶入狱, http://www.rfa.org/mandarin/Xinwen/1-04262016110404.html

163 研究翻墙软件被刑拘 陈乐福取保候审获释June 30, 2015, Free Radio Asia, http://www.rfa.org/mandarin/Xinwen/7-06302015115424.html

164 http://twister.net.co/?p=515; https://twitter.com/wenyunchao/status/608037838131761153

165 中国首次动用"反恐法" 济南男子翻墙观看ISIS视频被拘, http://www.rfa.org/mandarin/yataibaodao/shaoshuminzu/xl3-04272016101815.html

166 SMHRIC, "Crackdown escalates, more herders arrested for "inciting illegal gatherings via the Internet," March 24, 2016, http://www.smhric.org/news_595.htm; 微信声援被抓牧民 5名内蒙古牧民亦被扣, http://chinaexaminer.bayvoice.net/gb/people/2016/03/25/227309.htm

Authorities reported "punishing" nearly 200 internet users for spreading rumors in connection with major news events in 2015.[167] At least some were detained. Examples during the coverage period include human rights activist Wang Jianyin, who in June 2015 was detained for ten days in Nanjing for posting his opinion on the Tiananmen Square crackdown.[168] Kong Xiangde, an internet user from Anhui Province, was detained for ten days for allegedly posting misinformation about the judge who tried the case of Bo Xilai, the Chongqing party chief purged in 2012.[169] On July 6, an internet user from Guangzhou posted alleged misinformation about an explosion at a local nuclear plant on Weibo. He was detained for fi e days.[170]

Long-term detainees include 2010 Nobel Peace Prize winner Liu Xiaobo, who is serving an 11-year sentence on charges of "inciting subversion of state power" for publishing online articles, including the prodemocracy manifesto Charter 08.[171]

In a more positive development in November 2015, the authorities reduced the seven year sentence of 70-year-old journalist Gao Yu, a contributor to the German news outlet Deutsche Welle, by two years and permitted her to serve the sentence at home.[172] Authorities detained Gao in April 2014 and tried her in November that year for leaking state secrets to a foreign website.

Though the people imprisoned represent a tiny percentage of the overall user population, their harsh sentences have a chilling effect on the close-knit activist and blogging community and encourage self-censorship in the broader public. Trials and hearings lack due process, often amounting to little more than sentencing announcements, and detainees frequently report abuse in custody, including torture and lack of medical attention.[173]

Chinese authorities abolished the extrajudicial sentence known as reeducation through labor in 2013 after domestic calls for reform.[174] However, individuals can be detained without trial under similarly poor conditions in drug rehabilitation and "legal education" centers.[175]

State agents also abduct and hold individuals in secret locations without informing their families or legal counsel. In 2012, the National People's Congress enacted an amendment of the Criminal Procedure Law that strengthened the legal basis for detaining suspects considered a threat to national security in undisclosed locations, among other changes. In response to public feedback, a clause was added requiring police to inform a suspect's family of such a detention, though they need not disclose where and why the suspect is being held. Despite this improvement, the amendment main-

167 China 'Punishes' Nearly 200 People for Spreading Rumors, August 31, 2015, the Wall Street Journal, http://blogs.wsj.com/chinarealtime/2015/08/31/china-punishes-nearly-200-people-for-spreading-rumors/

168 南京维权人士涉六四言论被捕 南宁异议人士六四绝食拘十日, June 5 2015, Radio Free Asia, http://www.rfa.org/mandarin/yataibaodao/renquanfazhi/ql1-06052015104649.html

169 安徽籍男子编造"薄熙来案一审审判长自杀"谣言，被行拘十日, June 11, the Paper, http://www.thepaper.cn/www/v3/jsp/newsDetail_forward_1340833

170 广州网民散布"大亚湾核电站爆炸"谣言被拘留5天, July 9, 2015, China News Net, http://www.chinanews.com/gn/2015/07-09/7395257.shtml

171 Sharon Hom, "Google and Internet Control in China: A Nexus between Human Rights and Trade?" (testimony, U.S. Congressional-Executive Commission on China, Washington, DC, March 24, 2010), http://1.usa.gov/1LKqeuV.

172 The Initium, November 24, 2015. https://theinitium.com/article/20151124-dailynews-Gaoyu/

173 Chinese Human Rights Defenders (CHRD), *We Can Beat You to Death With Impunity: Secret Detention & Abuse of Women in China's "Black Jails,"* October 21, 2014, http://bit.ly/1OAn0iN.

174 Xinhua, "Victims of Re-education Through Labor System Deserve Justice," *Global* Times, January 28, 2013, http://bit.ly/1NFKggC.

175 CHRD, *We Can Beat You to Death With Impunity: Secret Detention & Abuse of Women in China's "Black Jails"*; Amnesty International, "China's 'Re-education Through Labour' Camps: Replacing One System of Repression with Another?" December 17, 2013, http://bit.ly/1LtdZa4.

tained vague language that is open to abuse by police and security agents.[176] Dozens of human rights lawyers, including many representing clients in freedom of speech cases, disappeared or were held in undisclosed locations in 2015.[177]

Surveillance, Privacy, and Anonymity

In December 2015, China passed an antiterrorism law pending since November 2014.[178] The law contained no requirement for technology fi ms to provide the government with surveillance "back doors" and supply law enforcement agencies with encryption keys and user data, controversial specifications that ere included in a public draft.[179] The law also dropped the requirement that online service providers and telecommunication companies store their user data within China's borders,[180] though localization requirements may be implemented as part of the pending cybersecurity law.[181] In late 2015, the China Information Technology Security Evaluation Center requested U.S. technology companies pledge not to harm the national security of China, including storing data on Chinese users within China, in language similar to the antiterrorism law, but it is not clear if any did so.[182] The antiterrorism law did require companies to offer technical support to decrypt information at the request of law enforcement agencies. Regulations for the Administration of Commercial Encryption dating to 1999, and related rules from 2006, separately require a government regulator to approve encryption products used by foreign and domestic companies.[183]

Users hoping to avoid repercussions for their online activity face a dwindling space for anonymous communication as real-name registration requirements expand online, among mobile phone retailers, and at public internet facilities. The authorities justify real-name registration as a means to prevent cybercrime, though experts counter that uploaded identity documents are vulnerable to theft or misuse,[184] especially since some verification is done th ough a little-known, government-linked contractor.[185]

In 2012, the National People's Congress Standing Committee approved new rules to strengthen the

176 The amendment took effect on January 1, 2013. Observers praised other aspects of the measure, including tentative steps toward increasing police accountability for surveillance. Committee to Protect Journalists, "China's New Law Sanctions Covert Detentions," March 14, 2012, http://cpj.org/x/49d9.

177 Associated Press, "Lawyer kidnapped hours after release of Chinese journalist working for German weekly," *U.S. News*, July 10, 2015, http://bit.ly/1Gcm1DR.

178 http://www.nytimes.com/2015/12/28/world/asia/china-passes-antiterrorism-law-that-critics-fear-may-overreach.html

179 Erika Kinetz, "China plays down US concerns over anti-terror legislation," Associated Press, March 4, 2015, http://bit.ly/1jnhK6R.

180 反恐法对互联网企业的冲击有多大？December 29, 2015, http://www.globalview.cn/html/societies/info_8191.html

181 "China moves closer to adopting controversial cybersecurity law," Reuters, June 27, 2016, http://www.reuters.com/article/us-china-cyber-lawmaking-idUSKCN0ZD1E4.

182 Paul Mozur, 中国要求美国科技公司服从政府管控, September 17 2015, The New York Times, http://cn.nytimes.com/technology/20150917/c17pledge/; Netizen Report: China Joins Russia in Crusade to Keep User Data at Government's Fingertips, September 24 2015, Global Voices, https://globalvoices.org/2015/09/24/netizen-report-china-joins-russia-in-crusade-to-keep-user-data-at-governments-finge tips/

183 Adan Segal, "The Cyber Trade War," *Foreign Policy,* October 25, 2014, http://atfp.co/1Qq5LzN.

184 Danny O'Brien, "China's name registration will only aid cybercriminals," Committee to Protect Journalists blog, December 28, 2012, https://cpj.org/x/5177.

185 William Farris, "Guangzhou Daily Looks Into the Economics of the Weibo Real Name System," Google+, February 28, 2012, http://bit.ly/1Psal1W; *Guangzhou Daily*, "实名制数亿元市场仅两家瓜分 被指收费不透明," *News 163*, September 2, 2012, http://bit.ly/1VR4b0k; "Du Zi He Cha Wei Bo Shi Ming Guo Zheng Tong She Long Duan" [Real-Name Verification f Weibo Suspected Monopolized by Guo Zheng Tong], *Hong Kong Commercial Daily*, December 30, 2011, http://www.hkcd.com.hk/content/2011-12/30/content_2875001.htm.

legal basis for real-name registration by websites and service providers.[186] The rules threatened violators with "confiscation f illegal gains, license revocations, and website closures," largely echoing the informal arrangements already in place across the sector.[187] Comment sections of major news portals, bulletin boards, blog-hosting services, and email providers already enforced some registration.[188] The MIIT also requires website owners and internet content providers to submit photo identification when they apply for a license, whether the ebsite is personal or corporate.[189] Nevertheless, the 2012 rules extended regulation to the business sector who must gain users' consent to collect their personal electronic data, and outline the "use, method, and scope" of its collection. The rules offer no protection against law enforcement requests for these records.[190]

Microblog providers have struggled to enforce identity checks. Online reports of Sina Weibo users trading defunct identification numbe s to facilitate fake registration indicated that the requirements were easy to circumvent.[191] Sina's 2014 report to the U.S. Securities and Exchange Commission noted the company's exposure to potentially "severe punishment" by the Chinese government as a result of its noncompliance.[192] Implementation of the real-name policy also makes it harder for the state's hired commentators to operate undetected. One study reported officials encouraging commentators to use pseudonyms and fake documents to hide their affiliation with the p opaganda department.[193] In summer 2014, authorities issued interim rules for anyone "employing instant messaging tools as public information services," requiring service providers to verify user identities and register them with a government agency.[194] The government announced plans to begin enforcing real-name registration on all websites beginning on March 1, 2015. Alibaba, Tencent, Baidu, Sina Weibo, and other companies were reported to have deleted more than 60,000 accounts on various platforms because they did not conform to the new, stricter regulations.[195]

Internet commerce is undermining online anonymity. Many users voluntarily surrender personal details to enable financial transactions on social media si es. Mobile phone purchases have required identification since 2010, so p oviding a phone number is a common way of registering with other

186 "National People's Congress Standing Committee Decision Concerning Strengthening Network Information Protection," *China Copyright and Media* (blog), December 28, 2012, http://bit.ly/1RGoSqc.

187 Joe McDonald, "China Real-Name Registration Is Now Law in Country," *Huffington Post*, December 28, 2012, http://huff.to/1NFLFnw.

188 "Ministry of Culture Will Curb Trend of Internet Indecency in 2009" [in Mandarin], *Net Bar China*, January 6, 2009, http://bit.ly/1LKuY3H; Chen Jung Wang, "Real Name System Intimidates High School BBS," CNHubei, November 29, 2009, http://bit.ly/1OAp7CY; "Internet Society of China: Real Name System for Bloggers is Set," Xinhua, October 22, 2006, http://www.itlearner.com/article/3522.

189 Elinor Mills, "China seeks identity of Web site operators," *CNET News*, February 23, 2010, http://cnet.co/bXIMCp.

190 Tim Stratford et al., "China Enacts New Data Privacy Legislation," Covington & Burling LLP, January 11, 2013, http://bit.ly/RRiMaM.

191 C. Custer, "How to Post to Sina Weibo without Registering Your Real Name," *Tech in Asia*, March 30, 2012, http://bit.ly/1NFM0GP.

192 See Securities and Exchange Commission, "Form F-1 Registration Statement Under The Securities Act of 1933, Weibo Corporation."

193 Han, "Manufacturing Consent in Censored Cyberspace."

194 "China's Real Name Internet Part 5: 2013–2014," *Fei Chang Dao*.

195 Paul Carsten, "China censorship sweep deletes more than 60,000 Internet accounts," ed. Robert Birsel, Reuters, February 27, 2015, http://reut.rs/1AR2geU.

services.[196] One analyst estimated that 50 percent of microblog users had exposed their identific - tion numbers to providers by 2012, simply by accessing the platform from their mobile phone.[197]

Though not consistently enforced in the past, a crackdown on real-name registration for existing mobile subscriptions began in early 2015,[198] and was further tightened during the coverage period. Batches of unregistered mobile phone accounts were scheduled for closure starting in September 2015,[199] causing residents in Beijing to line up for registration in late August; about 40 percent of mobile phone users were not registered according to the real-name requirements.[200] Also in September, multiple virtual network operators in Fujian started to strengthen registration, requiring users to upload a photo showing their face and national identification ca d.[201]

China's "second generation" national ID cards—which are administered by police—are required to be digitally embedded with fingerprints; the first generation of cards became defunct in 2013.[202] The State Council aims to link credit, social security, and other personal information to these biometric databases. Writer Mo Zhixu laid out some possible implications, saying "ID numbers culled online will soon become useless for repeated use"; "relatives and friends will not … dare, to lend their ID numbers to anyone else"; and "personal credit information will necessarily include information about internet use."[203]

Chinese providers are required to retain user information for 60 days, and submit it to the authorities upon request without judicial oversight or notifying users.[204] In 2010, the National People's Congress amended the State Secrets Law,[205] obliging telecommunications operators and ISPs to cooperate with authorities investigating leaked state secrets or risk losing their licenses.[206] An amendment to the Criminal Procedure Law that took effect in 2013 introduced a review process for allowing police surveillance of suspects' electronic communications, which the Ministry of Public Security permits in many types of criminal investigation, but the wording of the amendment was vague about the procedure for the review.[207]

In January 2016, the deputy chief of the State Post Bureau announced that a mobile phone app will be developed this year to ensure real-name registration of express deliveries. Consumers will have to use the app to provide their mobile phone number and national ID number before sending out express mail. This signaled a wider trend that could undermine privacy. In June 2016, outside the

196 "Mobile phone real-name system implemented today, SIM card purchasers have to present their ID documents" [in Mandarin], *News 163*, October 1, 2010, http://bit.ly/aIyYL4.

197 Song Yanwang, "Internet Clean-Up Regulations Conceal Obscure Issues. Weibo's New Real-Name Registration Rule Poses Challenge for Telecom Operator" [in Mandarin], *Net China*, March 15, 2012, http://net.china.com.cn/txt/2012-03/15/content_4875947.htm.

198 "移动发狠招手机不实名将被停机 电信联通表示没听说过," May 20, 2015, http://bit.ly/1jnhXa1.

199 "史上最严"实名制要来：不实名按批次停机, August 27, 2015, http://news.mydrivers.com/1/444/444390.htm3

200 北京：9月起手机实名认证 补办登记排长队, August 30, 2015, CCTV.com, http://news.cntv.cn/2015/08/30/VIDE1440864239598471.shtml

201 福建省虚拟运营商实行实名认证 老用户也将进行认证, September 29 2015, http://www.mnw.cn/news/fj/995822.html?pooc

202 Cao Yin, "Efforts Stepped Up to Curb Fraudulent ID Card Use" [in Mandarin], *China Daily,* August 15, 2013, http://bit.ly/1G4jzzC; Zhou Dawei, "Do We Really Need to Fingerprint 1.3bn People?" *News China Magazine,* January 2012, http://bit.ly/1Qq5nBa.

203 Andy Yee, "How Social Commerce Tightens China's Grip on the Internet," Global Voices, May 22, 2013, http://bit.ly/1OvBcet.

204 OpenNet Initiative, "China," August 9, 2012, http://opennet.net/research/profiles/china-including-hong- ong.

205 Central People's Government of the People's Republic of China, "Presidential order of the People's Republic of China, No. 28" [in Mandarin], April 29, 2010, http://bit.ly/1LMMtXc.

206 Jonathan Ansfield, "China asses Tighter Information Law," *New York Times*, April 29, 2010, http://nyti.ms/1LMMx9j.

207 Luo Jieqi, "Cleaning Up China's Secret Police Sleuthing," *Caixin*, January 24, 2013, http://bit.ly/1LjK1BT.

coverage period of this report, CAC issued regulations requiring app providers from the mainland to adopt real-name registration for their users and keep user activity logs for 60 days. The regulation will take effect from August 1, 2016.[208]

Privacy protections under Chinese law are minimal. In the words of one expert, the law explicitly authorizes government access to privately held data, and "systematic access" to "data held by anyone" is a realistic possibility once e-government strategies are fully implemented.[209]

Real-name registration is just one aspect of the pervasive surveillance of internet and mobile phone communications in China. The DPI technology used for censorship can monitor users and personal text, and instant message exchanges have been cited in court documents. One academic study reported that when users entered blacklisted search terms on Baidu, their IP addresses were automatically sent to a location in Shanghai affilia ed with the Ministry of Public Security.[210] Cybercafes check photo identification and ecord user activities, and in some regions, surveillance cameras in cybercafes have reportedly transmitted images to the local police station.[211] Given the secrecy surrounding such capabilities, however, they are difficult o verify. During the coverage period the public security bureau in Lianyungang, Jiangsu Province developed a new mobile phone application for real-name registration in cybercafes. All 426 cybercafes in the city adopted the application, which was planned for use nationwide.[212]

As with censorship, surveillance disproportionately targets individuals and groups perceived as anti-government. In January 2015, the Xinjiang government issued a new regulation requiring real-name registration for Uyghurs attempting to purchase mobile phones, computers, and other electronic devices with storage, communication, and broadcast features. Stores selling such equipment were required to install software that provides police with real-time electronic records on transactions.[213]

Intimidation and Violence

Allegations of torture and extralegal harassment are widespread among Chinese detainees, particularly political prisoners, a category that encompasses the majority of freedom of expression cases. In May 2015, Human Rights Watch reported "physical and psychological torture during police interrogations, including being hung by the wrists, being beaten with police batons or other objects, and prolonged sleep deprivation" in a review of hundreds of ordinary criminal cases. "Political prisoners … have experienced much of what is described in this report and often worse," the report said.[214]

208 He Huifeng, Nectar Gan, All mainland app providers ordered to keep user logs for months to curb spread of 'illegal information', June 28, 2016, South China Morning Post, http://www.scmp.com/news/china/policies-politics/article/1982756/all-mainland-app-providers-ordered-keep-user-logs

209 Zhizheng Wang, "Systematic Government Access to Private-Sector Data in China," *International Data Privacy Law* 2, no. 4 (2012): 220–229, http://bit.ly/1Pf4jT8.

210 Becker Polverini and William M. Pottenger, "Using Clustering to Detect Chinese Censorware" (presentation, Eleventh Annual Workshop on Cyber Security and Information Intelligence Research, 2011), http://bit.ly/1Ra1XCx.

211 Naomi Klein, "China's All-Seeing Eye," NaomiKlein.org, May 14, 2008, http://bit.ly/2nf29.

212 江苏连云港警方首创网吧实名认证App, September 20, 2015, Xinhuanet, http://news.xinhuanet.com/politics/2015-09/20/c_128248099.htm

213 Bai Tiantian, "Xinjiang asks real-name registration for cellphones, PCs," *Global Times*, January 29, 2015, http://bit.ly/1NFNqRo.

214 Human Rights Watch, "Tiger Chairs and Cell Bosses: Political Torture of Criminal Suspects in China," May 13, 2015, https://www.hrw.org/report/2015/05/13/tiger-chairs-and-cell-bosses/police-torture-criminal-suspects-china.

During the coverage period, family members of online journalists and activists were subject to criminal investigations apparently launched in retaliation for digital activity. In August, 2015, two brothers of the Radio Free Asia journalist Shohret Hoshur, who is based in the U.S., were charged with endangering state security and leaking state secrets. Shohret Hoshur, who covers news affecting Uyghurs in Xinjiang, told the International Federation of Journalists that his brothers are not politically active and had been detained in relation to his work.[215] Separately, in March 2016, German-based journalist Chang Ping and New York-based digital rights activist Wen Yunchao reported family members had been detained in connection with their alleged roles commenting on, or distributing, an anonymous online letter calling for Xi Jinping's resignation.[216]

Internet users also risk being held under house arrest. In such cases, including the extralegal house arrest of poet Liu Xia (wife of Liu Xiaobo) since 2010, internet and mobile phone connections are often severed to prevent the individual from contacting supporters and journalists.[217] While there are several cases of long-term house arrest, the circumstances and degree of confinement can be adjusted arbitrarily over time. Dissident and human rights lawyer Gao Zhisheng, who published an online letter criticizing the jailing of activist Guo Feixiong in April 2015, stopped communicating with supporters in December 2015, indicating a possible escalation of his punishment.[218] Gao has been under house arrest since 2014. Some groups attempt to monitor the number of dissidents known to be held under house arrest, but there are no statistics showing how many were targeted specifically for online activity.[219]

Law enforcement officials f equently summon individuals for questioning in relation to online activity, an intimidation tactic referred to euphemistically as being "invited to tea."[220] In December 2015, human rights activist Xu Lin reported having been abducted by plain clothed security agents in Guangzhou for eight hours in relation to songs about defending human rights he had composed and distributed online.[221] In a separate case, Lifa Yao, an independent candidate for the local people's congress election in Hubei, was "invited to tea" with security agents so that he could not participate in online lectures on local elections he organized through QQ in August 2015.[222] Activists have also been instructed to travel during sensitive political events, effectively keeping them away from their normal online and offline activities.

University professors were subject to disciplinary proceedings in reprisal for online activity during the coverage period. In Guangdong, a professor in the English department was fi ed for posting

215 China's Great Media Wall: The fight for f eedom, International Federation of Journalists, http://www.ifj.trynisis.com/fileadmin/documents/I J_2016_English.pdf

216 Agence France-Presse, "Dissidents say China relatives released in letter probe," *Daily Mail,* March 30, 2016, http://www.dailymail.co.uk/wires/afp/article-3515212/China-dissidents-brother-denies-politics-arrest-media.html. Wen Yunchao contributed to the China chapter of the 2015 edition of *Freedom on the Net.*

217 PEN America, "Chinese Writers React to Crackdown," February 25, 2011, http://bit.ly/1OvBtOi.

218 Dissident Chinese Lawyer 'Incommunicado' After Online Anger Over Activist's Sentence, December 2, 2015, Radio Free Asia, http://www.rfa.org/english/news/china/china-gaozhisheng-12022015095428.html

219 CHRD, "Deprivation of Liberty and Torture/Other Mistreatment of Human Rights Defenders in China," June 30, 2013, http://bit.ly/1NFNC37.

220 China Blog Staff, "'Sorry, no comment - we might get invited to tea,'" *China Blog, BBC*, December 9, 2013, http://bbc.in/1LKxQ0k.

221 徐琳：12.17因《大撒币之歌》传唤记, December 26, 2015, http://www.boxun.com/news/gb/pubvp/2015/12/201512260204.shtml

222 大陆民间自发人大普选网路视屏研讨会遭遇国保干扰, http://chinaexaminer.bayvoice.net/gb/truth/2015/08/28/166158.htm

"improper" opinions on the internet in July 2015.[223] In October, Shaanxi university lecturer Feng Honglian, known online as Wumian, was informed by the university that her classes were terminated and she was not allowed to leave campus; she had mobilized internet users to demonstrate in front of local government building in March. State security agents told her not to speak out online in exchange for keeping her job.[224] Also in October 2015, a professor from Hunan University was not allowed to continue his class after he created a website promoting Chinese political reform.[225]

Technical Attacks

China is a global source of cyberattacks, accounting for 28 percent of the DDoS attack traffic o - served worldwide by Akamai in 2015.[226] The survey traced the attacks to computers in China using IP addresses, meaning the machines themselves may have been controlled from elsewhere. Symantec reported China was the world's largest originator of malicious bot activities (46 percent) in 2015.[227]

Attacks found to have originated in China can rarely be traced directly to the state, but the scale and targets of the illegal cyber activity have led many experts to conclude that Chinese military and intelligence agencies either sponsor or condone it. The geographically diverse array of political, economic, and military targets that suffer attacks reveal a pattern in which the hackers consistently align themselves with Chinese national goals. Hackers based in China were also suspected of carrying out major global cyberattacks during the coverage period, including one against the United States government Office f Personnel Management in which attackers stole the fingerprints f 5.6 million federal employees;[228] and one in December against the Australian Weather Bureau.[229] In October 2015, attacks targeted seven U.S. companies in the wake of the U.S.-China Cyber-Agreement, which Xi Jinping signed in September on a visit to the U.S.[230] Both countries promised not to conduct cyber-enabled theft in the agreement.[231]

Hackers, known in Chinese as *heike* (dark guests), employ various methods to interrupt or intercept online content. Both domestic and overseas groups that report on China's human rights abuses have suffered from distributed denial-of-service (DDoS) attacks, which temporarily disable websites by bombarding host servers with an unmanageable volume of traffic. In one 2015 example, the U.S.

223 编造政治谣言、发表言论过激博文，广东一英语系副主任被撤职, November 12 2012, the Paper, http://www.thepaper.cn/newsDetail_forward_1395720

224 西安著名网民"无眠"被学校停课 变相监控, October 1, 2015, Radio Free Asia, http://www.rfa.org/mandarin/Xinwen/5-10012015122455.html

225 湖南大学教授个人网站介绍"联邦制"被停课, October 16 2015, Radio Free Asia, http://www.rfa.org/mandarin/yataibaodao/renquanfazhi/ql2-10162015101124.html

226 Akamai, Akamai's state of the internet Q4 2015 report. https://www.stateoftheinternet.com/downloads/pdfs/2015-Q4-cloud-security-report.pdf

227 Symantec Internet Security Threat Report, https://www.symantec.com/security-center/threat-report

228 US government hack stole fingerprints f 5.6 million federal employees, September 23, 2015, the Guardian, https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprint

229 Robert Hackett, Chinese Hackers Infiltra ed Australian Weather Bureau Computers, Report Says, December 2m 2015, Fortune, http://fortune.com/2015/12/02/chinese-hack-australian-computers/

230 美国网络安全公司称，有中国政府背景黑客继续攻击7家美国企业, October 19 2015, Radio Free Asia, http://www.rfa.org/mandarin/yataibaodao/meiti/hc-10192015120641.html; https://www.crowdstrike.com/blog/the-latest-on-chinese-affilia ed-intrusions-into-commercial-companies/

231 Adam Segal, The Top Five Cyber Policy Developments of 2015: United States-China Cyber Agreement, Council on Foreign Relations, January 4, 2016, http://blogs.cfr.org/cyber/2016/01/04/top-5-us-china-cyber-agreement/

based website *64Tianwang* suffered repeated cyberattacks throughout the year.[232] It reports on corruption and human rights abuses in China.

In March 2015, the hosting service GitHub faced a DDoS attack that crippled its services. Sources indicate that the assault originated in China.[233] The monitoring organization Citizen Lab analyzed the incident and found that "while the attack infrastructure is co-located with the Great Firewall, the attack was carried out by a separate offensive system, with different capabilities and design, that we term the 'Great Cannon.' The Great Cannon is not simply an extension of the Great Firewall, but a distinct attack tool that hijacks traffic o (or presumably from) individual IP addresses, and can *arbitrarily replace unencrypted content as a man-in-the-middle*."[234]

Yahoo faced a MITM attack during the 2014 Hong Kong protests,[235] and Microsoft Outlook faced one in January 2015.[236] In April 2015, Google and Mozilla both announced that they would revoke authority of root certifica es belonging to the CNNIC,[237] meaning that sites with those certifica es would not be recognized by the browsers, potentially interrupting users' connections to a range of sites, including banks and e-commerce platforms.[238]

Another well-documented tactic is spear-phishing, in which customized email messages are used to trick recipients into downloading malicious software by clicking on a link or a seemingly legitimate attachment.[239] Tibetans, Uyghurs, and others subject to monitoring are frequently targeted with emailed programs that install spyware on the user's device.[240] In December 2015, Reuters reported that attacks attributed to Chinese authorities had targeted Hotmail accounts operated by overseas Tibetans, Uyghurs, and others using phishing software in the past; Microsoft, which owns Hotmail, will inform victims of suspected government hacking attempts going forward, the report said.[241]

232 六四天网、中国舆论监督网再遭攻击, August 18 2015, Radio Free Asia, http://www.rfa.org/mandarin/yataibaodao/meiti/ql2-08182015102821.html

233 Sebastian Anthony, "GitHub battles 'largest DDoS' in site's history," *ArsTechnica*, March 30, 2015, http://bit.ly/19AxkWX.

234 Bill Marczak et al., "China's Great Cannon," Citizen Lab, April 10, 2015, https://citizenlab.org/2015/04/chinas-great-cannon/.

235 Netresec, "Verifying Chinese MITM of Yahoo," *Netresec* (blog), October 1, 2014, http://bit.ly/1k3GUYg.

236 Michael Kan, "Microsoft's Outlook.com faces brief man-in-the-middle attack in China," *PC World*, January 19, 2015, http://bit.ly/1Pse8fT.

237 Lucian Constantin, "Like Google, Mozilla set to punish Chinese agency for certifica e debacle," *PC World,* April 2, 2015, http://bit.ly/1jxt7IX.

238 Dan Goodin, "Google Chrome will banish Chinese certifica e authority for breach of trust," *ArsTechnica*, April 1, 2015, http://bit.ly/1Hlskkq.

239 Dennis Fisher, "Apple Phishing Scams on the Rise," *Threat Post*, June 24, 2013, http://bit.ly/1OvBTV2.

240 Dylan Neild, Morgan Marquis-Boire, and Nart Villeneuve, "Permission to Spy: An Analysis of Android Malware Targeting Tibetans," research brief, Citizen Lab, April 2013, http://bit.ly/1OvBOAO.

241 Joseph Menn, "Microsoft failed to warn victims of Chinese email hack: former employees," Reuters, December 31, 2015, http://www.reuters.com/article/us-microsoft-china-insight-idUSKBN0UE01Z20151231

Freedom House

Colombia

	2015	2016
Internet Freedom Status	Partly Free	Partly Free
Obstacles to Access (0-25)	8	8
Limits on Content (0-35)	8	8
Violations of User Rights (0-40)	16	16
TOTAL* (0-100)	32	32

* 0=most free, 100=least free

Population:	**44.3 million**
Internet Penetration 2015 (ITU):	**56 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2016 Status:	**Partly Free**

Key Developments: June 2015 – May 2016

- In March 2016, a website critical of the student loans system was taken down by the hosting provider, after the government entity in charge of student loans filed a complaint for trademark infringement. Civil society organizations demanded that the entity cease abusing the complaints system to take the website down (see **Content Removal**).
- The director of the government's child protection entity filed a writ for the p otection of constitutional rights requesting a journalist to remove several critical tweets, and for Twitter to delete the journalist's account. Attracting widespread backlash on social media, the petition was withdrawn (see **Content Removal**).
- Illegal and excessive surveillance by certain sectors of the government and military continued to raise concerns. In December 2015, anonymous informants warned that investigative journalists had their communications intercepted illegally in retaliation for a news story on a possible prostitution network tied to the national police (see **Surveillance, Privacy, and Anonymity**).

Introduction

Colombia's internet freedom climate over the last year has been marked by persisting concerns over excessive and illegal surveillance, paired with criminal penalties for defamation and minor copyright violations.

Despite steady improvements over the last fi e years, challenges such as poor infrastructure, low digital literacy, and high costs still hamper widespread access to the internet in Colombia. Issues surrounding net neutrality have also emerged at the forefront of debate in Colombia, prompted by the expansion of zero-rating programs. When users manage to overcome access and affordability issues, however, they are able to view and disseminate content relatively freely.

Although there are occasional cases of content removal, takedowns are isolated rather than systematic and mostly stem from muddy legislation rather than onerous governmental policies. In a recent case, the official entity in cha ge of student loans exploited the trademark infringement notice mechanism made available by the registrar and hosting provider in order to take down a Colombian website that publicly denounced what its authors perceived as an abusive student loans system. On the other hand, while courts have ruled that search engines should not be held liable for links in their search results, a May 2015 ruling could place more burden on media to update articles online regarding the status of individuals in criminal investigations.

While prosecutions for dissemination of content online are still rare, harsh penalties for minor copyright violations and criminal penalties for defamation constitute serious violations of users' rights. This is the case of Diego Gómez, a biology student who could face four to eight years in prison and substantial fines a ter sharing a thesis of another person on Scribd, even though he did not claim any profit or attribution.

Additional challenges to users' rights come in the form of violence and impunity. For the past fi e decades, the Colombian government, various paramilitary groups, and guerrilla groups have been engaged in armed conflict. Despi e peace talks between the government and the FARC since 2012, high levels of insecurity persist. At least sixteen journalists have been murdered and many more have been threatened since 2005, with little response from the judiciary. Self-censorship both online and offline has become a p ophylactic measure against such threats, particularly in rural areas where violence and impunity are more pervasive than in cities.

Illegal surveillance continues to be an issue, as journalists have been followed both online and offline because f their work exposing corruption and irregularities at the core of institutions such as the National Police. Further reducing any chance of this situation changing, the legal commission for oversight of intelligence activities has not been able to fulfill its duties because f bureaucratic obstacles. In recent years, Colombian nongovernmental organizations—namely the Foundation for Freedom of the Press in Colombia (FLIP), Fundación Karisma, Dejustica, Colnodo, and, lately, the Colombian Jurists Commission (CCJ)—have made calls for more information regarding the scope of government surveillance and threats to users' privacy, issues that will likely gain greater traction in Colombia as internet usage increases.

Obstacles to Access

Although internet penetration has steadily increased, Colombia still faces obstacles to access primarily stemming from socioeconomic factors. The lack of basic utilities and affordable internet access constitutes an informal barrier to information and communications technologies (ICTs). The implementation of zero-rating programs such as Facebook's Free Basics will increase access to a selection of online platforms, but critics worry that it may weaken the application of the net neutrality principle and potentially determine or limit users' experience of the internet.

Availability and Ease of Access

Internet access has increased steadily in Colombia over the past decade. According to the most recent figu es from the International Telecommunication Union (ITU), Colombia's internet penetration rate reached 56 percent by the end of 2015, compared to 53 percent in 2014 and 30 percent in 2009.[1] Nevertheless, with nearly half of the population still without internet, significant obstacles o access remain. Lack of infrastructure in rural areas, low levels of digital literacy, and high prices all stand in the way of widespread access.

Internet access is facilitated primarily by DSL and cable connections.[2] Colombia's average internet connection speed is 4.5 Mbps—a figu e that places it between Peru and Ecuador, and in the same level as Argentina, in a regional comparison.[3] Many Colombian users access the internet outside of their homes, and cybercafes and education centers play a key role in expanding access. Almost 18 percent of internet users accessed the internet through cybercafes and 25 percent through education centers, while free public access points served a negligible percentage of internet users.[4]

Colombia's mobile penetration rate reached 116 percent at the end of 2015, and mobile phones are increasingly used to access the internet.[5] Mobile connections range from basic data plans to full access,[6] but it is not clear if official mobile in ernet penetration figu es count zero-rated data plans as mobile internet connections.

There is significant geographical dis arity in internet penetration rates in Colombia. While the capital, Bogotá, has a fi ed-internet subscription rate of 20 percent, the southern rural departments of Amazonas, Vaupés, Vichada, Guainía, and Guaviare range between 0.2 and 0.7 percent.[7] Only 0.7 percent of Colombia's population lives in this region; however, the land accounts for approximately 55 percent of the country's geographical area.[8] Although many indigenous languages are spoken in Colombia, there do not appear to be significant effo ts to offer online content in these languages. Even the official ebsites of Amazonas, Vichada, and Guajira—each of which lays claim to a large indigenous population—are in Spanish, with no option to display them in any of the indigenous languages

1 International Telecommunication Union (ITU), "Percentage of Individuals Using the Internet 2000-2015," accessed September 7, 2016, http://bit.ly/1LOr3mK.

2 Ministry of ICT, ICT Quarterly Bulletin, Q1 2016, accessed September 7, 2016, http://bit.ly/2bbfb6D.

3 For comparison, Argentina had an average internet speed of 4.7 and Ecuador had an average speed of 4.4 at the end of fourth quarter of 2015. The global average speed was 5.6 Mbps. Akamai, State of the Internet, Q4 2015 Report, accessed September 7, 2016, http://akamai.me/1UthiDG.

4 DANE, Basic Indicators in ICT in Colombia 2015, April 7, 2016, http://bit.ly/1VBwOxH.

5 International Telecommunication Union, "Mobile-cellular subscriptions 2000-2015," http://bit.ly/1LOr3mK.

6 Ministry of ICT, ICT Quarterly Bulletin, Q1 2016, accessed September 7, 2016, http://bit.ly/2bbfb6D.

7 Ministry of ICT, ICT Quarterly Bulletin, Q1 2016, accessed September 7, 2016, http://bit.ly/2bbfb6D.

8 DANE population projection for 2016 and the geographic area of the departments.

present in those territories although they offer the display option for English, French, or Italian.[9]

High internet prices and low levels of digital literacy also present substantial obstacles to internet access in Colombia. A 2015 Digital Consumers Survey revealed that 45 percent of people without internet in their homes cite high prices as the reason why they do not acquire the service, while 32 percent state that they do not think the internet is necessary.[10] The ITU's scale of fi ed-broadband prices lists Colombia as the 76th most affordable country out of 181 countries, placing it around the global median, with an average price of US$18.48 per month.[11] For comparison, Colombia's minimum legal monthly wage was set as COP 689.455 (US$206.5) in 2016.[12] However, the latest report of the Affordability Drivers Index (ADI), which measures the conditions that determine the likelihood that broadband prices will be reduced, ranked Colombia in fi st place.[13]

The ICT ministry claims that internet access has increased by 16 percent since 2010 thanks to official programs such as Vive Digital, with more than two million tablets and laptops delivered to public schools all around Colombia.[14] Administered by the ICT ministry, Vive Digital aims to expand infrastructure, services, internet applications, and the number of Colombian internet users.[15] Colombia Aprende, the Education Ministry's platform for the promotion of literacy launched in 2004, also aims to expand the use of digital applications and devices, training some 16,000 teachers of digital literacy across the nation.[16] However, the delivery of tablets has received some criticism for not properly training teachers on how to handle them.[17]

Colombia signed the Marrakech VIP Treaty in 2013 but its ratification is still pending [18] This has delayed reforms to current laws that seek to promote access to published works for people who are blind, visually impaired or print disabled.[19]

Restrictions on Connectivity

No legal provisions impose connectivity restrictions in Colombia. The government does not place limits on bandwidth, nor does it impose control over infrastructure, except in emergency situations when internet service providers (ISPs) are required to make their infrastructure available for official response.[20] In keeping with this lack of restriction, the government has not centralized telecommunications infrastructure, nor has it established tools to fil er or block social media applications or communications apps.

9 Official ebsite of the Department of Amazonas, accessed February 19, 2016, http://bit.ly/1JtV75d; Official ebsite of the Department of Vichada, accessed February 19, 2016, http://bit.ly/1KzLbeu; Official ebsite of the Department of La Guajira, accessed February 19, 2016, http://bit.ly/O9WQZ8.

10 DANE, Basic Indicators in ICT in Colombia 2015, April 7, 2016, pg. 6, http://bit.ly/1VBwOxH.

11 ITU, Measuring the Information Society Report 2015, 31, http://bit.ly/1oGaDJs.

12 Decree 2552, December 30, 2015, http://bit.ly/1oGaDJs.

13 Alliance for Affordable Internet, The 2015-16 Affordability Report, accessed September 7, 2016, http://bit.ly/1XRxJbE.

14 "El Gobierno Cumple lo que Promete El plan Vive Digital es una Realidad," [The government fulfills what it p omises – the plan Vive Digital is a reality], MinTIC Colombia, accessed September 7, 2016, http://bit.ly/1Ty5kXw. The figu es shown by the government on this website have no studies or evidence to support them.

15 ICT Ministry, "Vive Digital," accessed September 7, 2016, http://bit.ly/1lbnQBQ.

16 Education Ministry, "Crea-TIC," accessed September 7, 2016, http://bit.ly/2e3XWVu.

17 "Reto para profesores públicos: aprender a usar las Tabletas para educar," *Publimetro*, February 20, 2015, http://bit.ly/1oONtAE.

18 WIPO, Marrakesh Treaty to Facilitate Access to Published Works for Persons Who Are Blind, Visually Impaired or Otherwise Print Disabled. List of contracting parties. http://bit.ly/1gusI6x.

19 Law 1680 of 2013, http://bit.ly/21zwaBa.

20 Law 1341, Art. 8, July 30, 2009, http://bit.ly/1WQQuL7.

Colombia only has one internet exchange point (IXP), called "NAP Colombia" (operating since 1999), through which ISPs exchange traffic o improve efficiency and speed. Loca ed in Bogotá, the IXP is managed by the Colombian Chamber for Informatics and Telecommunications.[21] Eighteen telecommunication enterprises have a direct connection with the IXP, most of which are privately owned.

ICT Market

Colombia is home to 56 ISPs, and while 87 percent of the market is concentrated in the hands of four companies, there are nonetheless multiple market options from which to choose.[22] Market entry is straightforward, and it is possible for anyone to establish an ISP by following the general requirements of the ICT Law, which establishes free competition and prioritizes efficient use f infrastructure and access to ICTs.[23]

Registration requirements are neither excessive nor onerous. Business owners must provide personal and tax identification as ell as a description of services, but no fee is required. This information is published in an open registry, and the ICT ministry then has 10 days to verify the data, after which the business may begin operating. Based on the required criteria, registration can be denied when information is incomplete or false, or when an ISP does not have the proper commercial status to offer such services.[24] Service providers are obligated to pay a contribution of 0.01 percent of their annual income to an ICT Ministry Fund (Fontic) devoted to the development of nationwide ICT projects.[25] ISPs must also apply for licenses to utilize the radioelectric spectrum, although there have been no complaints of difficulties or bias with this p ocess.

The mobile landscape is more concentrated than the ISP market. Although there are nine providers, more than 70 percent of the market is in the hands of two companies, Claro and Movistar, which also dominate the mobile internet market.[26] In 2013 the Superintendency of Industry and Commerce sanctioned Claro for abusing its dominant position. As a result, the company was sentenced to pay a fine estima ed at COP 87,000 million (approximately US$ 26 million).[27] As with ISPs, mobile service providers must also contribute 0.01 percent of their annual income to Fontic.

The ICT ministry establishes public selection mechanisms for mobile service providers.[28] A 2013 spectrum auction resulted in two new players entering the market. While this is a step in the right direction, diminished market concentration has not yet been seen.[29] In March 2013, the ministry renewed the spectrum licenses of Claro and Movistar for a new 10-year term without major alterations, suggesting that little is likely to change in terms of market dominance in the next decade.[30]

21 NAP Colombia, "FAQ," http://bit.ly/24ul175.

22 Telmex Colombia S.A., UNE EPM Telecomunicaciones S.A., Colombia Telecomunicaciones S.A., and Empresa de Telecomunicaciones de Bogotá, Colombia S.A. are the four dominant providers. Ministry of ICT, ICT Quarterly Bulletin, Q1 2016, accessed September 7, 2016, http://bit.ly/2bbfb6D.

23 Law 1341 of 2009, http://bit.ly/1WQQuL7.

24 Decree 4948, December 18, 2009, http://bit.ly/1gVegGu.

25 Law 1341 of 2009, http://bit.ly/1WQQuL7.

26 Ministry of ICT, ICT Quarterly Bulletin, Q1 2016, accessed September 7, 2016, http://bit.ly/2bbfb6D.

27 Administrative decisions 53403 and 66934, 2013, http://bit.ly/1S8qTOy.

28 Law 1341 of 2009, Art. 11, http://bit.ly/1Qb3RnE.

29 Ministry of ICT, ICT Quarterly Bulletin, Q1 2016, accessed September 7, 2016, http://bit.ly/2bbfb6D.

30 Resolution 597, 2014, ICT Ministry.

Regulatory Bodies

Colombia's ICT sector is subject to numerous regulatory bodies with varying but limited degrees of independence from the government. The three main regulatory bodies are the ICT ministry, the Communication Regulation Commission (CRC), and the National Spectrum Agency (NSA). The Superintendency of Industry and Commerce also has some control duties as part of its consumer protection obligations.

The president appoints the ICT minister, who oversees the telecommunications sector through the ICT ministry. The ICT minister also chairs the CRC, which is responsible for ensuring efficient service and promoting competition in the telecommunications sector and is formed by the minister and three commissioners who are also appointed by the president. The ICT minister designates the head of the NSA, which is the agency in charge of planning, management and supervision of the use of the radioelectric spectrum. While some have suggested that such an executive-driven design prevents objective oversight of the sector, affording the president a great deal of influence in its operation, to date, there are no clear examples of executive bias in rulings.[31]

A 2014 report by the Organisation for Economic Co-operation and Development (OECD) recommended that the CRC develop more independence from Colombia's central government, as the board cannot deliberate without the presence of the ICT minister, and the ministry of finance fixes the agency's budget. In line with this recommendation, the prohibition to the CRC to session without a ministry representative was recently eliminated.[32] The OECD also advised the ICT ministry to refrain from regulating the sector, and focus solely on promoting the development and use of ICTs.[33]

Since 2010, a government-appointed concessionaire has been responsible for allocating the .co domain. For the domains org.co, edu.co, mil.co, and gov.co, applicants must comply with specific requirements; for edu.co, for example, the applicant must be an educational institution.[34]

Limits on Content

While no content is systematically blocked under Colombian law besides child pornography, the presence of guerrilla groups online has been subject to different forms of restriction over the past years. In February 2016, Twitter decided to suspend the Twitter account of the National Liberation Army (ELN) after it called for an "armed strike." Censorship of FARC websites does not appear to be systematic, and FARC members have functional social media accounts. Over the past few years, several court cases have exempted intermediaries from liability for content posted by third parties. After becoming the first South American country to launch Facebook's Free Basics in January 2015, net neutrality continues to generate debate among Colombian digital rights activists.

31 Carlos Cortés, "Mobile Internet in Colombia - Challenges and Opportunities for Civil Society: The 2013 Spectrum Auction," Open Society Foundation, December 13, 2015, http://bit.ly/1QDvnJ1.

32 Law 1753, Art. 207, http://bit.ly/1sbO3tQ.

33 OECD, Review of Telecommunications Policy and Regulation in Colombia, April 2014, http://bit.ly/1MOiNZP.

34 Dominio, "Historia del Dominio Co," [History of the Domain .Co], Cointernet, http://bit.ly/1iQywea.

Blocking and Filtering

Blocking or fil ering of political, religious, or social content is not common in Colombia.[35] YouTube, Facebook, Twitter and international blog-hosting services are freely available.

Although there are no legal restrictions on publishing materials about the decade old conflict b - tween the government, the FARC guerrilla group, and other paramilitary and guerrilla groups, there have been reports of censorship of content disseminated by the FARC in recent years.[36] Content on FARC's online accounts often consists of political or organizational propaganda rather than active recruitment or direct incitement to violence, which is illegal under international law. Despite instances such as the shutdown of FARC's website during the initiation of peace talks with the Colombian government in 2012,37 censorship does not appear to be systematic, and FARC members have functional social media accounts. Media coverage about censorship of FARC websites is scarce and the government has not commented on shutdowns of FARC websites or social media pages; therefore, it is not clear whether shutdowns of FARC websites were caused by technical blockings, cyberattacks, or decisions made by the organization itself, which operates in secrecy.

According to the ICT Ministry, the only content that is subject to blocking measures is child pornography, which is illegal under international law.[38] Decree 1524 (2002) requires ISPs to undertake technical measures to prevent the online availability of child pornography.39 In response to an information request, the ICT ministry stated that the criteria used to determine which content should be blocked are set every two years by a commission that includes the Colombian Child Care Office (ICBF), the Ombudsman, the National Prosecutor, and UNICEF. The Cybernetic Police Center of the Office for Criminal In estigation and the National Police's Directorate of Criminal Investigation and Intelligence (DIJIN) evaluate requests to block content and, if the content qualifies, send the URLs o the ICT ministry, which in turn notifies the ISPs who ultima ely block access to the sites. Individuals who feel adversely affected by the blocking measure may submit a complaint before DIJIN, which studies the case and decides to maintain or remove the blocking. Although it is an important protection mechanism, the legal basis of the blocking procedure and the appeal process is murky at best, since neither of the laws restricting child pornography (Law 679 and Decree 1524) specify the process outlined by the ICT ministry. The possibility for civil or judicial oversight is limited because information about which websites are blocked is classified, possibly out f fear that individuals would use circumvention tools to access child pornography sites if a list were made public.[40] The scope of issues upon which the police and other institutions exert control in order to protect minors are very broad and range from sexual abuse to "inappropriate content", and "other issues."[41] In July 2015, some profiles on the social net ork Ask.FM, popular amongst young people, were taken down because they were being used to incite children to harm themselves.[42] It is not clear, however, if the police asked

35 Communication from ICT Ministry in response to Request of Information Nº 661596, February 24, 2015.

36 "Tentáculos de las FARC en Internet," [FARC's tentacles on Internet], *El Espectador*, May 10, 2012, http://bit.ly/1jiDekV.

37 "Jefe máximo de las FARC dice que van a La Habana sin rencores," [FARC's top leader says they go to Havana without resentment], *El Universal,* September 3, 2012, http://bit.ly/1JiYLn9; See also "Colombia: Guerrilla Group's Peace Negotiation Rap Video," *Global Voices,* September 3, 2012, http://bit.ly/1QXlcz7.

38 Communication from ICT Ministry in response to Request of Information Nº 661596, February 24, 2015.

39 Law 679 of 2001, http://bit.ly/1RanTw8 ; Decree 1524, July 24, 2002, http://bit.ly/1NRSVKZ.

40 Communication 5245, ICT Ministry to Foundation for Press Freedom; See also: Law 679, Decree 1524, July 24, 2002, http://bit.ly/1NRSVKZ.

41 "Te Protejo" website, http://bit.ly/1n56U6s.

42 "Ask.FM, la red que obsesiona a los adolescentes, cierra en Colombia," [Ask.FM, the network that obsesses teenagers, closes in Colombia], *W Radio,* July 23, 2015, http://bit.ly/1Rardr5.

the social network to remove the profiles or if they the accounts ere blocked in line with the legal procedure outlined above.

Since the arrival of Uber, the government has been trying to regulate the service with little success. In May 2016, after the release of yet another order by the ministry of transportation regarding the matter, traditional cab drivers and owners demanded the blocking of the Uber app. Invoking the net neutrality principle, the ICT ministry stated that there are no legal grounds for such blocking and that the app itself is not illegal.[43]

Content Removal

The Colombian government does not regularly order the removal of content, although periodic court cases have resulted in judicial orders requiring the removal of specific info mation deemed to violate fundamental rights. During this period however, a critical site was repeatedly targeted by a government entity for trademark infringement. In March 2016, the website icetextearruina.com was taken down twice by hosting provider GoDaddy on grounds of trademark infringement. The complaint was presented by ICETEX, an official entity in cha ge of student loans. The website is owned by the Association of Users of Student Loans (ACUPE), a legally recognized organization created by a small group of citizens set to denounce what they perceive as an abusive system of student loans. Civil society organizations have denounced ICETEX for engaging in censorship, and demanded that the entity cease abusing the complaints system to take the website down.[44]

In another case in January 2016, the director of the Colombian Institute of Family Welfare (ICBF), a government entity, filed a petition for a writ f protection of fundamental rights (*acción de tutela*) against a journalist, requesting him to remove several posts on Twitter, where she was accused of being negligent and corrupt. The director also asked Twitter to delete the journalist's account.[45] However, the petition had to be withdrawn because it did not fulfill legal equirements.[46] The complaint was criticized on social media as disproportionate.[47]

Meanwhile in February 2016, former mayor of Bogotá Gustavo Petro publicly denounced that more than 200 videos recorded during his administration were no longer available through the official YouTube account for the Mayor's Office, which acco ding to Petro, was motivated by political interests of the recently elected mayor. Civil society organizations expressed concerns about its negative impact on the right to access public information.[48] The new administration alleged that YouTube sent

43 "Por qué el Mintic no puede bloquear Uber" [Why the ICT Ministry cannot block Uber], *El Espectador*, June 28, 2016, http://bit.ly/2aeM5DE.

44 "Bloqueo de página web por solicitud del ICETEX es una forma de censura" [Website blocking as per ICETEX demand is a form of censorship], Joint statement by Fundación Karisma and Fundación para la Libertad de Prensa, March 23, 2016, http://bit.ly/22Z1YQR.

45 "Sigue Polémica por Tutela de Cristina Plazas Contra Gonzalo Guillen," [Controversy continues over petition by Cristina Plazas against Gonzalo Guillen], *El Universal*, January 23, 2016. http://bit.ly/1QCP08V.

46 "Cristina Plazas retiró tutela en contra de Gonzalo Guillen," [Cristina Plazas withdraws petition against Gonzalo Guillen], *El Espectador*, January 26, 2016, http://bit.ly/1nOJIKE.

47 "Espaldarazo de la FLIP a Gonzalo Guillen en su Pleito con Cristina Plazas," [Gonzalo Guillen backed by Flip in his dispute with Cristina Plazas], *Las Dos Orillas,* January 22, 2016, http://bit.ly/1TEWrwG.

48 "Actuaciones dudosas por parte de la Alcadía de Bogotá y Canal Capital en YouTube," [Dubious decisions taken by Bogotá Mayor's office and Canal Capital], *Fundación para la Libertad de Prensa*, February 29, 2016, http://bit.ly/2a1wxQv.

a copyright violation notice and that all the videos were hidden to prevent sanctions on the platform.[49]

Some unconfi med reports suggest that content produced by the FARC guerrilla group has been subject to removal or restriction in the past.[50] On February 13, 2016, Twitter decided to directly suspend two accounts belonging to the leftist guerrilla movement ELN. The decision came after the ELN called for an "armed strike" via Twitter. The social network argued that this decision followed its global policy prohibiting threats of violence, and explained that, in contrast, FARC accounts were not suspended because their profiles did not p omote acts of violence.[51]

Several court cases pertaining to content disputes have exempted search engines from liability for posting links to content in their search results.[52] In May 2015, a court ruling strengthened the precedent that search engines should not be held liable for links in their search results.53 The dispute involved a citizen requesting online newspaper *El Tiempo* and Google to "erase any negative information" regarding her involvement in a human trafficking in estigation in 2000, a crime for which she had been prosecuted but never convicted. The Court ruled that *El Tiempo* must update the original note about the case and must use "robots.txt" and "metatags" to make the information harder to find in an online sea ch, but did not order Google to de-index the information from its search results. Reception to the ruling was mixed among free speech and digital rights advocates. Although many praised the fact that it exempted intermediaries from liability,[54] some worried that the ruling might place an excessive burden on the media.[55]

Media, Diversity, and Content Manipulation

Colombia has a vibrant media environment with a number of digital media outlets and online spaces for political debate. Many professional media enterprises thrive in Colombia's largest cities and, in general, the government does not interfere with operations. Authorities do not issue official guid - lines or directives to online media outlets or blogs, nor does the government employ or encourage individuals to defend official actions in online forums. F ee or low-cost blogging services are available and are very popular. Along with Google, Facebook, YouTube, Yahoo, and Twitter, the Alexa ranking features BlogSpot and WordPress among the top 20 websites in Colombia.[56]

Nevertheless, self-censorship is a notable problem for journalists in the realm of traditional me-

49 "Petro, Peñalosa y el choque por ocultar videos en Youtube" [Petro, Peñalosa and the conflict that follo ed the concealment of YouTube videos], *El Espectador*, February 24, 2016, http://bit.ly/2a1yv3j.

50 "Continúa La Censura - Bloquearon la página en Facebook de la delegación de paz Farc-Ep," [Censorship Continues – Farc-Ep Peace delegation Facebook page is blocked], Diálogos de Paz, June 13, 2013, http://bit.ly/2c4KGgq; "About Cyberwar against Farc-Ep," Farc-EP Peace Delegation, October 2, 2013, http://bit.ly/2cln6xJ.

51 "Por promover paro armado Twitter suspende cuentas del ELN," [Twitter suspends ELN accounts for promoting armed strike], *El Espectador,* February 13, 2016, http://bit.ly/1TZyL5e; See also: "Twitter le cierra las puertas al ELN" [Twitter closes its doors on ELN], *Semana,* February 13, 2016, http://bit.ly/1SOAGuz.

52 Constitutional Court, Judgement T-040/13, January 28, 2013, http://bit.ly/1FyIMlk; Constitutional Court, Judgement T-453/13, July 15, 2013, http://bit.ly/1R6lHaO; Constitutional Court, Judgement T-634/13, September 13, 2013, http://bit.ly/1OyMApE.

53 Constitutional Court, Judgement T-277/15, May 12, 2015, http://bit.ly/1iQCR1b.

54 Electronic Frontier Foundation, "Google to France: We Won't Forget It for You Wholesale," August 3, 2015, http://bit.ly/1P2iyYL.

55 Fundación Karisma, "Corte Constitucional colombiana decide sobre caso de derecho al olvido en Internet," [Colombian Constitutional Court decides on right to be forgotten on internet], July 6, 2015, http://bit.ly/1FmskVr.

56 Alexa, "Top Sites in Colombia," accessed February 26, 2016, http://bit.ly/1n5rG5V.

dia—and likely spills over into online media as well.[57] According to a national survey of journalists conducted in 2015 by Proyecto Antonio Nariño (PAN), an alliance of organizations focused on freedom of expression and access to information, 36 percent of respondents stated that they avoided publishing information due to fear of aggression; 30 percent feared losing their jobs or having their media outlets closed; 16 percent feared pressure from state actors; 15 percent believed that media outlets in their region modify their editorial positions; 25 percent feared the presence of illegal actors; 27 percent stated that they did not publish information because they feared affronts from state actors; and 8 percent because they feared lawsuits for defamation.[58]

Given that financing is often extremely difficult, government advertising can make a significant difference in an outlet's long-term existence. PAN's survey revealed that 66 percent of respondents believed that some media in their department avoid publishing on sensitive issues because they fear loss of advertising, closure, or administrative sanctions, while 62 percent stated they knew cases where journalists changed their position in exchange for advertising or political favors.[59] Although funding from the government, partisan, or corporate interests may manipulate online reporting, online media appear to have more independence from these funding sources, whereas official advertisement and favorable government relations are often a necessary condition for the continued operations of many offline outlets, especially in rural Colombian provinces.[60]

Zero-rating programs such as Facebook's Free Basics have recently generated substantial debate among Colombian digital rights activists. Law 1450 (2011) and Resolution 3502 (2011) stipulate that ISPs may offer internet plans according to "the needs of market segments or of their users," which in practice allows them to offer plans in which the data consumption on certain applications (such as WhatsApp or Facebook) does not affect the contracted data limit. Mobile service providers offer several kinds of data plans, many of them obscure in terms of the network management being applied, as well as which kind of content and applications may affect data consumption and charges.[61] Fixed internet service is subject to the same transparency and regulation issues. CRC has presented drafts on how to evaluate zero-rating plans,[62] and opened a blog to post information about regulatory matters to allow anyone interested to debate with the authority.[63]

Colombia was the first country in South America to launch Facebook's Free Basics[64] in January 2015, in partnership with the mobile carrier Tigo. Offering users access to 16 applications for free for two months, it was welcomed by the government as a catalyst for expanding internet access across the

57 Although there are studies concerning self-censorship among journalists, to date, there are none concerning self-censorship among ordinary internet users.

58 Survey results on Freedom of Expression and Access to Information in Colombia, September 2015, pg. 35-42, http://bit.ly/1VDzisl.

59 Survey results on Freedom of Expression and Access to Information in Colombia, September 2015, pg. 38, http://bit.ly/1VDzisl.

60 Censura Indirecta, "Indirect Censorship Project," Press Release, http://bit.ly/1NZ6ZUM.

61 Fundación Karisma, "¿Cómo se contrata en América Latina el acceso a Internet? ¿Qué tiene que ver esto con la neutralidad de la red?" [How does Latin America engage on Internet Access? What that has to do with Net Neutrality?], June 15, 2016, http://bit.ly/1OQxgWZ.

62 Proceedings of the Colombian Board for Internet Governance, April 14, 2016, http://bit.ly/23ZXOqo.

63 "Regulador de comunicaciones lanza blog para hablar sobre TIC" [Communications regulator launches blog to discuss ICTs], *El Espectador*, May 17, 2016, http://bit.ly/1WGEYWw; See also first post addressing the matter of zero rating plans: "¿Qué es la oferta Zero Rating?" [What is Zero Rating?], May 16, 2016, http://bit.ly/1VeeYjT.

64 In September 2015, Internet.org changed its name to Free Basics.

country.[65] While favorable media coverage argues that the program is better than no access at all,[66] critics have raised concerns about user privacy and net neutrality, as it also risks limiting users to a narrow range of services provided for free.

Digital Activism

Colombian social movements have increasingly used online platforms to campaign and investigate issues.[67] Colombia's intellectual property law enforces harsh penalties for violations, and online campaigns such as #CompartirNoEsDelito ("Sharing is not a crime") have sought to promote open access to scientific and li erary knowledge (See Prosecutions and Detentions for Online Activities). Since 2011, there have been four failed attempts to address Colombia's obligations under the Free Trade Agreement signed with United States regarding intellectual property, one of which sought to impose a notice-and-takedown system for copyright infringement.[68] Negative reactions from civil society, copyright experts and the academic community, and pressure from social media may have motivated lawmakers to put these initiatives on hold.[69]

Social media channels promoted a number of political and social protests during this coverage period. In August 2015, some 30,000 people rallied in major cities to pay tribute to Colombia's soldiers and policemen, to criticize the government's handling of the peace process and to express opposition to the bilateral ceasefi e. There was also considerable social media activity surrounding a rally promoted by Centro Democrático on April 2, 2016. Using the hashtags #Abril2ALaCalle and #eshoradesaliralacalle, promoters encouraged people to mobilize against the peace process and government corruption scandals. Pro-ceasefi e users, including the top leader of the FARC (Rodrigo Londoño Echeverry–a.k.a. "Timochenko"), voiced their counterarguments using the hashtags #HagámosleConejoALaGuerra and #YoDefiendoLosDialogos [70]

Violations of User Rights

Although prosecutions for online expression are rare in Colombia, harsh penalties for minor copyright violations and criminal penalties for defamation continue to pose a serious threat to users' rights. In an ongoing trial, one user still faced up to eight years in prison under Colombia's excessively harsh copyright laws, after he posted an academic article on the website Scribd. Although the government has taken some positive steps to prosecute illegal surveillance in recent years, concerns remain over widespread surveillance and violations of privacy.

65 Ministry of ICT, "Mark Zuckerberg llega este miércoles a Colombia para sellar alianza con el Gobierno," [Zuckerberg arrives in Colombia to seal Alliance with government], January 13, 2015, http://bit.ly/1CePl69.

66 José Carlos García, ¿Por qué se critica tan duro a Internet.org? Análisis," [Why the hard critique to Internet.org? Analysis], *El Tiempo,* January 20, 2015, http://bit.ly/1EVQjtQ; Álvaro Montes, "Mucho más que Facebook" [More than Facebook], *Semana*, January 17, 2015, http://bit.ly/1DPrh9K.

67 Somos Defensores, "Una Puerta hacia la Paz," *Revista Revelando,* 2013, 87, http://bit.ly/1jO7wfu.

68 The fi st was rejected in Congress; the second, although it became law, was declared unconstitutional by the Constitutional Court; the third project lost the support of the national government, and was removed immediately; the last one was introduced, but not enough to be subjected to the fi st debate in Congress, it was withdrawn.

69 "Manisfestación virtual contra la llamada Ley Lleras 2" [Virtual protest against the so-called Lleras 2 Law], *El Colombiano,* http://bit.ly/1QnK069; "La nueva ley Lleras recarga el ciberespacio de protestas," [The new Lleras law fills cybe space with protests], *El Colombiano, March 28, 2012,* http://bit.ly/1QnPYnn.

70 "Sin respaldo masivo, uribistas marcharon contra el proceso de paz," [Without massive support, uribistas marched against the peace process], *El Universal,* August 7, 2015, http://bit.ly/1OtL9Dp; "Uribismo saldrá a las calles el 2 de abril," *El Espectador*, February 22, 2016 http://bit.ly/1T4elJB.

Legal Environment

Article 20 of Colombia's National Constitution guarantees freedom of information and expression and prohibits prior restraint. This article was developed by the Constitutional Court in accordance with the standards of the Inter-American Court of Human Rights. Article 73 further provides for the protection of "the liberty and professional independence" of "journalistic activity." Although there are no specific p ovisions protecting freedom of expression online, a blogger has the same liberties and protections as a print or broadcast journalist.[71] The Constitutional Court confi med the application of such protections to the internet in a 2012 ruling.72 In its decision, the court stressed the Joint Declaration on Freedom of Expression and the Internet, which states that "freedom of expression applies to the internet, as it does to all means of communication," and that "restrictions on freedom of expression on the internet are only acceptable if they comply with established international standards… are provided for by law, and…are necessary to protect an interest which is recognized under international law [the "three-part" test]."[73]

Despite the protections for free expression established in Colombian law, Colombia still has criminal penalties for defamation, which have been applied to online speech. According to the Colombian penal code, individuals accused of insult can face between 1.3 and 6 years in jail and a fine f US$3,000 to US$345,000, while individuals accused of libel can face between 1.3 and 4.5 years in jail, with the same possible fines [74] Although there are no penalties in place for libel, defamation, irresponsible journalism, or rumor mongering that are specific o online content, cases pertaining to online defamation have occasionally been brought before the court with varying outcomes.

The courts have not applied the penal code's provisions on libel and slander to third party intermediaries; however, the penal code includes a concerning provision regarding online publication or reproduction of insults against others. According to Article 222 of the penal code, "whoever publishes, reproduces, or repeats insult or libel" may also be subject to punishment. This article raises concerns as it leaves open the possibility for charges of indirect insult and libel. The following article in the penal code establishes the use of "social mediums of communication or of other collective divulgence" as an aggravating circumstance that can increase the penalty for insult or libel. The use of the internet was considered an aggravating circumstance in the case against Gonzalo Hernán López (See Prosecutions and Detentions for Online Activities).[75]

In July 2015, two bombings in the capital city of Bogotá injured ten people.[76] In the wake of the attacks, the Prosecutor General declared that anyone who shares photos or videos of possible terrorist attacks in publications or on social networks instead of surrendering the material directly to the authorities is subject to prosecution.77 The statement received widespread criticism since such prosecutions would lack legal basis and would entail a serious violation of the right to expression and

71 Several decisions of the Constitutional Court state that Freedom of Expression is a universal right. See for example: Constitutional Court, Judgement C-442/11, May 25, 2011, http://bit.ly/1YG6pic.

72 Constitutional Court, Judgement T550/12, January 18, 2012, http://bit.ly/1VfPNt8.

73 UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, et al, "Joint Declaration on Freedom of Expression and the Internet," Organization of American States, 2011, http://bit.ly/1LSySYx.

74 Art. 220-222 of the Penal Code, http://bit.ly/1LC0FAz.

75 Law 599 of 2000, Criminal Code, Title V, http://bit.ly/1ZcoeFG.

76 "Diez lesionados dejaron las dos explosiones en Bogotá" [Ten injured left after explosions in Bogotá], *El Tiempo*, July 2, 2015, http://bit.ly/1NAhhao.

77 Adriaan Alsema, "Colombia government threatens to imprison citizens who publish photos or videos of attacks," *Colombia Reports*, July 6, 2015, http://bit.ly/1G5cCqT.

information.78 However, no one has yet been prosecuted under this edict.

Prosecutions and Detentions for Online Activities

Prosecution, imprisonment, or detention for ICT activities is quite rare in Colombia, and writers, commentators, or bloggers are not systematically subject to imprisonment or fines as a result of posting material on the internet.[79]

However, Colombia's first online criminal defamation sentence has set a concerning precedent for violations of user rights. In November 2015, the Foundation for Press Freedom (FLIP) reported it had submitted a petition to the Inter-American Commission on Human Rights,[80] after Colombian courts convicted Gonzalo López, an internet user who anonymously posted a comment criticizing a public official on a newspaper's website.[81] Gonzalo López was sentenced in July 2014 to 18 months and 20 days in prison and issued a fine of COP 9,500,000 (US$4,700), although he did not serve jail time based on provisions in Colombian law that allow certain defendants to avoid imprisonment depending on their sentence and prior record. In October 2014, using a writ of protection of fundamental rights (acción de tutela), López again challenged the sentence for violating his right to freedom of expression, but his appeal was denied in February 2015. The Constitutional Court did not select the case for revision, exhausting his options to overturn the conviction.[82]

Colombia has harsh penalties for copyright violations and currently lacks the flexible fair use standards employed in many countries. An ongoing case involving Colombian student Diego Gómez is at the center of a campaign to promote open access to scientific and literary knowledge (under the hashtag #CompartirNoEsDelito).[83] In July 2014, Gómez was charged with violating copyright violations for uploading an academic thesis onto Scribd. The author of the thesis complained and pushed for a criminal prosecution. Different voices in online and offline media criticized the decision to investigate the biologist and pointed out that Gómez did not seek personal attribution and did not profit by sharing the document [84] If convicted, Gómez may face up to eight years in prison on top of substantial fines

In November 2015, the Supreme Court confirmed the decision by the High Court of Bogotá to overturn the conviction of Joaquín Pérez Becerra, director of ANNCOL—a Sweden-based leftist news site that has been highly critical of the Colombian government.[85] After being arrested while traveling through Venezuela and brought to Colombia, Becerra was sentenced to eight years in prison in 2012

78 "Polémica desata declaración del Fiscal General que restringe el uso de videos y audios de ciudadanos" [General Prosecutor's declarations that restricts use of citizen's videos and audio raise controversy], *RCN Radio*, July 3, 2015, http://bit.ly/1QFkeWC.

79 The only documented case of an individual going to jail took place in 2010, well before the timeframe of this report. See: "Crónica del 'Falso Positivo' de Facebook en nueve episodios," *La Silla Vacia*, May 4, 2010, http://bit.ly/1L6Fv9U.

80 FLIP, "Caso de Gonzalo López se presenta ante la CIDH," [Case of Gonzalo Lopez presented to IACHR], November 20, 2015, http://bit.ly/1kLxuRK.

81 Colombian law does not prohibit anonymity, so the fact that the post was anonymous did not influence the charges against López.

82 Carlos Cortés, "Crónica de una ofensa inofensiva," [Chronicle of an unoffensive offense], *La Silla Vacía,* April 17, 2015, http://bit.ly/1ODNXEl.

83 "Diego Gómez y la importancia de los bienes comunes" [Diego Gómez and the importance of common goods], Pillku Amantes de la libertad, December 17, 2015 http://bit.ly/1oHMK3u

84 "Compartir no es un delito" [Sharing is not a crime], *El Espectador, July 16, 2014,* http://bit.ly/1laphQ5; "Compartir no es un delito," *Las 2 Orillas, December 26, 2014,* http://bit.ly/WaUTQ6.

85 "Ratifican absolución al director de Anncol, Joaquín Pérez Becerra" [Absolution ratified for Director of Anncol, Joaquin Perez Becerra], *El País, November 9, 2015,* http://bit.ly/1LfEeD2.

on the charge of criminal conspiracy as an ally of the FARC guerrilla group.86 According to the prosecutor's office, his ork in the news agency served FARC's interests and connected them with funds from his connections in Europe. After spending three years in prison, the High Court ordered his release, saying that they could not find adequa e evidence to support his conviction.[87]

Surveillance, Privacy, and Anonymity

Some steps have been taken to punish perpetrators of illegal surveillance, although it seems unlikely that these efforts have changed the overall environment for surveillance in Colombia, as intelligence agencies continue to operate with minimal oversight. Concerns about illegal surveillance by certain sectors of the government and military persist, with investigative journalists continuing to uncover grave privacy violations by the police and military.

In late 2015, anonymous informants warned that investigative journalists had their communications intercepted illegally by the National Police, notably in retaliation for a news story by journalist Vicky Dávila on a possible prostitution network tied to the police.[88] In response to reports of surveillance of investigative journalists, a disciplinary investigation against the Director of the National Police was announced in February 2016,[89] who submitted his resignation the next day, although he stated he was innocent.[90] The prosecutor in charge of the case has reportedly received death threats.[91] Other leaks have shown that journalists who cover sensitive issues, like the peace process, have been subject to monitoring. In October 2014, reporters revealed that military intelligence services maintained a list of professional and personal e-mail addresses of national and international journalists who had covered the peace talks between the Colombian government and FARC representatives, as well as personal email addresses of NGO members and foreign diplomats. The purpose of the list is unknown.[92]

Episodes of extralegal surveillance (known in Colombia as "Las Chuzadas"), carried out by intelligence agencies, the army or the police, have constituted an ongoing scandal in Colombia in recent years. In February 2014, the Colombian magazine *Semana* exposed an illegal wiretapping operation carried out by the army under the code name Andrómeda, against government representatives taking part in peace talks with FARC leaders in Havana, Cuba.[93] In May 2014, in the midst of presidential election campaigns, *Semana* revealed a video in which Andrés Fernando Sepúlveda, who worked for the presidential campaign of Oscar Iván Zuluaga—a front runner against President Juan Manuel Santos—was seen discussing confidential info mation about FARC members participating in the peace

86 "Condenado a 8 años de cárcel Joaquín Pérez Becerra, editor de Anncol" [Joaquín Pérez, Anncol's editor sentenced to 8 years of prison], *El Tiempo*, September 7, 2012, http://bit.ly/1PzU5KF.

87 "En libertad Joaquín Pérez, director de Anncol" [Joaquín Pérez, director of Anncol, was released], *El Espectador*, July 17, 2014, http://bit.ly/1KHNIBj.

88 "'El Gobierno nos dejó solos': Claudia Morales," [The government left us alone], *El Espectador, December 19, 2015,* http://bit.ly/1Yubc3p.

89 "Detalles de cómo la Procuraduría decidió abrir una investigación contra Palomino," [Details on how the prosecutor decided to open an investigation against Palomino], *El Espectador, February 16, 2016,* http://bit.ly/1S1eaND.

90 "Renuncia General Palomino a la Policía Nacional," [General Palomino resigns from National Police], *Caracol Radio, February 17, 2016,* http://bit.ly/1mHcJqz.

91 "Fiscal que investiga seguimientos ilegales a periodistas recibió amenazas," [Prosecutor who investigates ilegal monitoring of journalists received threats], *El Espectador, December 24, 2015.* http://bit.ly/1Segsbv

92 "La polémica lista de Inteligencia Militar" [The controversial list of Military Intelligence], *Semana*, October 28, 2014, http://bit.ly/1oXkObe.

93 "Alguien Espió a los Negociadores de La Habana?" [Who Spied on the Negotiators in Havana?], *Semana,* February 3, 2014, http://bit.ly/1fVeY0F; See also: "Las Chuza-DAS," *Semana*, December 19, 2009, http://bit.ly/1JYShZ7.

talks and strategies to use that information during the campaign.[94]

Courts have sought to rein in illegal and excessive surveillance, passing down sentences to former public officials in olved wiretapping scandals. On April 29, 2015, the Supreme Court sentenced Maria del Pilar Hurtado, former director of the government Administrative Security Department (DAS), and Bernardo Moreno, former secretary of the president's office, o 14 and 8 years in prison, respectively, on charges of illegal interception of private communications of journalists, politicians, and NGOs.[95] Some military officials ere fi ed in early 2015 as a result of the Andrómeda wiretapping leaks.[96] Although it is not clear whether Sepúlveda intercepted communications or paid for information from people participating in Andrómeda,[97] he signed a plea bargain and was sentenced to 10 years of prison for illegal interception of communications and use of malicious software, amongst other charges.[98] In this same case, criminal proceedings were initiated against an adviser of the presidential campaign Zuluaga (Luis Alfonso Hoyos), on charges of conspiracy, violation of personal data, abusive access to computer system, and use of malicious software. In February 2016, Hoyos' defense team called for the annulment of the trial because of alleged procedural irregularities.[99]

Although investigative journalists have sought to uncover surveillance practices, the scope of government and military surveillance in Colombia is still unclear. The lack of clarity regarding surveillance is aggravated by the fact that the only body in charge of overseeing surveillance activities has never exercised its faculties because of delays on the fulfillment f operative requirements set by the Intelligence Law. According to the human rights organization Dejusticia in December 2015, the Commission to Monitor the Activities of Intelligence and Counterintelligence has skipped the presentation of three annual reports addressed to the president about the observation of the legitimacy of intelligence activities and its corresponding follow up and the presentation of two legal concepts about audit reports made by the General Comptroller. It has also refrained from asking for information on intelligence expenditures related to the National Intelligence Plans from previous years.[100]

In July 2015, a hacker leaked 400GB of documents from the Italian information technology company Hacking Team, which is best known for providing spyware to governments. Among these documents were emails suggesting that the Colombian government had contracts with the company, evidence that supports research published by Citizen Lab at the University of Toronto in early 2014.[101] Leaked emails reference the National Police Offic 's purchase of Hacking Team's Remote Control System (RCS) called "Galileo," which is capable of accessing and hijacking the target devices' keyboard register, microphone and camera. Although National Police have denied any direct relation with Hacking Team and have only admitted to contractual ties with a Colombian company called Robotec, which

94 "El video del 'hacker' y Zuluaga" [The video of the hacker and Zuluaga] *Semana,* May 17, 2014, http://bit.ly/Tg67l4.

95 "Condena de 14 años para Hurtado y 8 para Bernardo Moreno por chuzadas," [Sentence of 14 years to Hurtado and 8 years to Bernardo Moreno for 'Chuzadas'], *El Tiempo,* April 30, 2015, http://bit.ly/1biN0yV.

96 "Purga en inteligencia de las Fuerzas Militares por escándalo de Andrómeda" [Purge in intelligence services and military forces because of Andromeda scandal], *Blu Radio*, January 23, 2015, http://bit.ly/1iAIJdW.

97 "'Hacker' del Proceso de Paz Dice que Compró Datos de Andrómeda" [Peace process hacker says he bought information from Andrómeda], *el tiempo*, may 15, 2014, http://bit.ly/1jy2v2q.

98 "Condenan a 10 años de prisión al 'hacker' Andrés Fernando Sepúlveda" ['Hacker' Andrés Fernando Sepúlveda sentenced to 10 years of prison], *El Espectador,* April 10, 2015, http://bit.ly/1afM3qs.

99 "Fiscalía imputará cargos contra Luis Alfonso Hoyos en caso hacker Sepúlveda," *El Colombiano, May 19, 2016.* http://bit.ly/1Sb6AjC; "La encrucijada de Luis Alfonso Hoyos," *Semana, September 26, 2015,* http://bit.ly/1oIchcV; "Defensa de Luis Alfonso Hoyos pidió anular proceso sobre nexos con el hacker Sepúlveda," *RCN Radio, February 26, 2016* http://bit.ly/24w7gVt.

100 Dejusticia, FOIA request addressed to the Follow-up Legal Commission of Intelligence and Counter Intelligence Activities and the Joint Intelligence Commission, December 7, 2015, http://bit.ly/1svsFPU.

101 Bill Marczak, et al. "Mapping Hacking Team's "Untraceable" Spyware," Citizen Lab, February 17, 2014, http://bit.ly/1kPDo0Y.

distributes Hacking Team's services,[102] the leaked documents indicate that the National Police contacted Hacking Team directly to activate spyware.[103] Another leaked email suggested that the U.S. Drug Enforcement Agency (DEA) may be engaged in surveillance practices in Colombia.[104] Although it is still unclear if Hacking Team software is currently being used by the National Police or U.S. DEA, and, if so, how it is being used, several Colombian civil society organizations criticized the excessive and apparently uncontrolled use of intelligence tools in the country, which they argue has been facilitated by "weak legislation" on intelligence matters.[105]

In September 2015, police sources reportedly said that they would start testing a centralized platform for monitoring and analysis, known as PUMA, and that operations would be limited to telephone lines and would not include social networks and chats.[106] At the same time, the General Comptroller of the Republic has launched an investigation against the National Police for alleged irregularities in the acquisition of the system. In August 2014, the Prosecutor General's office had ordered to stop the development of PUMA because of the lack of transparency and guarantees to its lawful use. Details about PUMA initially surfaced in June 2013, when journalists reported that the government was investing upward of US$100 million in a monitoring platform, which was to become operational by the end of 2014 and would provide the government with the capacity to intercept communications in real-time, extending to social media, email, telephone networks, and internet data traffic [107]

While intercepting personal communications in Colombia is authorized only for criminal investigation purposes and legally requires a judicial order,[108] service providers are required to collaborate with intelligence agencies by providing access to the communications history or technical data of any specific user withou a warrant.[109] Retention and treatment of user data by authorities other than the intelligence agencies and departments related to criminal investigation has not yet been regulated in Colombia. Colombian law also allows intelligence agencies to monitor the electromagnetic spectrum without a judicial order.[110] An additional threat to user privacy comes in the form of Article 2 of Decree 1704 (2012), which requires that ISPs create backdoor access points for criminal investigation purposes—which can be used under the Prosecutor General's authorization. A service provider that does not comply with these obligations faces fines and could lose its operating license [111]

Colombia has no general restrictions against anonymous communication, and there are no registration requirements for bloggers, cybercafe owners, or users. However, there are many regulations that can negatively impact anonymity. The police has access to a database that must be maintained

102 "Policía indicó no tener vínculos comerciales con fi ma Hacking Team" [Police declared that there are no commercial links with Hacking Team], *El Tiempo,* July 8, 2015, http://bit.ly/1WnPXRJ.

103 Carolina Botero and Pilar Sáenz, "In Colombia, PUMA is not what it seems," Digital Rights Latin America & The Caribbean, August 24, 2015, http://bit.ly/1JuchzP.

104 Ryan Gallagher, "Hacking Team Emails Expose Proposed Death Squad Deal Secret UK Sales Push, and Much More," *The Intercept*, July 8, 2015, http://bit.ly/1PCTFmi.

105 FLIP, CCJ, Dejusticia, Fundación Karisma and Colnodo, "Colombian Police Ought to Clarify Their Relationship with 'Hacking Team'," July 30, 2015, http://bit.ly/1KzZHD4.

106 "Plataforma Puma de la Policía entrará en operación, pero limitada," [Puma Platform will enter into operation, but limited], *El Tiempo*, September 30, 2015 http://bit.ly/1TtnbAj.

107 Daniel Valero, "Policía Podrá Interceptar Facebook, Twitter y Skype en Colombia" [Police will be able to tap Facebook, Twitter y Skype in Colombia], *El Tiempo*, June 23, 2013, http://bit.ly/1Mv2bmO.

108 Constitution of 1991, art. 250, http://bit.ly/1KLrfTl.

109 Statutory Law 1621, art. 44, April 17, 2013, http://bit.ly/1LDxHQX.

110 Statutory Law 1621, art. 17, April 17, 2013, http://bit.ly/1LDxHQX; See also: Constitutional Court, Judgement C-540/12, 2012, http://bit.ly/1IdXI2t.

111 Decree 1704, 2012, art. 7. http://bit.ly/1YGdzTA

by telecommunication service providers. This database contains user data, such as name, ID number, place and residence address, mobile phone number and service activation date.[112] Users must provide accurate information under penalty of perjury, which is punishable by a minimum of six years in prison.[113] The recently approved Police Act imposes sanctions on the activation of mobile numbers or SIM cards without the appropriate collection of subscriber's personal information.

Since 1993 Colombian law has banned the use of "communication devices that use the electromagnetic spectrum" to send "encrypted messages or messages in unintelligible language."[114] In response to an information request, the ICT ministry explained that those provisions apply only "to the content of the communications, not the encryption of the medium." Despite of the ambiguous wording of the law, the ICT ministry further claimed that these provisions only apply to radio-like devices and not to the internet.[115] The Intelligence and Counterintelligence Act stipulates that voice encryption service may be implemented "exclusively" for the intelligence agencies and "high government" officials by telecommunications service providers.[116]

Intimidation and Violence

Corruption, longstanding armed conflict and associa ed surveillance, and the war against drugs continue to be the greatest threats facing freedom of expression in Colombia, although online journalists have not faced the same level of danger as print journalists. There is no broad trend of retaliation specifically for online con ent in Colombia, but in general, a high level of intimidation towards media and human rights defenders creates a climate of fear that also affects online journalists.

According to the NGO FLIP, at least 16 journalists have been murdered and many more have been threatened since 2005, and at least 2 were killed in 2015.[117] These statistics represent a continuation of violence in a country that has seen at least 142 murders of journalists in the past four decades. Of these, 67 cases have already reached their statute of limitations, meaning that the victims' families will never see justice.118 Impunity for perpetrators of violence—a pervasive problem in Colombia's judicial system—is ranked by the nonprofit AN's *Freedom of Expression and Access to Information Index* as one of the gravest threats to freedom of expression.[119] Colombia has the third highest impunity rate on the Global Impunity Index of the Center for Studies on Impunity and Justice Institute.[120]

Due to the country's high level of violence, it is difficult o isolate deaths that have resulted specifically from online activity. Daniel Mejía, activist and director of the magazine *Senxura,* received a threat against his life and the lives of his family in October 2014, allegedly for his reporting on illegal brick factories in Sogamoso, which he published through traditional and online media.[121] Mejía

112 Law 418 of 1997, art. 99, http://bit.ly/1Gw5sg9; and Resolution 0912, 2008 of the National Police, Diario Oficial, ño CXLIV, Nº 47.233, January 15, 2009.

113 The penal code outlines penalties for perjury of bearing "false witness." Penal Code, art. 442, http://bit.ly/1S3N9sT.

114 Law 418 (1997) art. 102, http://bit.ly/1PXVz1z.

115 Communication Nº 811811, ICT Ministry to Karisma Foundation, April 27 of 2015.

116 Statutory Law 1621, art. 44, April 17, 2013, http://bit.ly/1LDxHQX.

117 Fundación Para La Libertad De Prensa (FLIP), "Periodistas Asesinados" [Journalists killed], http://bit.ly/1Gbwn7u.

118 FLIP, 60 AÑOS de espionaje a periodistas en Colombia, http://bit.ly/1E5ReYu.

119 Survey results on Freedom of Expression and Access to Information in Colombia, September 2015, pg. 43-46, http://bit.ly/1VDzisl.

120 Centro de Estudios sobre Impunidad y Justicia, "Índice Global de Impunidad 2015," [Global Impunity Index 2015], Universidad de las Américas Puebla, April 2015, pg. 39-42, http://bit.ly/1KPhqdy.

121 David Gagne, "Journalists Increasingly Under Fire in Colombia," *InSightCrime*, January 21, 2015, http://bit.ly/1YGf6Jt.

alleges that the threats came from paramilitary organizations with the participation of a member of the military forces.122 FLIP has also suggested that the murder of lawyer Edison Molina in September 2013 may have been linked to his online activity, as he denounced acts of corruption in local government.123 Despite the general lack of activity on the case,[124] in January 2014 it was reassigned to the Human Rights Unit of the Prosecutor General's Offic .[125]

A study by Fundación Karisma on violence against female journalists online found that attacks against women are more personal and aim to damage women's self-esteem. Female journalists interviewed explained that the effectiveness of online harassment lies in the uncertainty that comes from not knowing when the attack is going to happen, generating stress and self-censorship. The survey also noted the state's slow or inexistent response to reports of online threats or intimidation.[126]

Technical Attacks

Various types of cybercrime, including hacking, illegal interception and use of data, and the distribution and use of malware are criminalized under Law 1273, which was passed in 2009. Penalties range from three to four years' imprisonment, along with fines [127] While phishing—the stealing of sensitive personal data via malware disguised as legitimate email—appears to be a significant issue in Colo - bia,128 most evidence of hacking and other interception has involved interagency spying and intelligence work carried out primarily by the government, the army, and other official bodies (see Su veillance, Privacy, and Anonymity). Despite the president's recent emphasis on Colombia's vulnerability to cyberattacks, there are few known cases of technical violence perpetrated by private actors.[129]

A report on global security and "cyberwellness" prepared by the ITU in April 2015 ranked Colombia in fi th place in Latin America and ninth globally in terms of commitment and readiness.[130] However, following the army's Andrómeda hacking scandal in early 2014, President Santos publicly stated that Colombia's cyber defense sector was sorely lacking, and announced the creation of a commission focused on strengthening national cybersecurity.[131] Colombia then partnered with the Organization of American States (OAS) to develop two bodies—the Colombian Cyber Emergency Response Group

122 W Radio, "Señalan a militar de amenazar de muerte a periodista y activista de Boyacá" [Military accused of death threats against journalist and activist in Boyacá], News release, October 10, 2014, http://bit.ly/1yscrTp.

123 FLIP, "Protestas, Sin Garantías para Cubrir" [Protests, without Guarantee of Coverage], Annual Report on Freedom of the Press in Colombia, http://bit.ly/1KHQVR6.

124 FLIP, "Dos años de impunidad del asesinato del periodista Edison Molina" [The murder of journalist Edison Molina: two years in impunity], September 11, 2015, http://bit.ly/1K0SGbT.

125 "Édinson denunció y encontró la muerte," [Edinson denounced and he found death], *El Espectador*, February 2014, http://bit.ly/1cjvIfg.

126 Fundación Karisma, "Misoginia en internet: bombardeo a campo abierto contra las periodistas" [Misogyny on the internet: open field bombing against female jou nalists], February 24, 2016, http://bit.ly/1Qf9anl.

127 Rachel Glickhouse, "Explainer: Fighting Cybercrime in Latin America," Americas Society/Council of the Americas Online, November 14, 2013, http://bit.ly/1FyUXP1.

128 Mimi Yagoub, "Cyber Crime in Colombia: An Underestimated Threat?" *InSight Crime*, July 11, 2014, http://bit.ly/1PCXnMS.

129 "Santos Anuncia Creación de Comisión para Evaluar Riesgo de un Ciber-Ataque", [Santos Announces Creation of a Committee to Assess Risks of a Cyberattack] *Blu Radio,* February 7, 2014, http://bit.ly/1d2I9jB.

130 MinTic, "Colombia es fuerte en ciberseguridad" [Colombia is strong in cybersecurity], November 30 2015, http://bit.ly/1KQFiNN.

131 "En Ciberseguridad, 'Estamos en Pañales' y Expuestos a Todo Tipo de Ataques: Santos" [In Cybersecurity, 'We are in Diapers' and Exposed to All Kinds of Attacks], *El Espectador*, February 8, 2014, http://bit.ly/1d6jM4J.

(coICERT) and the Cyber Police Center (CCP).[132]

The next digital security policy for Colombia was released by the government on April 2016[133] and frames the plans and actions regarding a variety of cyber security issues ranging from national defense and protection of critical infrastructures to cybercrime and digital risk management.[134] Although broad participation has not always been granted,[135] civil society groups expressed concerns about the approach in this new policy as it still favors a military perspective.[136]

132 Phillip Acuña, "Colombia to receive cyber-security assistance from international experts," *Colombia Reports*, March 31, 2014, http://bit.ly/1YGfveW, and Carolina Botero Cabrera "Intimidad vs Seguridad un año después" [Privacy v. Security one year after], *El Espectador*, April 2, 2015, http://bit.ly/1DBAHEA.

133 Document CONPES 3854, National Council for Social and Economic Policy, National Planning Department, April 11, 2016, http://bit.ly/1SchHow.

134 Ministry of ICT, "Colombia cuenta con una Política Nacional de Seguridad Digital" [Colombia has a National Digital Security Policy], April 13, 2016, http://bit.ly/1SACmC0.

135 Carolina Botero Cabrera, "Intimidad vs Seguridad un año después" [Privacy vs. Security one year later], *El Espectador*, April 2, 2015, http://bit.ly/1DBAHEA.

136 FLIP, Comisión Colombiana de Juristas and Fundación Karisma, "Comentarios al CONPES sobre seguridad digital desde Sociedad Civil" [Civil Society remarks on digital security policy], February 5, 2016, http://bit.ly/240dD0a.

Freedom House

Cuba

	2015	2016
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	22	21
Limits on Content (0-35)	27	26
Violations of User Rights (0-40)	32	32
TOTAL* (0-100)	**81**	**79**

* 0=most free, 100=least free

Population:	**11.4 million**
Internet Penetration 2015 (estimated):	**5-31 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- The Cuban government launched its fi st-ever paid public Wi-Fi hotspots in June and July 2015, promising to further expand access points in 2016. While these hotspots have become a popular way to access the internet, limited and expensive connections still constitute a major barrier (See **Availability and Ease of Access**).
- Since the United States and Cuba officially eestablished diplomatic relations, new regulations have eased restrictions on U.S. telecom companies to start offering services on the island. Larger scale telecommunications initiatives however, such as a reported proposal by Google to further expand access on the island, remained unanswered by Cuban government (See **ICT Market**).
- Bloggers and independent journalists continued to face censorship, intimidation and arrests. Several removals of content on the government-sponsored blog platform, Reflejos, were reported during this period (See **Content Removal** and **Prosecutions and Detentions for Online Activities**).
- Despite severe censorship of content deemed to be "counter-revolutionary," Cubans have launched a number of independent web-based information sites, offering alternative discourses about the Cuban reality (See **Media, Diversity and Content Manipulation**).

Introduction

Despite modest steps to increase internet access, Cuba remains one of the world's most repressive environments for information and communication technologies.

High prices, old infrastructure, prohibition of home connections, and extensive government regulation have resulted in a pronounced lack of access. The normalization of relations between Cuba and the United States and the opening of ICT trade has eliminated the Cuban government's ability to blame low levels of internet access on the "blockade." Even with the embargo still in place, policy changes have opened the way for U.S. telecommunications companies to start offering services to the island. Propelled by U.S. President Barack Obama's historic visit to the island in March 2016, this shift in relations has inspired optimism among many observers, who believe it may entail an opening for ICTs in Cuba.

Cuba has taken some tentative steps to reinforce this optimism by improving internet access on the island, but it is still just a drop in the bucket when it comes to alleviating the most draconian restrictions on internet freedom in the Western hemisphere. Access to the high-speed internet provided by the new ALBA-1 fibe -optic cable was finally ex ended to citizens in late 2013 via the opening of new "navigation halls." In a more recent move in July 2015, the government opened its fi st public Wi-Fi hotspots, and has been expanding them across urban centers in 2015 and 2016. However, home internet connections were still banned for the vast majority of Cubans, and even with reduced prices, public internet access points still cost US$2 per hour to use, which is equal to one-tenth of minimum monthly wages. Even for those who might be able afford the new access points, the supply of internet access, mostly concentrated in the capital, is grossly out of proportion with the needs of a country of more than 11 million people.

While the Cuban government faces increased pressure from its own citizens and the international community to expand access to the global internet, the optimism derived from normalization of relations with the U.S. and the increasing access may be premature. Many worry that the Cuban policy is inspired by the example of China and that new infrastructure will not mean an end to controlled and fil ered access. Despite the noteworthy emergence of several web-based information sites offering alternative discourses about the Cuban reality, the government has continued to exert control over the digital landscape by blocking critical independent news sites, removing certain content deemed to be "counter-revolutionary," and arresting or harassing online writers.

Obstacles to Access

Penetration rates and internet speeds continue to lag behind regional averages, and access to the global internet in Cuba is extremely restricted, due to high prices and government regulation of access points. Many users are still relegated to a tightly controlled government-filtered intranet and related email service. Nevertheless, some openings have taken place over the past years, and more Cubans have gained access to the global internet or to other channels for sharing information with fellow citizens. Email access via mobile devices has been enabled and hundreds of state-run access points are now available, including the first paid public Wi-Fi hotspots. A thawing in U.S.-Cuban relations has fueled optimism that ICT connectivity will further improve in the coming years.

Availability and Ease of Access

According to Cuba's National Statistics Office, there were 3.9 million internet users in Cuba in 2015, representing 34.8 percent of the population, up from 27 percent in 2014.[1] The latest data from the International Telecommunication Union (ITU) places Cuba's internet penetration at 31 percent as of 2015, up from 28 percent in 2013 and only 14 percent in 2009.[2] These numbers, however, also include users who can only access the government-controlled intranet, and experts have estimated that a much smaller percentage of Cubans have periodic access to the global internet.[3]

For years, most Cubans have been denied internet access or relegated to a highly filtered government-controlled intranet, which consists of a national email system, a Cuban encyclopedia, a pool of educational materials and open-access journals, Cuban websites, and foreign websites that are supportive of the Cuban government. The intranet can be accessed through government-run internet access centers, the offices of the state-owned Telecommunications Company of Cuba S.A. (ETECSA), or state-run cybercafes. Although most foreign websites are now available at state-run access sites, the cost of accessing non-Cuban sites remains higher.

Select categories of users such as Cuban officials, doctors, or trusted journalists and intellectuals have been authorized to access a broader, but still limited, portion of the global internet or other ICT tools. Resolution 92/2003 prohibits email and other ICT service providers from granting access to individuals who are not approved by the government, and requires that they enable only domestic chat services, not international ones. Entities that violate these regulations can be penalized with suspension or revocation of their authorization to provide access.[4] The government claims that all schools have computer labs, but in practice, internet access is usually prohibited for students or limited to very short periods of access, certain email accounts, or supervised activities on the national intranet. In May 2015, the Minister of Higher Education announced upcoming internet access for teachers, researchers, and students at four universities on campuses and in residences, but implementation remains to be seen.[5]

While home connections are virtually non-existent, the government has taken modest steps to enable public access to wired and wireless internet over the last few years. According to ETECSA in September 2016, there were more than 1,000 public access points on the island, including state-run cybercafes, public Wi-Fi hotspots, and Wi-Fi at hotels and airports.[6] In a recent move towards in-

1 National Office of Statistics and Information (ONEI), "*Tecnología de la Información y las Comunicaciones, 2015,*" *[Information* and Communication Technology, 2015], http://bit.ly/2ct5MFj.

2 International Telecommunication Union, "Percentage of Individuals Using the Internet," 2000-2015, accessed September 10, 2016, http://bit.ly/1cblxxY.

3 Exact estimates of the number of individuals who access the "global internet" in Cuba are hard to come by, as methodologies used to define and calculate access are often unclear. Some of the independent estimates from 2011 and 2012 put the number at around five percent. A more recent public opinion study conducted in March 2015 found that 16 percent of respondents out of 1,200 Cuban adults surveyed had access to the internet, via cyber cafes (43 percent), at work (34 percent), at school or university (22 percent), at home (21 percent), or elsewhere (8 percent). See: "International Survey of Cubans Living in Cuba," Bendixen & Amandi International Poll for Univision Noticias/Fusion in Collaboration with *The Washington Post*, April 2015, http://fus.in/2czwMGg.

4 According to the resolution, "Cuban websites that offer e-mail services cannot implement the creation of e-mail (Webmail) via an automatic process for natural persons or entities that are not duly authorized." Legislación para el Sistema Nacional de Salud, Resolución Ministerial No 92/2003, July 18, 2003, http://bit.ly/1jhSxdD.

5 Eduardo Pinto Sánchez, "Garantizarán Acceso a Internet a Estudiantes y Docentes de La Universad de Oriente," *Sierra Maestra,* May 24, 2015, http://bit.ly/1Wn3j0j.

6 "Cuba supera los mil puntos públicos de acceso a Internet" [Cuba exceeds more than 1,000 public internet access points], *CiberCuba*, September 9, 2016, http://bit.ly/2eFOZVm.

creasing public access to the internet, the government launched its first paid public Wi-Fi hotspots in urban centers in June and July 2015, accessible through the government platform Nauta.[7] The number of hotspots increased from 35 to 65 in 2015, with promises for some 80 more in 2016.[8] These Wi-Fi hotspots have become a popular way to access the internet, despite the high cost and complaints about the quality of service. ETECSA has boasted that some 200,000 users connect daily at Wi-Fi zones.[9]

The opening of these hotspots followed an initial experiment with public Wi-Fi in early 2015, when the first free public Wi-Fi access point in Cuba opened in January 2015 in the art studio of Cuba's visual artist Alexis Leyva, better known as "Kcho."[10] In March 2016, Kcho's studio hosted Google's first online tech center on the island, offering faster internet speeds and equipment.[11] While currently enabling a minor subsection of the general public to access the global internet for free, reports have still pointed to certain pages being blocked at the center, and certain restrictions placed on the use of USB flash drives and external hard drives.[12]

Access also expanded somewhat after the connection and activation in 2013 of ALBA-1, a 1,600 km high-speed undersea cable stretching between Cuba and Venezuela,[13] although not as impressively as many had hoped. Broadband service became selectively available on the island at government offices and state-owned access points, but not for home connections.[14] In June 2013, citizens began being able to access the internet through broadband connections to the new fiber-optic cable at 118 government-run "navigation halls." In December 2015, ETECSA counted 339 state-run cybercafes, and announced 100 more for 2016.[15]

To overcome access limitations, some Cubans have in turn developed improvisational underground networks, setting up illegal antennas, and systematically passing around USB flash drives with content downloaded from the internet (see Media, Diversity, and Content Manipulation). Informal local area networks use wired or wireless technology to exchange information, mostly entertainment content in the form of cybergames, music, and photos. For years, an informal network known as Street Net (SNET) has been connecting users through Ethernet cables and makeshift Wi-Fi antennas.[16] Some recent experiments have even managed to bring ETECSA's hotspots to homes through the use

7 Sandra Lilley, "Cuban Internet Usage: Public Wi-Fi spots Are a Big Draw," *NBC News*, August 12, 2015, http://nbcnews.to/1P6EDEJ.

8 "El acceso a internet en Cuba: una asignatura pendiente a pesar de las mejoras," [Access to internet in Cuba: a pending task despite improvements], *EFE,* February 6, 2016, http://bit.ly/2c9UHJ3.

9 "Unos 200 mil usuarios se conectan diariamente en las zonas wifi de Cuba" [Some 200,000 users connect to Wi-Fi hotspots on a daily basis in Cuba], *EFE,* March 29, 2016, http://bit.ly/2cnCs6g.

10 Jessica Plautz, "Cuba's first free public Wi-Fi is a gift from a contemporary artist," *Mashable*, March 16, 2015, http://on.mash.to/1KDovaf.

11 "Google abre en Cuba su primer centro tecnológico en el estudio del artista Kcho," [Google opens its first technological center in Cuba in the studio of the artist Kcho], *EFE,* March 23, 2016, http://bit.ly/1RzWYjI.

12 "Google entra por el aro en Cuba," [Google has jumped through hoops in Cuba], *14ymedio,* April 7, 2016, http://bit.ly/2cjJs3V.

13 "Llega a Cuba el Cable Submarine de Fibra Optica para Ofrecer Internet de Banda Ancha" [Underwater Fiber Optic Cable Arrives in Cuba to Offer Broad Band Internet] *El País*, February 10, 2011, http://bit.ly/1R5IuUp.

14 "Cuba First High-Speed Internet Connection Activated," *BBC*, January 24, 2013, http://bbc.in/V0ggOM.

15 "Cuba: Se incrementan posibilidades de acceso a Internet," [Cuba: possibilities for internet access increase], *Cubadebate,* December 24, 2015, http://bit.ly/2cgioST; See also: Cubasí, "Exclusiva con la Presidenta de ETECSA: Crece penetración de internet en Cuba" [Exclusive interview with the president of ETECSA: internet penetration grows in Cuba], Ministry of Communications, http://bit.ly/2flhZ3 .

16 "De la Comunidad del Anillo a SNET: las redes en la Tierra Media," *Cavicache Media,* March 1, 2016, http://bit.ly/2cLcsUA.

of street nets.[17] The Cuban authorities appear to largely turn a blind eye to such efforts since much of the content shared on these networks appears to be apolitical, but news has emerged of selective dismantling of these networks in some Havana neighborhoods.[18] The underground economy of internet access also includes account sharing, in which authorized users sell access to those without an official account for one or t o convertible pesos (CUC) per hour.

High costs and slow speeds also constitute major barriers, mainly due to weak domestic infrastructure. Most Cubans continue to face extremely slow connections of up to 1 Mbps, even at Wi-Fi hotspots.[19] While the government has cut prices for internet access points, hourly charges still amount to roughly 10 percent of the average monthly salary.[20] In February 2015, ETECSA temporarily reduced the hourly charge for using the internet at state-run cybercafes from US$4.50 an hour to US$2.00 per hour.[21] For a much lower fee of US$0.60 an hour, Cubans were able to access domestic websites only.[22] According to one blogger's account, users at navigation halls can access foreign news sites like the BBC, *El País*, and the *Financial Times*, as well as Miami-based *El Nuevo Herald* and *Diario de las Américas* if they can afford the higher fees for international websites.[23] However, sites such as Radio/TV Martí, the U.S. government broadcaster that transmits to the island, have been blocked (see Blocking and Filtering). The price cut received little attention in the state media, and news spread by word of mouth. ETECSA later announced that the lowered price would go into long-term effect beginning July 1, 2015, including the new Wi-Fi access points that were opened in parks and other public venues around the island.[24]

Users pay for government-run internet service directly at navigation halls or by purchasing a "Nauta" card (a pass that links to ETECSA's interface of the same name and can only be used at specific l - cations), which allows them to access temporary accounts, valid for 30 calendar days as of the date of the fi st session. They are also able to open permanent accounts upon request, complete with username, password, and email address, if they can afford the cost of the service—and the high level of surveillance associated with such accounts. ETECSA monitors the accounts and retains the right to end a user's access for a sweeping range of violations (see Surveillance, Privacy and Anonymity).

In early 2008, after a nearly decade-long ban, the government began allowing Cubans to buy personal computers, but prohibitively high costs place computers beyond the reach of most of the population.[25] Out of a country of more than 11.3 million people, the number of computers was only a little over one million in 2014 according to the National Office f Statistics, and, of these, only about half had connectivity.[26] Phones that utilize Global Positioning System (GPS) technology or satellite

17 "Internet llega a los hogares cubanos a pesar de ETECSA" [Internet arrives to Cuban households despite ETECSA], *Cubanet*, June 16, 2016, http://bit.ly/2eFWFqw.

18 "El régimen desmantela una red Wi-Fi clandestina en Víbora Park" [Regime dismantles a clandestine Wi-Fi network in Vibora Park], *Diario de Cuba*, May 31, 2014, http://bit.ly/1m8kE92; Sheyla Delgado Guerra, "The "messy" and costly result of illegality," ed. Walter Lippmann, *WalterLippmann* (blog), December 7, 2012, http://bit.ly/1VdF8V6; See also Juan O. Tamayo, "Cuba clamps down on Wi-Fi networks," *Miami Herald*, June 16, 2014, http://hrld.us/1iAp91C.

19 Jack Karsten and Darrel M. West, "Cuba slowly expands Internet access," *Tech Tank* (blog), Brookings Institute, July 2, 2015, http://brook.gs/1KDrxLF.

20 Isbel Díaz Torres, "The Mean Salary of Cubans," *Havana Times*, August 6, 2013, http://bit.ly/2cW21x3.

21 Associated Press, "Cuba lowers prices to Internet access: now an hour costs 10% of monthly salary," *Fox News Latino,* February 19, 2015, http://bit.ly/1G73BiB.

22 "Salas de navegación en Cuba listas para acceso a Internet" [Navegation halls in Cuba ready to Access the internet], *Cubadebate*, June 4, 2013, http://bit.ly/2elWjlt.

23 García, "Internet in Cuba: A Success in Spite of Everything," Translating Cuba, May 29, 2014, http://bit.ly/2esPoW2.

24 Yurisander Guevara, "Wifi en el ambien e," *Juventud rebelde*, June 17, 2015, http://bit.ly/1HW0n5U.

25 Dough Aamoth, "Personal Computers Finally Available in Cuba," *TechCrunch*, May 3, 2008, http://tcrn.ch/1MlKp7n.

26 "Cuban ICT statistics report for 2014," *The Internet in Cuba* (blog), August 22, 2015, http://bit.ly/1Lb11Qd.

connections are explicitly prohibited by Cuban customs regulations.[27] Additional restrictions are placed on modems, wireless faxes, and satellite dishes, which require special permits in order to enter the country.[28]

Although Cuba still has the lowest mobile phone penetration rate in Latin America, the rate is rising due in part to changes in government-imposed restrictions on telecommunications. According to ETECSA, by January 2016, approximately 3.3 million Cubans owned mobile phones lines, or about 30 percent of the population.[29] As the number of mobile phone users has grown, the state-owned ETECSA has begun implementing small changes that benefit use s. In 2012, ETECSA eliminated fees for receiving phone calls from within Cuba, cut the cost of sending a text message (from US$0.16 to $0.09), and reduced the daytime cellphone rates from US$0.60 to $0.35 per minute.[30] In January 2014, ETECSA also announced it would allow balance transfers on cards between prepaid users.[31] In July 2014, ETECSA in turn said that the minimum mobile phone service fee—which had been US$5 per month—would be eliminated.[32]

Despite price cuts and occasional promotions, the cost of mobile service is still too high for the vast majority of Cubans. The government's strategy seems to be predicated on convincing Cuban exiles to pay for these services for their relatives in Cuba—viewed by many as an attempt to attract new funds. Since January 2014, friends and relatives living abroad can use an online service to pay the phone bills of users living on the island.[33] Through this system of refilling c edit on cell phones from outside the country, the Cuban diaspora (including almost three million Cubans living abroad) covers all or part of the cost of cell phone use for their families in Cuba. According to the Miami-based Havana Consulting Group in 2014, 54 percent of mobile payments to ETECSA come from the Cuban diaspora.[34]

Due to second generation cell phone infrastructure, most mobile phone users are unable to browse the web, but it is possible to send and receive international text messages and images with certain phones. Moreover, a growing number of Cubans have more advanced smartphones, often gifts from wealthier relatives living abroad.[35] In March 2014, a new Nauta service was launched, which allows users to send and receive emails on their mobile phones but only with a .cu email account. The cost of the service (US$1 per 1Mb of data transfer) is taken from the mobile phone's credit rather than from the balance of the users' Nauta internet account.[36] Despite the fact that users can only activate this service at few locales in Havana and that it is still very expensive, the service, which is the

27 Cuban Customs Website (Aduana General de la República de Cuba),"Artículos que necesitan autorización a la importación," http://bit.ly/1hbJFOl.

28 Cuban Customs Website (Aduana General de la República de Cuba), accessed September 14, 2016, http://bit.ly/2cZ8Udg.

29 "Cuba cerró el 2015 con más de tres millones de líneas móviles," [Cuba ended 2015 with more than three million mobile lines], *Cuba Debate,* February 5, 2016, http://bit.ly/2cpTnGQ.

30 "Telecoms in Cuba: Talk is cheap," *Americas View* (blog), *The Economist*, January 24, 2012, http://econ.st/1Wn3Nnj.

31 "ETECSA anuncia nuevos servicios para telefonía celular en el 2014" [ETECSA announces new services for cellphones in 2014], *CubaDebate*, January 26, 2014, http://bit.ly/2d0eGuz.

32 "ETECSA Anuncia Eliminación de Pago Obligatorio de Cinco Cuc para Móviles" [ETECSA announces elimination of mandatory payment of 5CUC for mobiles], *On Cuba*, July 3, 2014, http://bit.ly/1Vfj3Af.

33 "ETECSA Informa Nuevos Servicios de Pagos por Internet para Cubanos" [ETECSA announces new internet payment services for Cubans], *On Cuba*, January 20, 2014, http://bit.ly/1G77ggd; José Remón, "ETECSA a la carga: Pagando la factura de mi pariente en Cuba" [Payment the bill for my family member in Cuba], *Café Fuerte*, January 22, 2014, http://bit.ly/1R5LPTs.

34 Andrea Rodriguez, "Cuba mobile email experiment causes chaos," Associated Press in *Yahoo News*, May 16, 2014, http://yhoo.it/1gUEAQU.

35 Andrea Rodriguez, "Cuba mobile email experiment causes chaos," Associated Press in *Review Journal*, May 16, 2014, http://bit.ly/2cKTGqO.

36 Yoani Sanchez, "A Few Days With Nauta," *Translating Cuba* (blog), March 24, 2014, http://bit.ly/1gUENnt.

cheapest option for email to date, quickly proved popular.[37] The Nauta email service has occasionally encountered disruptions, and was temporarily inaccessible for several days in November 2015, which ETECSA attributed to a technical failure.[38]

While some announcements have anticipated increasing connectivity and expanding network capabilities on the island, significant infrastructu e upgrades are still needed, prompting speculation among observers as to whether such plans are realistic. In June 2015, an internal document outlining a national strategy for broadband connectivity in Cuba was leaked online, which outlined an objective to connect 50 percent of households to broadband internet and 60 percent to mobile internet connections by 2020.[39] In February 2016, ETECSA announced a pilot project to provide fibe -optic home internet service in two Havana neighborhoods, operated by Chinese telecom operator Huawei.[40] A more recent report indicated that a free trial would be taking place in Old Havana in August 2016.[41] However, details on the actual implementation of these projects and their potential expansion to other areas remain unknown.

Restrictions on Connectivity

The backbone structure of the internet in Cuba is entirely controlled by the government, and state authorities have the capability and the legal mandate to restrict connectivity at will. At times of heightened political sensitivity, the government has used its complete control of the cell phone network to selectively obstruct citizens' communications. All calls and SMS from dissidents' cell phones are monitored and service is sometimes cut for those working as freelance or citizen journalists voicing views the government does not condone.[42]

ICT Market

While recent years have seen an expansion in the number of internet and mobile phone users, the ICT sector remains dominated by government fi ms. There are only two internet service providers (ISPs) in Cuba: The Center for Automatic Interchange of Information (CENIAI) and ETECSA (sometimes called ENET).[43] Both are owned by the state. Cubacel, a subsidiary of ETECSA, is the only mobile phone carrier.

Following the announcement of a normalization of relations between the United States and Cuba

37 EFE, "Heavy use of Cuba mobile e-mail service strains cellular network," *Fox News Latino,* June 25, 2014, http://bit.ly/1MujoN3.

38 "Cuarto día sin servicio de correo Nauta en toda la Isla" [Fourth day without Nauta email service on the island], *14ymedio,* November 14, 2015, http://bit.ly/2eGqhE6.

39 "ChiriLeak: Hoja de ruta de la Banda Ancha en Cuba," [ChiriLeak: Roadmap for Broadband in Cuba], *La Chiringa de Cuba (blog)*, June 8, 2015, http://bit.ly/2cISJAN.

40 "Cuba says it will launch broadband home internet project," *Associated Press,* February 1, 2016, http://apne.ws/1nZf15t; "Internet in Cuban homes: connection bit by bit," *OnCuba,* February 10, 2016, http://bit.ly/2e6jrGe.

41 "Old Havana fiber trial o begin August 20th? Many unanswered questions," *The Internet in Cuba (blog),* July 29, 2016, http://bit.ly/2cIoCJM.

42 Yoani Sanchez, "Another Tiny Crack in the Wall: Email on Cellphones But State Security Is Likely Reading It," *Latino Voices*, *Huffington Post*, May 24, 2014, http://huff.to/1MNIQjC; See also Yoan David González Milanés, "Cortan el servicio del cellular a periodista independiente de @HablemosPress," *Háblalo Sin Miedo* (blog), January 20, 2012, http://bit.ly/1Lb5oKX.

43 The private fi m Telecom Italia previously held shares of ETECSA until February 2011, when the state-owned company Rafin S.A., a financial m known for its connections to the military, bought Telecom Italia's 27 percent stake for US$706 million. Since then, the telecom company has been completely owned by six Cuban state entities. See: Jerrold Colten, "Telecom Italia Sells Etecsa Stake to Rafin SA For $706 Millio ," *Bloomberg Business*, January 31, 2011, http://bloom.bg/1YFxlyo.

in December 2014, regulatory amendments have opened the way for U.S. ICT companies to start offering services to the island. Showcasing U.S. business interest in penetrating Cuba's ICT market, in March 2015, IDT Corp reached the first U.S. deal with ETECSA to provide direct international long distance calls between Cuba and the United States.[44] In September 2015, Verizon was the first U.S.-based wireless company to offer roaming in Cuba, quickly followed by Sprint and others.[45] Companies whose services are closely related to internet use, such as MasterCard, Airbnb, or Netflix, also announced their entrance into the Cuban market.[46] In March 2016, PayPal also announced it would start offering money transfer services to and from Cuba.[47]

However, large-scale offers to expand internet access on the island have faced more skepticism. In June 2015, Google reportedly offered to quickly expand Wi-Fi internet access across the island.[48] Demonstrating lingering distrust, the only official Cuban reference to the proposal was a statement by Ramón Machado Ventura, first secretary of the Communist Party, in July 2015: "We must have internet, but our way, knowing that the intention of imperialism is to use the internet in another way, to destroy the Revolution."[49]

These developments come after a period of domestic changes in Cuba, as the government began implementing limited market reforms. Restrictions on private enterprise were eased under the 2012 "update" of Cuba's economic model. Recent data from the Cuban National Statistics Office reports a near tripling of registered .cu domain between 2012 and 2014, which may reflect the growing use of websites by companies after laws permitting private sector businesses were liberalized.[50] Although proposed reforms did not initially extend to the communications sector,[51] in November 2013, ETECSA announced that it would allow private workers to market local and long-distance telephone services to the population as self-employed communications agents. The agents may also sell prepaid cards for fixed and mobile telephone services and internet access.[52] The Cuban government also began to allow the limited creation of private cooperatives by computer science graduates in 2012, but tight internet restrictions, along with prohibitively high computer and software pricing, resulted in a nonexistent official market, although a black market for such commodities exists.[53]

Regulatory Bodies

No independent regulatory body for managing the ICT sector exists in Cuba. In 2000, the Ministry of Informatics and Communication (MIC) was created to serve as the regulatory authority for the internet. Within the MIC, the Cuban Supervision and Control Agency oversees the development of internet-related technologies.[54]

44 Mini Whitefield, "First U.S. telecom company connects directly with Cuba," *Miami Herald*, March 6, 2015, http://hrld.us/1NsaxN3.

45 "Competition heats up for roaming, calling services in Cuba," *Miami Herald,* May 10, 2016, http://hrld.us/1qcuP5g.

46 Associated Press, "Airbnb moves into Cuba to start home," *CBC News,* April 2, 2015, http://bit.ly/1MNKSjG.

47 "PayPal Brings Money Transfers to Cuba," *Fortune,* March 21, 2016, http://for.tn/1qr1GEz.

48 "Sources: Google offered Cuba expansion of web access," *Miami Herald,* July 2, 2015, http://hrld.us/1NAJ227.

49 "Top Cuban Official Rejects Nongovernment Wi-Fi Offerings," *Newsweek,* July 13, 2015, http://bit.ly/1O7IRw3.

50 Oficina Nacional de Estadística e Información, *Tecnología de la Información y las Comunicaciones (TIC)*, August 2015, http://bit.ly/2cwntFX; "Cuban ICT statistics report for 2014," *The Internet in Cuba* (blog), August 22, 2015, http://bit.ly/1Lb11Qd.

51 Nick Miroff, "Cuba is Reforming, but Wealth and Success are Still Frowned Upon," *Business Insider*, September 4, 2012, http://read.bi/1OX6fPk.

52 "Communication agents will see telephone and Internet time," *The Internet in Cuba* (blog), November 27, 2013, http://bit.ly/1G7d5dB.

53 "Se Buscan Socios," *Juventud Rebelde*, December 15, 2012, http://bit.ly/2cUAN73.

54 For the website of The Ministry of Informatics and Communications, see: http://www.mincom.gob.cu/

Limits on Content

Cuban law places strict limits on free speech and outlaws independent media. Although many foreign news websites are accessible from internet access points, websites focused on Cuban news and websites from Cuban dissidents or expats are often blocked. Various institutions, such as universities, further restrict content by frequently blocking social media sites. Despite connectivity limitations, Cubans have been able to access content through improvisational underground networks and USB flash drives containing content downloaded from the internet. Several independent web-based information sites have also emerged, offering alternative discourses about the Cuban reality.

Blocking and Filtering

Rather than relying on the technically sophisticated fil ering and blocking used by other repressive regimes, the Cuban government continues to limit users' access to information primarily via lack of technology and prohibitive costs. Restrictions on email in the workplace, however, have been growing in recent years, and dissident websites and blogs continue to be subject to periodic disabling or blocking. Moreover, a series of recent tests conducted by *14ymedio* found that ETECSA's cellphone network, Cubacel, has been systematically fil ering domestic SMS containing specific ords, such as references to "democracia" (democracy) and "derechos humanos" (human rights).[55]

The wording of certain government provisions regarding content regulation is vague and allows for a wide array of posts to be censored without judicial oversight. Resolution 56/1999 stipulates that all materials intended for publication or dissemination on the internet must fi st be approved by the National Registry of Serial Publications.[56] Meanwhile, Resolution 179 (2008) authorizes ETECSA to "take the necessary steps to prevent access to sites whose contents are contrary to social interests, ethics and morals, as well as the use of applications that affect the integrity or security of the state."[57]

The websites of foreign news outlets—including the British Broadcasting Corporation (BBC), *El País*, the *Financial Times,* and *El Nuevo Herald* (a Miami-based Spanish-language daily)—are accessible in Cuba. However, ETECSA commonly blocks dissident or independent news sites, such as *Cubanet*, *Penúltimos Días*, *Diario de Cuba*, *Cubaencuentro*, *Hablemos Press*, and *14ymedio*.[58] The sites of some Cuban activists and dissident organizations based on the island, such as the Patriotic Union of Cuba (UNPACU), the Christian Liberation Movement (MCL), and the civic project Estado de SATS, also face blocking. Revolico, a platform for posting classified ad ertisements for products circulating on the black market was only recently unblocked, according to reports in August 2016.[59] Beginning in 2007, the government systematically blocked core internet portal sites such as Yahoo, MSN, and Hotmail.

55 "Cubacel censura los SMS con las palabras "democracia" o "huelga de hambre"" [Cubacel censors SMS with the words "democracy" and "hunger strike"], *14ymedio*, September 3, 2016, http://bit.ly/2bS1VE2.

56 Ministerio de Cultura, Resolución No. 56/99, *Las Publicaciones Seriadas Cubanas*, http://bit.ly/2cIwMlL.

57 Resolution 179 (2008), http://bit.ly/2cAH6wF

58 "Cuba internet access still severely restricted," *BBC News,* March 21, 2016, http://bbc.in/2d11BG9; See also: "Cubans are using simple hacks to get around limited and expensive internet," *Quartz,* August 21, 2016, http://bit.ly/2bDxE9F; "El Wi-Fi público les da una primera prueba de Internet a los Cubanos," [Public Wi-Fi gives Cubans a fi st internet trial], *Wall Street Journal*, August 21, 2015, http://bit.ly/2d97v6L .

59 "El Gobierno levanta la censura contra Revolico" [Government lifts censorship against Revolico], *14ymedio,* August 12, 2016, http://bit.ly/2eH7pVK; See also: Jason Koebler, "Cuba's Black Market Is a Website That Exists Primarily Offline" *Motherboard* (blog), *Vice*, August 27, 2015, http://bit.ly/1Q3uKJf.

As of 2015, some of these sites remain blocked in some government institutions,[60] although they are largely accessible from hotels.

Blocking occurs not only at the national level but also at the level of various intranet networks and at access points. In March 2015, the Nauta intranet banned Larry Press' blog, *The Internet in Cuba*, one of the best sources about Cuban ICTs.[61] In January 2015, the University of Computer Sciences (UCI) banned Fernando Ravsberg's blog *Cartas desde Cuba*, which had been hosted on the *BBC Mundo* platform from 2008 to 2013 until becoming independent.[62]

Social-networking platforms such as Facebook and Twitter are sometimes blocked at certain universities and government institutions, but may be accessed—with consistent monitoring and varying reliability—from Wi-Fi hotspots, some cybercafes and hotels. Restrictions continued to inhibit the use of certain Voice over Internet Protocol (VoIP) services such as Skype, although VoIP is not blocked at Wi-Fi hotspots and apps such as IMO have become a popular way to video chat with relatives abroad.[63] In recent years, the government also increased its control over the use of email in official institutions, installing a platfo m that restricts spam and specifically p events the transmission of "chain letters critical of the government."[64]

Content Removal

While ETECSA does not proactively police networks and delete content, a recent report about the government-sponsored blog platform, Reflejos [65] denounced that several blogs hosted on the platform, under the cubava.cu domain, had been censored, either because they did not fit certain "Terms of Use" or because connectivity levels are so low that authors are unable to update their sites, which also causes permanent suspension.[66]

In February 2016, Cuban blogger Yasmín Silvia Portales Machado reported on her Twitter account that a blog on sexual diversity called "Proyecto Arcoiris" (Rainbow Project) was censored by Reflejos. Platform moderators claimed that the blog was censored because a specific aragraph "slandered the Revolution" and therefore violated the website's rules. The paragraph in question referred to labor camps that existed in Cuba from 1965 to 1968, where thousands of men were imprisoned, mainly accused of homosexuality.[67]

Yoani Sánchez's *14yMedio* blog was also removed permanently from Reflejos in Ma ch 2015. Al-

60 Sociedad Interamericana de Prensa, Inc., (Inter American Press Association), "Cuba," in *Reports and Resolutions*.

61 "If you are reading this, you are probably not in Cuba," *The Internet in Cuba* (blog), March 30, 2015, http://bit.ly/1Wnebvj.

62 Fernando Ravsberg, "La UCI censura "Cartas desde Cuba"," *Cartas Desde Cuba* (blog), January 29, 2015, http://bit.ly/1Kzr3t5; See also Cuba Red, "Otra censura. Fernando Rasverg.Increible," posted by elapap, February 2, 2015, http://bit.ly/2d4rMf5.

63 "The Cuban Internet: Letter from Havana," *Foreign Affairs,* April 19, 2016, http://fam.ag/2cV544o; see also: Sayli Sosa, "IMO in Cuba: Shortening Distances Between Relatives," *Havana Times*, July 30, 2015, http://bit.ly/2e7qezq.

64 "Cuba Anuncia Cambio de Platforma Estatal para Correos Electronicos," [Cuba Announces Statewide Change to Email Platform], *Café Fuerte,* August 31 2012, http://bit.ly/RqHp8C.

65 Reflejos is a go ernment-sponsored platform for blogs created and managed within Cuba. It belongs to the Youth Club of Computing and Electronics (JCCE), an institution of the national Ministry of Communications.

66 María Matienzo Puerto, "Guerra contra las subculturas en la plataforma 'Reflejos'" [ar against the subcultures on the plaform Reflejos], *Diario de Cuba*, June 20, 2016, http://bit.ly/2d6Lfrh; See also: "Censura en Cuba se cobra otra víctima en la plataforma bloguera," [Censorship in Cuba claims another victim on blogging platform], *Cibercuba*, May 3, 2016, http://bit.ly/2cIgd7V.

67 "An LGBT Blog Is Suspended Over Mention of Cuba's 1960s-Era Labor Camps," *Global Voices*, February 11, 2016, http://bit.ly/2d6KIG0.

though the government said that there were no prohibited topics on the platform, which was open to all Cuban users, they required bloggers to register with information cards and prohibited the publication of unlawful or counter-revolutionary content. During the short time in which it was active, Sanchez's blog published a variety of content that ranged from cultural commentary to recipes to opinion columns.[68]

Media, Diversity, and Content Manipulation

Cuba has one of the most restrictive media environments in the world. The constitution prohibits privately owned media, and restricts any speech that is deemed counter-revolutionary. The government closely monitors users who post or access political information online and delivers harsh penalties to those it perceives as dissidents. Demand for access to content among the Cuban population, however, has led to elaborate underground networks of internet access.

The cost of access to technologies that facilitate information sharing continues to be high, and the Cuban government has pursued individuals who violate telecommunications access laws. Nonetheless, many Cubans find ways o access restricted content, and a vibrant community of bloggers in Cuba utilizes the medium to report on conditions within the country. Cubans are often able to break through infrastructural blockages by building their own antennas, using illegal dial-up connections, or developing blogs on foreign platforms. There is also a thriving improvisational system of "sneakernets," in which USB flash dri es and data discs are used to distribute materials (articles, prohibited photos, satirical cartoons, video clips) that have been downloaded from the internet or stolen from government offices [69] The "Paquete Semanal" ("Weekly Package") has become a popular offline al ernative for accessing music, movies, TV series, mobile phone apps, magazines and classifieds [70]

Despite severe censorship in official media, some jou nalists have started using the internet to disseminate content that the official p ess is reluctant to publish. In May 2014, Yoani Sánchez launched an independent online news site, *14ymedio*. Although the site is blocked in Cuba, the editorial team is able to post content by emailing it to friends abroad. Users access content from the site through proxies and offline ersions that are shared via USB flash dri es.[71] While the government policy on political content is still very restrictive, this past year has seen a significant change in the number f sites and independent information produced by Cubans, although not necessarily linked to political themes or opposition groups. Sites such *Periodismo de Barrio* and *El Estornudo* have produced critical reports, while other media sites (*El Toque, Vistar Magazine, OnCuba*) have provided information on various topics, entertainment, and cultural programming, expressing a multitude of views on social issues in Cuba today.[72]

On the other hand, the government has tried to direct popular demand for videos, games, and on-

68 14ymedio, "Web Platform Reflejos Closes the '14ymedi ' Blog," *Translating Cuba*, March 27, 2015, http://bit.ly/1QD7dhM.

69 Jonathan Watts, "Cuba's 'offline in ernet': no access, no power, no problem," *The Guardian*, December 23, 2014, http://gu.com/p/44dcf/stw; See also: Emilio San Pedro, "Cuban internet delivered weekly by hand," *BBC*, August 10, 2015, http://bbc.in/1TjpO8x; Jack Karsten and Darrel M. West, "Cuba slowly expands Internet access," *Tech Tank* (blog), Brookings Institute, July 2, 2015, http://brook.gs/1KDrxLF.

70 "Cuban internet delivered weekly by hand," *BBC News,* August 10, 2015, http://bbc.in/1TjpO8x.

71 Tiffany Pham, "How She Did It: Yoani Sánchez Launches Cuban News Outlet 14ymedio," *Forbes*, November 30, 2014, http://onforb.es/1yz5eDp.

72 Daniel Wizenberg, "New Cuban journalism emerges on the internet, beyond the official and opposition media" *Journalism in the Americas (blog)*, July 20, 2016, http://bit.ly/29Zw3tO; See also: "Millennials lead private media opening in Communist-run Cuba," *Reuters,* September 16, 2016, http://reut.rs/2cvgQnk.

line social networking to government-controlled platforms. Following in the footsteps of other repressive regimes contending with a highly literate and digitally interested audience, the government launched its own copycat versions of popular websites, such as Wikipedia, Twitter, and Facebook. This allows the government to direct citizens to closely monitored, censored versions of these platforms. In 2010 the government launched Ecured, a copycat version of Wikipedia,[73] and in 2013 they launched the social networking site *La Tendedera*, which is accessible from youth centers.[74] In March 2015, the Cuban government launched the blogging platform Reflejos, whe e content can only be published from a Cuban IP.[75]

A report on digital journalism published by *Fundación Telefónica* also notes how Cuban authorities have activated "defense mechanisms" online, by accusing critical and independent sites of perpetrating a constant media campaign against the island. The authors explain how such a narrative "converts independent voices into 'mercenaries' or traitors, with the ultimate objective of criminalizing dissent." A product of this "cyberwar" is the creation of networks of progovernment journalists nicknamed "El Enjambre" ("The Hive") who disseminate content online to counter alternative discourses about the Cuban reality.[76]

Digital Activism

Along with low internet penetration, social media access continues to be limited and Cubans have not been able to organize large-scale campaigns around political objectives. Available at Wi-Fi hotspots, Facebook has become a popular platform for social networking, while other platforms such as Twitter are less widely used.[77] New initiatives to create platforms for free speech and information access—such as the creation of the fi st public Wi-Fi network in the studio of artist Kcho, with government permission, and the emergence of independent information sites—have tested the boundaries of the government's restrictions on speech over the past year.

Political activists seeking to raise further awareness via social media, however, have encountered government clampdowns. Cuban activists inside and outside Cuba launched the campaign #TodosMarchamos (We All March) in mid-2015 to denounce human rights violations on the island and recurring repression against the "Ladies in White," a dissident group that protests against the Cuban government every Sunday.[78] Members of #TodosMarchamos have been arrested during protests, including ahead of President Obama's visit to Cuba in March 2016.[79]

In December 2014, in the aftermath of pronouncements by President Obama and President Raul Castro about a rapprochement between the United States and Cuba, performance artist Tania Bruguera published a public letter to the two presidents and the Pope in which she proposed relocating

73 "Ecured is Not Open like Wikipedia," *The Internet in Cuba* (blog), December 21, 2011, http://bit.ly/1FyuMI7.

74 "Rouslyn Navia Jordán, "Una Tendedera para interconectarnos," *Juventud Rebelde*, December 3, 2014, http://bit.ly/1YFFfbl.

75 Dirección de Comunicación Institucional Joven Club, "La plataforma de blog "Reflejos" tu o hoy su lanzamiento oficial en el Palacio Central" [Reflejos blog platfo m officially launched oday at the Central Palace], news release, Ministry of Communications, March 18, 2015, http://bit.ly/1NRxREB.

76 Ramón Salaverría ed., "Ciberperiodismo en Iberoamérica," *Fundación Telefónica*, February 2016, http://bit.ly/1ZZQE5i.

77 A survey conducted by Ding found that 95 percent of users go on Facebook for social purposes at local Wi-Fi hotspots: "New survey finds 70% f Cuban internet users use local Wi-Fi hotspots every week," *Ding,* June 7, 2016, http://bit.ly/2cInNiz.

78 "Activistas organizan un 'tuitazo' para denunciar la represión del régimen," [Activists organize a Twitter campaign to denounce the regime's repression], *Diario de Cuba*, May 30, 2015, http://bit.ly/2d9o0zZ.

79 "'The oppression is high': Cuban police break up protest ahead of Obama's visit," *The Guardian*, March 20, 2016, http://bit.ly/2cG20d5; See also: "Decenas de detenidos durante jornada de "Todos Marchamos"" [Dozens detains during Todos Marchamos day], *Cubanet,* February 14, 2016, http://bit.ly/2cm10Mq.

her 2009 performance *Tatlin's Whisper #6* to the Plaza of the Revolution, thereby offering an open mic to the Cuban citizenry to express their views about their country's future.[80] Her project used the hashtag *#YoTambienExijo* (I Also Demand) on social media platforms to promote the performance from outside the island. Upon traveling to Havana on December 26, however, she was summoned to a meeting with government officials and old that she did not have authorization for the performance. When she publicly stated that she intended to go ahead with the performance, she was detained by authorities, along with a number of other online and offline activists who exp essed support for her project (see Prosecutions and Detentions for Online Activities).

Violations of User Rights

Cuba outlaws a wide range of speech deemed to be counter-revolutionary or a threat to the public order. In recent years, the Cuban government has moved from issuing long, multi-year sentences to using short term detentions as a means of harassing independent journalists and bloggers. Several episodes of censorship and intimidation against bloggers and independent journalists were reported during this coverage period.

Legal Environment

The Cuban legal structure is not favorable to internet freedom. The constitution explicitly subordinates freedom of speech to the objectives of a socialist society, and freedom of cultural expression is guaranteed only if such expression is not contrary to "the revolution."[81] The penal code (Law 62, Fifth Section) sets penalties ranging from a few months to 20 years in prison for any activity considered to be a threat to the Cuban state or public order, including a provision that authorizes the state to detain, reeducate, or monitor anyone who shows a "proclivity to commit crimes" by violating the norms of the socialist society.[82] Meanwhile, the Law to Protect Cuba's National Independence and Economy (Law 88), passed in 1999, punishes any activity that threatens Cuban sovereignty or facilitates the U.S. blockade. Anyone who passes information to the U.S. government that could bolster the blockade can face up to 15 years in prison. Spreading subversive materials can incur a penalty of three to eight years in prison, while collaborating with foreign media outlets is punishable by up to fi e years in prison.[83]

In 1996, the government passed Decree-Law 209, which states that the internet cannot be used "in violation of Cuban society's moral principles or the country's laws," and that email messages must not "jeopardize national security."[84] In 2007, a network security measure, Resolution 127, banned the use of public data-transmission networks for the spreading of information that is against the social interest, norms of good behavior, the integrity of people, or national security. The decree requires access providers to install controls that enable them to detect and prevent the proscribed activities,

80 Coco Fusco, "The State of Detention: Performance, Politics, and the Cuban Public," *e-flux* 60 (2014), http://bit.ly/1YFFfbl.

81 Constitution of the Republic of Cuba, 1992, art. 53 and 39(d), accessed September 1, 2015, http://bit.ly/2cIwwTN.

82 Código Penal [Penal Code], art. 72 and 91, http://bit.ly/2cIwwTN.

83 Committee to Protect Journalists, "International Guarantees and Cuban Law," trans. María Salazar, March 1, 2008, http://bit.ly/1hbJO4p.

84 Reporters Without Borders, "Going Online in Cuba: Internet under Surveillance," October 2006, http://bit.ly/1f4pnF0; See also Decreto 209 (Decree 209), September 13, 1996, http://bit.ly/1VdG1Nk.

and to report them to the relevant authorities.[85] Furthermore, access to the internet in Cuba generally requires complete identification, hindering anonymity nearly impossible.[86]

Prosecutions and Detentions for Online Activities

Under Raúl Castro, the Cuban government appears to have shifted its repressive tactics from long-term imprisonment of bloggers to short-term detentions, interrogations, and legal harassment.[87] Reporters associated with independent online newspapers or forums, including *Hablemos Press,* Somos Mas, Foro por los Derechos y Libertades or UNPACU have faced significant harassment.

On February 17, 2016, independent journalist Juan Carlos Fernández was arrested in Pinar del Río province. Four agents from the political police (Seguridad del Estado) threatened him with prosecution under Law 62 of the Criminal Code, for the offense of "professional intrusion." The agents also said that the journalist's computer would be confiscated "the next time we see you on the street reporting something," and defined as illegal the two information projects Recio contributes to: independent newspaper *14ymedio* and magazine *Convivencia* (see also Intimidation and Violence).[88]

Short-term arrests and detentions of activists tend to increase surrounding key political and social events. Coinciding with Pope Francis' visit to Cuba in the month of September 2015, the dissident group Cuban Commission for Human Rights and National Reconciliation (CCDHRN) registered 882 arbitrary arrests and detentions.[89] Continuing an upward trend in recent years, these numbers were again exceeded in November 2015 with 1,447 reported arrests, and in March 2016, CCDHRN recorded 1,416 cases, with 498 of these taking place during President Obama's visit to the island.[90] In December 2015, UN High Commissioner for Human Rights Zeid Ra'ad Al Hussein expressed concern with such high numbers of arbitrary arrests and short-term detentions.[91] Bloggers and online activists are often caught up in such crackdowns. Because it is difficult to distinguish between independent blogging and political activism in Cuba, however, it is often impossible to accurately pinpoint whether detentions were in retaliation for online speech specifically.

The government has also prosecuted individuals associated with underground cyber-networks. In 2012, the government opened a criminal investigation of two highly profitable cyber-networks illegally using ETECSA's fixed and mobile networks. The defendants, who are being prosecuted for illegal economic activity and fraud, face fines coupled with sentences of three to 10 years in prison.[92] In May 2014, Cuban authorities raided and seized equipment from another underground Wi-Fi network with 120 members.[93]

85 Giovanni Ziccardi, *Resistance, Liberation Technology, and Human Rights in the Digital Age*, (Netherlands, Springer, 2013) 220.

86 Isbel Diaz Torres, "Wi-Fi for Cubans and Mobile E-Mail Service," *Havana Times*, March 10, 2014, http://bit.ly/1G7q7b7.

87 Human Rights Watch, "Cuba," in *World Report 2016,* accessed September 18, 2016, http://bit.ly/1ZNmEc1; See also: Committee to Protect Journalists (CPJ), *After the Black Spring, Cuba's New Repression*, July 6, 2011, https://cpj.org/x/4472.

88 Juan Carlos Fernández, "Hora y media con el Gran Hermano" [An hour and a half with the Big Brother], *14ymedio*, February 18, 2016, http://bit.ly/2cKdFWH.

89 "Comisión opositora denuncia 882 detenciones políticas en Cuba en septiembre," [Opposition Commission denounces 882 political detentions in Cuba in September], *El Nuevo Herald,* October 5, 2015, http://hrld.us/2cHtK2O.

90 "La CCDHRN denuncia 498 arrestos políticos en Cuba durante la visita de Obama" [CCHHRN denounces 498 political arrests in Cuba during Obama visit], *14ymedio,* April 4, 2016, http://bit.ly/1XeGVWS.

91 "UN Human Rights Chief urges Cuba to halt harassment of civil society activists," OHCHR, December 15, 2015, http://bit.ly/2dbmLQy.

92 Sheyla Delgado Guerra, "The "messy" and costly result of illegality," ed. Walter Lippmann, *WalterLippmann* (blog), December 7, 2012, http://bit.ly/1VdF8V6.

93 Juan O. Tamayo, "Top Dissidents Detained in Cuba," *Miami Herald*, June 11, 2014, http://hrld.us/2cRiQrM.

Despite the continued policy of legal harassment and detentions of bloggers, the government recently released two prominent political prisoners. In July 2015, the government released the well-known blogger and writer Ángel Santiesteban Prats, who had been jailed on trumped-up charges since early 2013.[94] Santiesteban was arrested in connection with his political views several times prior to his December 2012 trial. Such harassment increased after Santiesteban's creation of the blog *The Children No One Wanted*, in which he criticized the government. Santiesteban reported mistreatment and torture during his imprisonment.[95] In December 2014, as part of negotiations with the United States, the Cuban government released the American USAID contractor Alan Gross, who had been held for over fi e years on charges that he distributed illegal communications technology to Cubans.[96]

Surveillance, Privacy, and Anonymity

Surveillance of ICTs in Cuba is widespread, and dissident bloggers are subject to punishments ranging from fines and sea ches to confiscation f equipment and detentions. Anonymity and encryption technologies are strictly prohibited in Cuba,[97] and web access points, such as Wi-Fi hotspots, cybercafes and access centers, are closely monitored and users are required to register with their identification information.[98]

Despite constitutional provisions that protect various forms of communication and portions of the penal code that establish penalties for the violation of the secrecy of communications, users' privacy is frequently violated. Tools for content surveillance are likewise pervasive. Under Resolution 179/2008, ISPs are required to register and retain the addresses of all traffic for at least one ear.[99] The government routes most connections through proxy servers and is able to obtain all user names and passwords through special monitoring software called Avila Link, which is installed at most ETECSA and public access points.[100] In addition, delivery of email messages is consistently delayed, and it is not unusual for a message to arrive censored or without its attachments.

Web use at Wi-Fi hotspots and "navigation halls" remains tightly controlled. A recent decree from the Ministry of Communications reaffi med the government's continued monitoring of internet traffic, stating that ETECSA will immedia ely end a user's access if he or she commits "any violation of

94 Angel Santiesteban, "#PapaEnCuba [Pope in Cuba]: A Shout for Danilo Maldonado (El Sexto)," trans. Alicia Barraqué Ellison, *Translating Cuba* (blog), April 23, 2013, http://bit.ly/1iQgV6c ; See also: Angel Santiesteban, "Prison Diary VI: Inside View of the Trial," *Translating Cuba* (blog), March 28, 2013, http://bit.ly/1KHj6Q9.

95 Reporters Without Borders, "Dissident Blogger Completes Year in Detention," February 28, 2014, http://bit.ly/1JtNknT.

96 Julie Hirschfeld Davis, "Alan P. Gross Gains the Freedom from Cuba He Thought Would Never Come," *The New York Times*, December 17, 2014, http://nyti.ms/1KDBPLF.

97 According to the Cuban Mission to the United Nations, encryption is only permissible if authorized by the Ministry of Communications and the Ministry of the Interior. Letter from the Permanent Mission of Cuba to the ONU to the High Commission on Human Rights, 2015, República de Cuba Misión Permanente ante la Oficina de las Naciones Unidas en Ginebra y los Organismos Internacionales con sede en Suiza, "Nota No. 211/2015," [Note No. 211/2015], http://bit.ly/1JtNsUE; See also: Rolando Cartaya, "Crítica Relator de ONU Control a Cifrado de Datos Personales en Cuba," *MartiNoticias*, June 24, 2015, http://bit.ly/1R5ZzgY.

98 Ellery Roberts Biddle, *Rationing the Digital: The Policy and Politics of Internet Use in Cuba Today*, July 2013, Internet Monitor (The Berkman Center for Internet & Society), http://bit.ly/1LCRoID; See also Isbel Diaz Torres, "Wi-Fi for Cubans and Mobile E-Mail Service," *Havana Times*, March 10, 2014, http://bit.ly/1G7q7b7; See also Yoani Sánchez, "Unos días con nauta," *14ymedio* (blog), March 24, 2015, http://bit.ly/1G7q7b7.

99 José Cuervo, "Resolución n˚ 179/2008 Proveedores de servicios de acceso a Internet al público," *Informática jurídica*, February 16, 2015, http://bit.ly/1PC8Vjg.

100 Lorenzo Franseschi-Bicchiera, "The Internet in Cuba: 5 Things You Need to Know," *Mashable*, April 3, 2014, http://on.mash.to/1Fmi1Rg /; Infosurgents: Tracking the Information Revolution, "Internet Filtering" University of Michigan, http://bit.ly/1KHrM9m.

the norms of ethical behavior promoted by the Cuban state."[101] Users must show their national ID cards and sign an agreement stating that they will not use the service for anything "that could be considered …damaging or harmful to public security"—a vague term that could presumably extend to political dissent.[102] Wi-Fi hotspots similarly prompt users to enter their national ID numbers.

If users attempt to send an email with attachments, ETECSA's own NAUTA interface system greets them with a pop-up window reminding them that "other people may see what you are sending" and asking if they wish to continue. Although the pop-up window is marked "Internet Explorer" and appears to be a real message generated by the search engine, several Cuban online users have said that they had never seen such a message when using internet cafes in Havana's tourist hotels. Such claims suggest that ETECSA may have programmed computers at its new access points to prompt users as a reminder that the government is monitoring their online activities.

Intimidation and Violence

Although the majority of cases of physical violence against activists in Cuba appear to be in retaliation for public protests rather than online activity, prominent online users have faced violence from police forces, and users who have been jailed for extended periods of time report being mistreated and tortured. For example, In March 2016, the Cuban blogger and activist Valle Roca, who runs the blog *Yurielconteston* and a YouTube channel, was beaten while covering a protest by the Ladies in White group and detained for fi e days. This was not the fi st time he had been targeted while covering protests.[103]

Those jailed for their online activities have also denounced abuse and harsh prison conditions. Released in July 2015, the prominent blogger Ángel Santiesteban Prats, who was jailed on trumped up charges, reported severe mistreatment and torture during his detention.[104]

Technical Attacks

Technical attacks do not appear to be a primary method of censorship in the country, but have targeted some online outlets. In May 2014, *14ymedio* was hacked one day after it was launched. Users who tried to access the site were redirected to a site called Yoani$landia, which insulted the director of the outlet, Yoani Sánchez.[105] The site was restored shortly after the hack.

101 Gaceta Oficial de la epública de Cuba Ministerio de Justicia, Resolución No. 197/2013, http://bit.ly/2cAsf92.

102 Ibid.

103 Committee to Protect Journalists, "Cuban blogger jailed for fi e days after trying to cover protest," March 26, 2016, http://bit.ly/2cwBr8M.

104 Reporters Without Borders, "Ángel Santiesteban-Prats (Cuba) en libertad condicional desde julio de 2015" [Ángel Santiesteban-Prats (Cuba), conditionally released since July 2015], http://bit.ly/2cwD8Di.

105 Associated Press, "'Hackeado' portal digital de la bloguera cubana Yoana Sánchez," *Miami Diario*, May 21, 2015, http://bit.ly/1R6cway; See also: Amnesty International, "Cuba," *Amnesty International Report 2014/15*, http://bit.ly/1Bm8EI5.

Freedom House

Ecuador

	2015	2016
Internet Freedom Status	Partly Free	Partly Free
Obstacles to Access (0-25)	8	8
Limits on Content (0-35)	11	12
Violations of User Rights (0-40)	18	21
TOTAL* (0-100)	**37**	**41**

* 0=most free, 100=least free

Population:	**16.1 million**
Internet Penetration 2015 (ITU):	**49 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- The use of copyright infringement notices to take down content critical of the government has become common practice. While a Spanish fi m acting on behalf of Ecuador's public institutions has been behind many of these requests, government institutions have also started to issue removal requests claiming copyright infringement (See **Content Removal**).
- Defamation lawsuits and frequent verbal attacks continued to threaten critical commentary online, and two politicians were sentenced to 15 and 30 days in jail for their comments on social media (**Prosecutions and Detentions for Online Activities**).
- Evidence mounted that Ecuador's government engages in surveillance of a wide range of individuals, as leaked documents have exposed illegal spying on politicians, journalists and activists (see **Surveillance, Privacy and Anonymity**).
- Several online news outlets suffered cyberattacks after publishing articles detailing the links between Ecuador's intelligence agency and Hacking Team, and others were attacked while covering antigovernment protests in June 2015 (see **Technical Attacks**).

Introduction

Ecuador's internet freedom climate deteriorated during this period, threatened by politically motivated content removals, frequent legal and verbal attacks against government critics online, and cyberattacks against news sites.

While internet access continued to increase over the past year, Ecuador's a contradictory position on internet freedom has become more pronounced. The government of President Rafael Correa, who came into power in 2007, has been an early adopter of information technology, and online platforms played a central role in the party's initial election campaign. Through its Ministry of Telecommunications, the government has engaged in widespread campaigns to improve internet access and digital literacy all over the country. The protection of foreign whistleblowers such as Julian Assange (despite recent tensions)[1] and Edward Snowden, who was granted safe passage in order to travel to Russia, have given Ecuador fame as a defender of internet freedom. However, this image contrasts with the reality at home.

Heavy control on the printed press has been slowly transitioning to the online world. Takedowns, cyberattacks and phishing malware are part of the everyday lives of activists, journalists and political dissidents. The government has not been proactive in defending citizens against these threats; instead, it has actively exerted control over the digital space. The abuse of copyright infringement notices, progovernment troll centers, and heavy sanctions for private media under the 2013 Communications Law all continued to present limits on content. President Correa has repeatedly encouraged the public to "use the law" against his critics on social media and to dox users who insult him.

Moreover, a series of leaks have provided compelling evidence of active monitoring of the public web and government targeting of opposition figu es for surveillance. Legal actions against alternative media because of their posts on blogs, Facebook and Twitter also point to active monitoring of the online sphere.

Obstacles to Access

Internet access continued to increase during this coverage period. The quality of service has improved and become more readily available with the expansion of 4G technology. However, zero-rating programs have drawn criticism over uneven access to online content and applications as the current legal framework has proven to be ineffective in defending net neutrality. Legislation approved in early 2015 has raised questions about the independence of the new regulatory body, as well as the scope of a provision that grants the government the power to take over telecommunications services in times of national emergency.

Availability and Ease of Access

Internet access in Ecuador has steadily increased in the last few years. The Pacific Caribbean Cable System (PCCS), a new high speed fibe -optic cable completed by a consortium of operators in Au-

1 Nick Miroff, "Ecuador cuts off Internet access for WikiLeaks founder Julian Assange," *The Washington Post,* October 19, 2016, http://wapo.st/2ejNvA6.

gust 2015,[2] represents part of a larger advance in infrastructure improvements in Ecuador. As the country's fibe -optic cabling continued to expand from 45,000 km in 2015 to 59,861 km in 2016,[3] PCCS is expected to multiply local internet consumption capacity by 60.[4]

As of 2015, the International Telecommunications Union (ITU) measured internet penetration in Ecuador at 48.9 percent, compared to 45.6 percent in 2014 and 35 percent in 2012.[5] According to an Akamai report from the fi st quarter of 2016, Ecuador's average internet speed was 5.3 Mbps.[6]

Multiple internet subscription options are available. Broadband (commonly used in urban zones) and satellite connections (often used in rural areas) have become increasingly popular in recent years. According to the Agency for Regulation and Control of Telecommunications (ARCOTEL), 9.4 percent of the population had fi ed internet subscriptions at the end of 2015, while 38 percent had mobile internet subscriptions.[7]

Although mobile phones continued to be taxed as luxury items along with other electronic devices such as computers and tablets,[8] there were 12.8 million mobile phone subscriptions in 2015, representing 79.4 percent of the population.[9] In December 2015, the government relaxed import quotas by allowing every user to import a phone valued up to US$ 2,000 every year.[10] For local cell phone assemblers, tariffs dropped from 3 to 1 percent. However, mobile internet penetration continued to be unevenly distributed, as the richest 20 percent of the population owned 60 percent of smartphones.[11] Cell phones, along with clothing, are the biggest market for contraband in the country.[12]

In early 2015, Movistar and Claro reached a deal with the government to access the radio frequency bands to improve 3G connectivity and install 4G services, in exchange for paying over US$ 300 million and improving 3G coverage. This contract will expire in 2023 and is expected to reach more individuals than previous attempts to introduce 4G technology.[13] Government data for 2015 shows 7.5 percent using 4G technology,[14] which is available in 49.6 percent of the territory.[15] These numbers

2 Sofía Ramírez, "Un nuevo cable submarino se instala," [A new undersea cable is installed], *El Comercio*, Quito, July 14, 2015, http://bit.ly/2dv79sA.

3 Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL), "Seguimos creciendo en el despliegue de las telecomunicaciones: Ecuador ya cuenta con 59.861 km de fibra óptica," [The deployment of telecommunications keeps growing: Ecuador already has 59,861 km of fiber optic], anuary 28, 2016, http://bit.ly/1RQd8of.

4 Vicepresidencia de la República del Ecuador, "Cable submarino de fibra ó tica en su etapa final de instalación" [Undersea cable in the last stage of installation], accessed September 29, 2016, http://bit.ly/21ctrM8.

5 International Telecommunication Union, "Percentage of Individuals using the Internet," accessed September 29, 2016, http://bit.ly/1cblxxY.

6 Akamai, State of the Internet Report, Q4, 2015 report, accessed September 29, 2016, http://akamai.me/2b5MgzU.

7 Agencia de Regulación y Control de las Telecomunicaciones, "Servicio de Acceso a Internet," [Internet Access Service], accessed September 29, 2016, http://bit.ly/1qcC7Xs.

8 "Equipos tecnológicos pagan más por nuevos aranceles," [Technological devices will pay more with new duties], *El Mercurio,* January 28, 2015, http://bit.ly/21Ojo5z.

9 International Telecommunication Union, "Mobile-cellular phone subscriptions 2000-2015," accessed September 29, 2016, http://bit.ly/1cblxxY.

10 Ecuadorian Foreign Trade Commission, Resolution 049-2015, December 29, 2015, http://bit.ly/1Jxl6zx.

11 Jaime Albuja, Andrés Navas, David Paguay, Andrea Moreno & Pablo Nájera, "Technological GINI: a study of the inequality in Ecuador," *2015 Second International Conference on eDemocracy & eGovernment (ICEDEG).*

12 Javier Ortega, "Poderosas mafias del contra ando penetran en Quito con celulares ilegales," [Powerful contraband mafias penetrate Quito with illegal cell phones], *El Comercio*, April 23, 2015, http://bit.ly/1z1k4qN

13 Mercedes Alvaro, "Ecuador Signs 4G Contracts With America Movil, Telefonica," *The Wall Street Journal,* February 18, 2015, http://on.wsj.com/1DsXlo9.

14 Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), "Servicio Móvil Avanzado," [Advanced Mobile Phone System], March 2016, http://bit.ly/1p7oE2U.

15 Augusto Espín, "Rendición de cuentas MINTEL 2015," [2015 MINTEL Report], March 23, 2016, http://bit.ly/24ZRUb9.

are expected to increase with the digital television switchover as it will free more spectrum for mobile use.[16]

While fi ed and mobile broadband internet with low download capacity (500 Mb) is affordable for most users, Ecuador has the steepest price in the region for higher download capacity (1 GB) adjusted for purchasing power parity.[17] It is unclear to what extent these plans offer full connectivity as the three mobile operators in the country sell zero-rated services in at least 67 different modalities.[18] Facing increasing demand, small internet retailers provide internet access to Ecuadorians for less than US$1 per hour.

Even though prices per Mbps for both fi ed and mobile broadband dropped by 25 percent in the last year,[19] socio-economic factors continued to impact internet access. Some 17.7 percent of families in urban areas had internet access compared to 8.5 percent in rural areas. Access also varies across and within provinces, as users are more concentrated in the most economically active centers. For example, in 2013, an average of 8 to 10 percent of rural households in Ecuador's Amazon and mountainous regions had internet access, and only 4 percent in the coastal region.[20]

Ecuador has shown improvements in expanding internet access to rural areas over the past three years through programs facilitated by the Ministry of Telecommunications (MINTEL). Ecuador's state-run Infocentros—community centers with network access that began to be installed in June 2012—provide free internet in 78 percent of rural cantons in the country.[21] Infocentros have played an important role in reducing digital illiteracy (from 21.4 percent in 2012 to 12.2 percent in 2015) by offering free workshops across the country.[22] MINTEL's mobile classrooms project, intended to offer access to those without Infocentros nearby, has also benefi ed more than 380,000 people since its inception.[23] MINTEL and the Ministry of Education expect to provide full access to all public schools through its National School Connectivity Plan.[24] The National Secretariat of Higher Education has

16 A complete blackout of TV signals is programmed for the end of 2016. See: Ministerio de Telecomunicaciones y Sociedad de la Información. "Ecuatorianos deben adquirir televisores con estándar ISDBT-TB," [Ecuadorians must acquire televisions with ISDBT-TB standards], September 30, 2014, http://bit.ly/1QyBCAJ.

17 María F. Viences & Fernando Callorda, "La brecha digital en América Latina: precio, calidad y asequibilidad de la banda ancha en la región," [The digital divide in Latin America: price, quality and affordability in the region], *Diálogo regional sobre sociedad de la información*, January 2016, p. 18, http://bit.ly/1UG7nJP.

18 Apertura Radical, "Carta a MINTEL y SENESCYT: Para favorecer la innovación deben modificar la Ley de Telecomunicaciones," [Open Letter to MINTEL and SENESCYT: In order to promote innovation you must modify the Telecommunications Law], April 1, 2015, http://bit.ly/1R06yMq.

19 María F. Viences & Fernando Callorda, "La brecha digital en América Latina: precio, calidad y asequibilidad de la banda ancha en la región," [The digital divide in Latin America: price, quality and affordability in the region], *Diálogo regional sobre sociedad de la información*, January 2016, http://bit.ly/1UG7nJP.

20 Ministerio de Telecomunicaciones y Sociedad de la Información, "Análisis del porcentaje de hogares con acceso a internet," [Analysis of the percentage of households with internet access], March 2015, http://bit.ly/1RMVwXO.

21 There are 833 Infocentros with over 6 million visits since they were fi st implemented in 2010. See: Ministerio de Telecomunicaciones y Sociedad de la Información, "Infocentros comunitarios," [Community infocenters], accessed March 4, 2016, http://bit.ly/1iPMYxq.

22 Augusto Espín, "Rendición de cuentas MINTEL 2015," [2015 MINTEL Report], March 23, 2016, http://bit.ly/24ZRUb9.

23 "El éxito de los Infocentros Comunitarios y las Aulas Móviles," [The success of community infocenters and mobile classrooms], April 9, 2014, http://bit.ly/24JaHbv.

24 Ministerio de Telecomunicaciones y Sociedad de la Información, "Conectividad escolar," [Scholar connectivity], accessed March 4, 2016, http://bit.ly/1OVJDKB.

also taken steps to provide free Wi-Fi in public and private universities.[25] The number of cybercafes has multiplied since 2009, from 1,355 to 2,667 as of January 2016.[26]

Restrictions on Connectivity

Ecuador's physical infrastructure is not highly centralized. The government does not place limits on bandwidth, nor are there reports of control over infrastructure, although a provision in the 2015 Organic Law of Telecommunications grants the president the power to unilaterally take over telecommunications services in times of national emergency.[27] Civil society groups have raised concerns about the scope of this provision and its potential abuse by the government because of its vague standards and lack of oversight by an independent and impartial court.[28]

In June 2015, protesters against the government in Quito and Guayaquil encountered service problems. Explanations for these problems range from network saturation to the possible presence of cell phone jammers.[29] Local police did report the use of this equipment during the Pope's visit in July 2015,[30] but it is unclear if this equipment has been used to prevent demonstrators to communicate.

On December 3, 2015, during popular riots over constitutional reforms proposed by the government, several users reported problems accessing Twitter images across the country.[31] The blocking did not affect all users in the same way nor was it related to a specific IS , as was the case of Venezuela in 2014.[32] The problem was initially dismissed as a technical failure on Twitter's end. However, minutes later the company declared having investigated the issue without discovering any technical problems on their end.[33] Independent researchers performing tests on the servers that provided Twitter images to the country found different responses within the Ecuadorian territory.[34] According to Aldo Cassola, a network security researcher, if Twitter's performance was not compromised, this could either be a case of routing issues or potentially the effect of a Distributed Denial of Service (DDoS) attack to Twitter's Content Delivery Network.[35]

25 "El Código Ingenios propone redes gratuitas de internet en las universidades," [The Ingenios Act proposes free internet network in universities], *El Telégrafo*, January 10, 2016, http://bit.ly/1PnG94e.

26 Cybercafes initially provided internet access in commercial zones but adjusted their market as the demand shifted towards low and middle income users around 2011. See: "Cibers crecen aliados a tareas escolares y cabinas telefónicas," [Cybercafes grow along with schoolwork and payphones], *El Universo*, June 27, 2011, http://bit.ly/1oWW6IB; Total number of cybercafes obtained from: Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), "Servicio de Acceso a Internet," [Internet Access Service], http://bit.ly/2dNKJgW.

27 Asamblea Nacional República del Ecuador, Ley Orgánica de Telecomunicaciones [Telecommunication Law], http://bit.ly/2fsPlKj.

28 Katitza Rodriguez, "Leaked Documents Confi m Ecuador's Internet Censorship Machine," Electronic Frontier Foundation, April 14, 2016, http://bit.ly/1W144NE.

29 Alfredo Velazco, "The Internet, a Staging Post for Protests in Ecuador, is under threat," Global Voices, June 28, 2015, http://bit.ly/1QObmyR; See also: Aldo Cassola, Twitter post, June 13, 2015, 7:50 a.m., http://bit.ly/2ej6zhW.

30 Juan Carlos Mestanza y Javier Ortega, "Las Fuerzas Armadas y la Policía, listas para dar seguridad al Papa," [The Military and The Police ready to protect the Pope], *El Comercio*, July 3, 2015, http://bit.ly/1YACaYM.

31 "Usuarios de Twitter denuncian que sus fotos no se visualizan en Ecuador," [Twitter users denounce they cannot visualize their pictures in Ecuador], *El Comercio,* December 3, 2015, http://bit.ly/1XCiTJw.

32 The Associated Press, "Twitter reports image blocking in Venezuela," *USA Today*, February 14, 2014, http://usat.ly/1pwXB0R.

33 Twitter @Policy, Twitter post, December 3, 2015, 3:24pm, http://bit.ly/2f5ldb4.

34 Servers 192.229.163.25 and 104.244.43.103 were accessible from the U.S. but connection timed out when connecting from Ecuador. See: Ivan Muela, "¿Bloqueo de imágenes de TWITTER en Ecuador?," [Blocking of Twitter images in Ecuador?], December 3, 2015, http://bit.ly/1QGjh4M.

35 Aldo Cassola, Computer Scientist and Professor, Universidad San Francisco de Quito, interview on March 6, 2016.

ICT Market

Ecuador has 14 major internet service providers (ISPs) covering 99 percent of users and 329 small ISPs providing access to the rest of the market. State-owned National Telecommunications Corporation (CNT) dominated the fi ed-line market, with over 55 percent of subscriptions, followed by Suratel (13.3 percent) and Telconet (10.3 percent). Mobile internet service providers, on the other hand, are an oligopoly: Conecel (Claro) represented 58 percent of active cellular accounts, Otecel (Movistar) 32 percent, and CNT, 10 percent.[36] This concentration of suppliers does not negatively impact users, according to the National Superintendence of Market Power Control.[37]

In February 2015, the New Telecommunications Act entered into force, allowing the government to impose specific obligations o dominant operators with high market power based on their income; and to impose fines depending on the number f users.[38] The amount of such fines also experienced a tenfold increase,[39] collecting US$ 25 million through October 2015.[40]

There have been no reported government restrictions for new companies in the ICT sector. However, it has become difficult for small ent epreneurs to start an ISP in highly populated areas, mainly due to the number of competitors. As a result, they have migrated to outlying provinces.[41] Registration with ARCOTEL, although a simple process, is mandatory for cybercafes.

Regulatory Bodies

In February 2015, Ecuador's National Assembly passed the Organic Law of Telecommunications. Not to be confused with the similarly named Communications Law passed in 2013, the Organic Law on Telecommunications radically changed the regulation of the telecommunications sector. The new telecommunications law created a regulatory body, the Agency for the Regulation of Telecommunications (Arcotel), which is attached to the Ministry of Telecommunications and is responsible for the technical aspects of administration, regulation, and control of the telecommunications sector and the radio-electric spectrum.[42]

Arcotel's directors are all appointed directly by the president, which may undermine its independence.[43] Arcotel's effort to redistribute radio-electric frequencies has notably been criticized for being politicized and lacking transparency. In response to the removal of its frequency, the director

36 An ISP was considered "major" if it had at least 50,000 users. See: Agencia de Regulación y Control de las Telecomunicaciones, "Servicio de Acceso a Internet," [Internet Access Service], accessed January 2016, http://bit.ly/1qcC7Xs.

37 Superintendencia de Control de Poder de Mercado, Expedientes SCPM-CRPI-2015-020 (May 4, 2015) and SCPM-CRPI-2015-052 (September 30, 2015).

38 América Móvil, "Annual Report," December 31, 2104, http://bit.ly/1pqOpeL.

39 "Mayor multa para 'malos' operadores económicos," [Bigger fine for ' ad' economic operators], *El Universo,* December 14, 2015, http://bit.ly/1NPojKS.

40 Sofía Ramírez, "USD 420 millones recaudó la Arcotel seis meses del 2015," [USD 420 million collected by Arcotel during six months in 2015], *El Comercio*, October 7, 2015, http://bit.ly/1N1G7jZ.

41 Rodrigo Barahona, Former Internet Service Provider, Interview March 14, 2016.

42 Asamblea Nacional Republica del Ecuador, Ley Orgánica de Telecomunicaciones [Telecommunication Law]. http://bit.ly/1Kvdp7W.

43 Leticia Pautasio, "Ecuador: Ley de Telecomunicaciones entra en vigencia y Arcotel inicia sus funciones," [Ecuador: Telecommunications Law enters into force and Arcotel starts its functions], TeleSemana.com, March 6, 2015, http://bit.ly/22lJayl.

of the National Union of Journalists claimed this was an act of retaliation for their "fi m and critical stance [against] policies implemented by the government."[44]

Efforts by access providers and other internet-related organizations to establish self-regulatory mechanisms are allowed and, to a certain extent, promoted. Examples of this include the public assistance to develop public and private Computer Security Incident Response Teams (CSIRT) by EcuCERT; the local internet exchange point (NAP.ec) managed by AEPROVI, and the Ecuadorian IPv6 Task Force, among others. The allocation of digital assets, such as domain names or IP addresses, are not controlled by the government, nor are they allocated in a discriminatory manner.

Limits on Content

As the online public sphere has gained prominence as a forum for political and social discussion in Ecuador, the government has sought to exert control over content through a variety of mechanisms. The use of copyright law to censor critical content has become common practice, and public institutions have started to directly issue copyright infringement notices to take down content. Social media have especially been at the center of efforts to manipulate public opinion online in favor of the government, as journalists and government critics suffered retaliation for sensitive posts.

Blocking and Filtering

The government does not engage in systematic blocking or fil ering of content in Ecuador. YouTube, Facebook, Twitter, and blog-hosting services are freely available. There were no reports of the government blocking tools enabling circumvention of online fil ers and censors.

Reports have pointed to past instances of blocking of specific domains at go ernment request. An allegedly leaked internal memorandum from Telefónica (Movistar) noted an instance in 2014 when the Ecuadorian Association of Internet Providers (AEPROVI), which controls over 95 percent of the country's internet traffic, bloc ed access to specific domains at the go ernment's request.[45] While the authenticity of the memorandum has not been confi med by Telefónica, public documentation from SUPERTEL (now ARCOTEL) shows that the government and private ISPs have collaborated in the past to block specific domains o combat piracy,[46] and that AEPROVI maintains a cooperation agreement with ARCOTEL since 2012.[47] The text of the agreement remains unknown to the public, and it is unclear what mechanisms ARCOTEL and AEPROVI use to block internet domains. Likewise, mechanisms for public accountability are not in place or have not been disclosed.

44 Fundamedios, "Arcotel permanently removes independent journalists association's frequency," December 12, 2015, http://bit.ly/1PcWbxg; Plan V, "La Arcotel y los riesgos de la redistribución de frecuencias," [Arcotel and the risks of frequency redistribution], February 22, 2016, http://bit.ly/1WFXJW1.

45 Apertura Radical, "El gobierno ecuatoriano y la Asociación de Proveedores de Internet trabajan juntos para bloquear el acceso a páginas web," [The Ecuadorian government and the Ecuadorian Association of Internet Providers (AEPROVI) collaborate to block access to specific ebsites], http://wp.me/p3jTIV-8t.

46 Superintendencia de Telecomunicaciones, "Informe rendición de cuentas 2014," p.64, [2014 Supertel Report], January 13, 2015, http://bit.ly/22ufi v.

47 Convergencia Latina, "La SUPERTEL fi mará hoy un convenio de cooperación con la asociación de ISPs" [SUPERTEL will sign cooperation agreement today with ISP associaiton], April 17, 2012, http://bit.ly/1XNlCxV.

Content Removal

The use of copyright law to censor online content has been widely recognized for years in Ecuador. Tweets, images, blog posts, and videos were taken down as the result of complaints made by Ares Rights on behalf of Ecuadorian institutions, including the National Secretariat of Communications (SECOM), the National Secretariat of Intelligence (SENAIN), and the state television network (ECTV).[48]

Ares Rights, a company based in Spain, claims that the country's privacy laws forbid them from disclosing any document detailing the relationship with its clients.[49] While the government has not confi med its participation in these requests, it has not acted against the abuses of others on the government's behalf either.[50]

Moreover, public institutions have started to make their own requests to remove content for allegedly violating copyright protections. In March 2015, SECOM sent a letter to Fundamedios, a freedom of expression advocacy organization, stating that they would take legal actions if the latter would not remove the distinctive image of the National Secretary of Communication from one of their tweets.[51] Investigative portals such as *Focus Ecuador* and *Mil Hojas* have also been targeted with complaints from SECOM,[52] and the institution has even added a copyright symbol to the Presidency's official YouTube channel.[53]

In December 2015, Fundamedios received a notice from CloudFlare and Amazon Web Services about new complaints made by Ares Rights on behalf of SECOM.[54] Ecuador Transparente, a website operated by the Associated Whistleblowing Press, was also targeted by Ares Rights after publishing secret documents that contained information about political spying. The request was made on behalf of Rommy Vallejo, head of SENAIN.[55]

Besides the use of copyright law to target critical content online, a study released in August 2016 revealed the growing number of takedown requests for alleged violations of Twitter rules, such as the publication of private information. Between April and July 2016, Fundamedios recorded 806 takedown requests against 292 Twitter accounts. Approximately 30 of these accounts, which corre-

48 Maira Sutton, "State Censorship by Copyright? Spanish Firm Abuses DMCA to Silence Critics of Ecuador's Government," EFF, May 15, 2014, http://bit.ly/1IKGvUY; See also: Alexandra Ellerbeck, "How U.S. copyright law is being used to take down Correa's critics in Ecuador," Committee to Protect Journalists, January 21, 2016, http://bit.ly/1Lu5Uoj.

49 Adam Steinbaugh, "Ares Rights: Our Acts On Behalf of Ecuador Are Private," December 19, 2014, http://bit.ly/1ZpH37t.

50 Enrique Arosemena, former director of the State-owned TV station 'Ecuador TV,' denied a contract with Ares Rights but insinuated that Ares Rights was using the name of Ecuador TV to censor online. In 2014, he announced legal actions against the fi m but they never materialized. See: "Arosemena: 'EcuadorTV no tiene contrato con Ares Right'," [Arosemena: EcuadorTV does not have a contract with Ares Rights], *La República,* April 28, 2014, http://bit.ly/1T5ys9b.

51 "Ares Rights dice que los documentos sobre la SENAIN filtrados por Ecuador ransparente son reales," [Ares Rights: Senain documents leaked by Ecuador Transparente are real], Apertura Radical (blog), December 28, 2105, http://bit.ly/1Vi2MxJ.

52 Fundamedios, "Gobierno realiza tres denuncias más para deshabilitar portal de investigación Focus Ecuador" [Government issues three more complaints to disable the investigative portal Focus Ecuador], May 20, 2016, http://bit.ly/25c52Kg; See also: Fundamedios, "Secom denuncia a portal Mil Hojas por uso de documentos donde aparece el logo de "la marca país"" [SECOM denounces Mil Hojas for using documents with the "country brand"], June 3, 2016, http://bit.ly/1PaOh9i.

53 "Presidencia de la República del Ecuador ©SECOM" [Presidency of the Republic of Ecuador © SECOM], YouTube channel, accessed October 18, 2016, http://bit.ly/2eh4TSx.

54 Alexandra Ellerbeck, "How U.S. copyright law is being used to take down Correa's critics in Ecuador," Committee to Protect Journalists, January 21, 2016, http://bit.ly/1Lu5Uoj.

55 "Ares Rights dice que los documentos sobre la SENAIN filtrados por Ecuador ransparente son reales," [Ares Rights: Senain documents leaked by Ecuador Transparente are real], Apertura Radical (blog), December 28, 2105, http://bit.ly/1Vi2MxJ.

sponded to antigovernment users with high numbers of followers, were suspended after receiving repeated complaints. Ares Rights continued to be behind many of these requests.[56]

Showcasing efforts to actively monitor and remove specific con ent on social media, in September 2015, *Buzzfeed* uncovered a US$4.7 million contract dating from 2012 between the Mexican company Emerging MC and SENAIN, in which the former was required to "predict, anticipate and eliminate" material on social networks that "damage or may damage the integrity of persons, public or private institutions (…) promote or incite violence or acts contrary to the public welfare and morality (…) represent a plagiarism of identity [and] threats, identity theft, defamation, slander and insults." *Buzzfeed* also published the subsequent payments and the company's report on removed content.[57]

The media and communications regulator, the Superintendency of Information and Communications (Supercom), has aggressively pursued print media (including all media with an online presence)[58] under accusations of unbalanced reporting and "media lynching"—an allegation that is often applied to investigative reporting in Ecuador. The Communication Law passed in 2013 grants Supercom the power to audit, intervene, and control all information and media, as well as to enforce regulations governing information and communications. Corrections, sometimes scripted by Supercom, are often issued to media outlets on the basis that articles fail to provide appropriate context. However, civil servants oftentimes avoid commenting on stories prior to publication.[59]

Additionally, the law holds websites liable for content posted on their sites by third parties unless such parties are identifiable th ough personal data such as their national ID number. News outlets that have allowed readers to post comments critical of the government on their websites have faced removal requests, and others have closed their comments section entirely.

Media, Diversity, and Content Manipulation

Although the 2013 Communications Law gives the government broad authority to censor media content, Supercom has especially used the law to sanction privately-owned traditional media outlets, which are mostly offline. The go ernment's broader restrictions on traditional media outlets likely affect digital content associated with these outlets both by encouraging self-censorship and by restricting financial esources for independent media.

Mainstream media outlets such as *El Comercio, El Universo or Expreso* have lawyers that review "sensitive" notes before publication. Cases of corruption and investigative journalism are covered with extreme caution. *El Comercio,* for example, failed to publish a seven-series report on Hacking Team. Activists have also turned down invitations from mass media to talk about the subject after suffering harassment from anonymous sources.[60] Attempts to reprimand progovernment media under current

56 Fundamedios, "806 denuncias en contra de 292 cuentas de Twitter, revela monitoreo" [806 complaints against 292 twitter accounts, monitoring reveals], August 9, 2016, http://bit.ly/2b1JhKg.

57 James Ball & Paul Hamilos, "Ecuador's President Used Millions Of Dollars Of Public Funds To Censor Critical Online Videos," *BuzzFeed,* September 24, 2015, http://bzfd.it/1Lu6kee.

58 Follow-up legislation in 2014 exempted bloggers and social media users from regulation under the Communications Law, but extended the law to cover "all media with an online presence" (see Legal Environment).

59 Fundamedios, "Pedidos de rectificación y éplica: el mecanismo favorito de los funcionarios estatales para imponer su verdad," [Requirements for corrections and response: civil servants' favorite mechanism to impose the truth], October 15, 2015, http://bit.ly/1X6l3gU.

60 Andrés Delgado, "El miedo de vigilar a los vigilantes," [The fear of watching the watchers], blog post, January 15, 2016, https://eff.org/r.xdr2

legal provisions have been less successful.[61] "Whether you like it or not, you self-censor, you are very careful about your words and the headlines, often we would even ask each other how to redact a tweet," confessed a journalist working for a private newspaper, who requested anonymity.[62]

As the Communication Law gained momentum, print journalists posting sensitive content on social media have also been reprimanded, further contributing to self-censorship. The former political editor for *El Comercio,* Martín Pallares,[63] was fi ed by the newspaper after 13 years of service for failing to comply with the paper's guidelines for "good practices on social networks."[64] Similarly, Orlando Perez, editorial director of *El Telegrafo*, has reproached his columnists and even journalists working at other outlets for social media posts that were allegedly untruthful or "harmed the newspaper."[65]

Although the Communications Law exempts social media users from sanctions, the government has issued gag orders during states of emergency under Article 8 of the Telecommunications Act.[66] On August 15, 2015, President Rafael Correa signed a decree forbidding "the dissemination of unauthorized information [regarding the eruption of Cotopaxi Volcano] by any means of social communication, whether public or private, or via social media."[67] One month later, Minister of Security Cesar Navas announced that a fi st complaint will be filed with the ttorney General's Office against ce tain Facebook users for publishing "unscrupulous" opinions.[68]

New media outlets have emerged and thrived online, offering a wide range of political and social viewpoints.[69] However, the online media landscape remains highly distorted by state-owned or state-managed mass media outlets, which often use unidentified sou ces in order to propagate stories. On June 24, 2015, state-operated TV stations EcuadorTV, GamaTV and TC Television, broadcasted a video stitching together separate conversations from two private group chats on Telegram and WhatsApp in order to claim that a "soft coup d'état" was being planned by "the wealthiest families in Quito." The group chat members were conversing about the protests against the government that took place at the end of that month and, according to one of the victims of the privacy breach, the chats were manipulated and juxtaposed to change the narrative.[70] The media refused to turn

61 Superintendencia de la información y la comunicación, "SUPERCOM desecha denuncia contra medios y entidades relacionadas con comunicación," [SUPERCOM rejects complaint against media and communication related entities], April 1, 2015, http://bit.ly/1RmtTF9; See also: "Ley de comunicación no aplica a enlaces sabatinos de Correa," [Communication Law does not apply to Correa's weekly broadcasts], Ecuador Times AR, June 4, 2014, http://bit.ly/1PsA4Da.

62 Online interview, February 11, 2016.

63 Martin Pallares, "Ecuador's Political Eruption," *The New York Times*, September 1, 2015, http://nyti.ms/1o5i1g4.

64 Fundamedios, "Journalist fi ed for his comments on Twitter," August 20, 2015, http://bit.ly/1SgDttn.

65 Fundamedios, "Columnist reports censorship by State operated newspaper," August 5, 2015, http://bit.ly/1UPUIVC.

66 Understood as "aggression; international or internal armed conflict; serious internal disturbances, public calamity; or natural disaster or national, regional or local emergency."

67 Presidencia de la República de Ecuador, Decree 755, August 15, 2015, http://bit.ly/1PwqAa7.

68 Fundamedios, "Ministro anuncia inicio de procesos legales contra personas que divulgaron rumores sobre el volcán Cotopaxi en redes sociales" [Minister announces legal procedures against people that disseminated rumors on the Cotopaxi volcano on social networks], September 22, 2015, http://bit.ly/1NRR4rd.

69 During this period of coverage for example, after only two months of activity the website 4pelagatos.com, which is operated by journalists Roberto Aguilar, Martin Pallares, José Hernández and social media specialist Juan Gabriel Gonzalez, best known as CrudoEcuador, received nearly two million visits from more than half a million unique users. See: 4Pelagatos, "Gracias a nuestros lectores," [Thank you to our readers], March 20, 2016, http://bit.ly/21CuAN2.

70 Rebeca Morla, "Correa Officials Thumb Their Noses at Their Own Comm nications Law," *PanamPost*, July 7, 2015, http://bit.ly/21Hhezh.

over any information about the video (which first appeared online) or to allow the victims to explain themselves.[71]

Several reports on state-sponsored troll farms in Ecuador also reveal efforts to skew public opinion in favor of the government.[72] According to Catalina Botero, former Special Rapporteur for Freedom of Expression for the Inter-American Commission on Human Rights, investigations have identified the IP addresses of these computers in government offices [73] Private firms like Emerging MC have also been implicated in the manipulation of social media content (See Surveillance, Privacy, and Anonymity).

While there is a general mandate to protect Net Neutrality in the Telecommunications Act—outlined in the objectives (Article 3) and principles (Article 4 and 66) of the Law—Article 64 allows ISPs to establish "tariff plans consisting of one or more services, or for one or more products of a service, in accordance with his or her authorization certificates." The rule book for the TelCo Act not only missed a clear definition of net neutrality but reaffirmed that the only limitation for tariff plans was the requirement for ISPs to clearly state the limitations of "any discounts, promotions or bonuses for purchasing services."[74]

Digital Activism

Social media is paramount to the organization of protests in Ecuador. In 2015, proposed economic measures and constitutional reforms—notably an amendment to establish communication as a public service—generated huge public outcry (see Legal Environment). The website lasremiendas.com and the hashtag #ArchivenLasEnmiendas ("File the amendments") were widely used to highlight dissatisfaction with the proposals. On June 8, 2015, Congressman Andrés Páez posted a YouTube video on his Facebook page calling for a rally outside Quito's airport, which went viral and reached thousands of views in a few days.[75] A demonstration called "Black Sunday" was held the following week.[76]

Right after the 7.8 earthquake that hit Ecuador on April 16, 2016, killing 661 people and injuring tens of thousands, a government imposed media blackout rendered social media the main source of information for victims and onlookers alike.[77] In the weeks after the tragedy, volunteers organized themselves through social media, mapping affected zones and gathering further volunteers, money and equipment to help those affected. Live reports of lost and found people, online fundraising campaigns and automatic alerts were all crucial to recovery efforts.

Digital activism, however, does not always produce concrete results. After the publication of leaked

71 TV channels refused to provide information about how they got the information and to allow Valdivieso his right to respond, as mandated by the Communications Law. Ecuador Inmediato, "Andrés Valdiviezo sobre chats presuntamente conspirativos: De la mentira se ha pasado a algo peor, el montaje (AUDIO)," [Andrés Valdiviezo about allegedly conspiring chats: From lies we have moved to something worse], July 4, 2015, http://bit.ly/1q2qRg8.

72 Fundación 1000 hojas, "Troll center: derroche y acoso desde las redes sociales" [Troll center: waste and harassment on social media], http://bit.ly/1xwV6yx; See also: Samuel Woolley, "#HackingTeam Leaks: Ecuador is Spending Millions on Malware, Pro-Government Trolls", August 4, 2015, http://bit.ly/2cUSYMl.

73 "Catalina Botero compara acciones de Bukele con Correa en Ecuador," *La Prensa Gráfica*, February 19, 2016, http://bit.ly/1pVJfaX.

74 Andrés Delgado, "The Final Blow to Net Neutrality in Ecuador," January 3, 2016, http://bit.ly/1Pheecy.

75 Andrés Páez, YouTube channel, video statistics through March 25, 2016, http://bit.ly/2fp15Bp.

76 Focus Ecuador, "Personajes del año 2015," [People of the Year 2015], December 15, 2015 http://bit.ly/1SfWOrW.

77 4 Pelagatos, "El terremoto cuarteó la comunicación correísta," [The earthquake cracked the government's communication], April 16, 2016, http://bit.ly/GUW99Z.

emails that linked Hacking Team to the National Secretariat of Intelligence (SENAIN), several organizations published a statement in defense of privacy that was disseminated through several websites.[78] While they managed to gain public notoriety, trending on Twitter on July 13 with #PrivacidadYA, this did not lead to physical mobilizations or public protests.

Violations of User Rights

The country faces several threats to free expression, including criminal provisions against libel, government regulation and oversight of media content, and concerns about judicial independence. Recent leaks have shed light on the extralegal monitoring of environmental activists, politicians and journalists, as well as on the role of the National Secretariat of Intelligence beyond its stated mission. Harassment and threats against social media users have become common place, and in some cases have also taken place offline.

Legal Environment

A lack of legislation specifically ta geting online speech has allowed journalists and bloggers to enjoy relatively higher levels of freedom online than offline. Ecuado 's Constitution guarantees "universal access to information technologies and communication" (Article 16.2), and confers the ability to exercise one's right to communication, information, and freedom of expression (Article 384). The latter, however, was amended by the National Assembly in December 2015 to include the mandate that "*communication as a public service* will be provided through public, private and community media" (emphasis added). The move to categorize communication as a public service has especially raised criticism for undermining freedom of expression as a human right and opening the way for broad government regulation of media outlets.[79] Although Article 71 of the Organic Law of Communication, adopted in 2013, already included similar wording on communication as a public service, a constitutional amendment would cement and strengthen this principle.[80]

The 2013 Communication Law calls for the establishment of a government committee to regulate media and issue civil and criminal penalties to journalists or media outlets that fail to report in a manner that the regulator deems fair and accurate. Although Article 4 states that the law "does not regulate information or opinions expressed by individuals on the internet," the definition f social media outlets in Article 5 includes "content which can be generated or replicated by media outlets on the internet." Follow-up legislation in 2014 exempted bloggers and social media users from regulation under the Communications Law, but expanded the definition f "mass media" to include "those [websites] that operate on the internet, whose legal status has been obtained in Ecuador and distribute news and opinion content."[81]

78 David Bogado, "Hacking Team y Ecuador: Pronunciamiento En Defensa De La Privacidad," [Hacking Team and Ecuador: a statement in defense of privacy], Electronic Frontier Foundation, July 13, 2015, http://bit.ly/1J4t7pc.

79 Silvia Higuera, "Ecuador declares communication "a public service"; Fundamedios considers it a "serious setback"," Journalism in the Americas, December 8, 2015, http://bit.ly/1OS1mWp; See also: Fundamedios, "Assembly approves amendment to constitution that makes communication a public service," December 2, 2015, http://bit.ly/1NtiDpz; John Otis, "How Ecuador's plans to make communications a public service is threat to free press," Committee to Protect Journalists (blog), January 20, 2015, http://bit.ly/1PEHiKg.

80 Asamblea Nacional, Ley Orgánica de Comunicación [Organic Law of Communication], June 25, 2013, http://bit.ly/1pgZrCC.

81 Decree 214, Art. 3, January 27, 2014, http://bit.ly/208xLfH; See also: Alianza Regional, "Artículo XIII: Informe sobre control estatal de las redes sociales" [Article XIII: Report on state control of social networks], May 2016, http://bit.ly/1rQZOWx.

Changes to the penal code that entered into force in August 2014 eliminated criminal charges for insult, but retained them for slander and libel.[82] Article 179 restricts protections for whistleblowers by establishing a prison sentence of six months to one year for any person "who, by virtue of his/her state or office, employment, p ofession, or art, has knowledge of a secret whose divulgement might cause harm to another and reveals it." The article makes no exception for revealing information in the public interest. Article 229 places further restrictions on divulging information by banning the revelation of registered information, databases, or archives through electronic systems in a way that violates the intimacy or privacy of someone else, with no exceptions for whistleblowers or journalists. Article 307 establishes a penalty of fi e to seven years in prison for creating economic panic by "publishing, spreading, or divulging false news that causes harm to the national economy in order to alter the prices of goods."

In early 2015, Carlos Ochoa, the country's Information Superintendent, declared that reforms are being prepared to amend the Communication Law, but said that new regulations on social media would need further public debate across the country before being considered.[83] Regulation on the protection of personal data are also being developed.[84] Finally, the National Assembly has presented a new bill that would allow the takedown of websites without a court order.[85]

The lack of judicial independence is another ongoing concern. A 2014 report from the Due Process of Law Foundation has noted how "Ecuador's justice system is currently being subjected to political usages that seriously jeopardize judicial independence in those cases where the government's interests are at stake."[86]

Prosecutions and Detentions for Online Activities

Lawsuits for defamation have increasingly threatened online users. During the coverage period, two politicians—Sebastian Cevallos and Jeannine Cruz Vaca—were sentenced to 15 and 30 days in jail, respectively, for "defamatory" content posted on Twitter under article 396 of the Criminal Code, which punishes "expressions that discredit or dishonor." Bolívar Castillo, mayor of Loja and an ally of the government, said that he sued Jeannine Cruz to set a precedent. Cruz had posted a video and tweet criticizing the mayor's management of a water sanitation project.[87] Previously Castillo had sued *La Hora* newspaper because they "failed to provide in-depth coverage" of one of his public speeches.[88] The suit against Cevallos was filed by a civil se vant and niece of the former labor minister, after Cevallos tweeted about an alleged case of nepotism.[89]

82 Ministerio de Justicia, Derechos Humanos y Cultos, Código Orgánico Integral Penal, 2014, http://bit.ly/1juCXok.

83 "Carlos Ochoa: Regulación a redes sociales necesita antes un gran debate en el país," [Carlos Ochoa: Social media regulation requires a big national debate], *El Universo*, February 11, 2015, http://bit.ly/1Rtn30v.

84 The project has not been made public, its focus and scope are unknown. See: Derechos Digitales, "Latin America in a Glimpse," November 6, 2015, http://bit.ly/1REQWOD.

85 Usuarios Digitales, "Boletín de Prensa: Proyecto de Ley orgánica de protección de los datos personales ¿Impactará la libertad de expresión y flujo de info mación?" [Press Release: Law Proposal for Protection of Personal Data, Will it impact freedom of expression and the free flow f information?], September, 19, 2016, http://bit.ly/2dBdz5T.

86 Luis Pásara, "Independence in the Ecuadorian justice reform," Due Process of Law Foundation, July 2014, http://bit.ly/1l9TIGu.

87 Lineida Castillo, "2 personas sentenciadas en 52 días por comentar en Twitter," [Two people sentenced in 52 days for commenting on Twitter], *El Comercio*, January 6, 2016, http://bit.ly/1PMKkLB.

88 Fundamedios, "Mayor reports newspaper that failed to provide in depth coverage," May 1, 2015, http://bit.ly/1q2rHto.

89 Cuenca: político condenado a 15 días de cárcel por denunciar presunto caso de nepotismo en Twitter [Cuenca: politician condemned to 15 days in jail for denouncing alleged case of nepotism on Twitter], *La Hora,* November 11, 2015, http://bit.ly/2dybSaJ.

Online writers have also incurred high penalties in civil libel cases. On July 22, 2015, the National Court of Justice ordered a blogger to pay a fine f US$ 46,000 for "moral damage" against President Correa. Blogger Miguel Palacios Frugone had previously sued President Correa for libel after the president called him a "rapist." President Correa responded in kind by countersuing Palacios for defamation over 20 articles that he produced on his blog "Desde mi Trinchera" ("From my Trench").[90]

In June 2015, journalist Roberto Aguilar from EstadoDePropaganda.com, a blog critical of the government's control over mass media, was sued on charges of defamation by Fernando Alvarado, the legal representative of the National Secretariat of Communications.[91] The complaint was finally dismissed fi e months later.

The Security Coordinating Minister, César Navas, also announced the beginning of legal proceedings against social media users who posted "unscrupulous" comments in the aftermath of the Cotopaxi volcanic eruption in August 2015.[92] A presidential decree issued on August 15 had forbidden "the dissemination of unauthorized information by any means of social communication, whether public or private, or via social media."[93]

Surveillance, Privacy, and Anonymity

The National Secretariat of Intelligence (SENAIN) is in charge of producing "strategic SIGINT [signals intelligence] for the integral security of the state, society and democracy." Created in 2009 by a presidential decree, SENAIN has continuously expanded its capacities and budget, reaching US$ 58 million in 2015. Most of the budget has been allocated to "special expenses for communications and counterintelligence."[94] A secret document published by the whistleblowing website Ecuador Transparente in June 2014 outlines what SENAIN considered as "risk factors and threats against democratic stability." These included political parties,[95] "local movements", mass media, private banks, chambers of commerce, environmental and indigenous organizations, rural communities and unions.

In July 2015, Italian spyware company Hacking Team was compromised and their financial and commercial transactions exposed. While the National Secretary of Intelligence, Rommy Vallejo, quickly noted that SENAIN had no contractual relationship with Hacking Team,[96] leaked documents have suggested otherwise and researchers have sought to establish a connection. Firstly, National Representative Lourdes Tiban held a press conference showing documents (from February 2013) previously leaked by Anonymous Ecuador, in which the former National Secretariat of Intelligence, Pablo

90 Belén Marty, "Rafael Correa Fines Columnist for Libel and Calls Him a Rapist," PanAm Post, July 29, 2015, http://bit.ly/1OLIF9g; "Miguel Palacios sobre sentencia a favor del presidente Correa: 'Me siento una hormiga enfrentando a King Kong'," *El Comercio*, July 27, 2015, http://bit.ly/1OLnTFA.

91 Fundamedios, "Journalist Roberto Aguilar is called to make judicial confession at the request of Communication Secretary," June 25, 2015, http://bit.ly/1NkR53D.

92 Fundamedios, "Ministro anuncia inicio de procesos legales contra personas que divulgaron rumores sobre el volcán Cotopaxi en redes sociales" [Minister announces legal procedures against people that disseminated rumors on the Cotopaxi volcano on social networks], September 22, 2015, http://bit.ly/1NRR4rd.

93 Presidencia de la República de Ecuador, Decree 755, August 15, 2015, http://bit.ly/1PwqAa7.

94 Secretaría Nacional de Inteligencia, "Programación Anual de la Política Pública," [Annual Program for Public Policy], February 11, 2015, http://bit.ly/1pQ7SG2.

95 Cited as right-wing political parties are: PSC-MG, PSP, CREO, Concertación and SUMA. Cited as left-wing parties are: MPD, Pachakutik, certain factions of the socialist party. See: Ecuador Transparente, "Reporte de la Inteligencia Ecuatoriana (SENAIN) sobre factores de riesgo y amenazas a la estabilidad democrática," [Report by Ecuadorian Intelligence (SENAIN) about risk factors and threats to democratic stability], December 28, 2015, http://bit.ly/1Q3yJ6v.

96 Fundamedios, "Senain warns it will take legal action against those who release information linking it to hacking team," July 16, 2015, http://bit.ly/1XVLaXm.

Quezada, authorized Illuminati Lab to act as an intermediary between SENAIN and Hacking Team.[97] Secondly, Robotec (Colombia) and Theola (Belize) were identified as in ermediaries between SENAIN and the Italian Company.[98] Thirdly, several researchers, helped by the victims exposed in the Hacking Team database, were able to confi m the veracity of the documents.[99] Finally, the governments of Chile[100] and Cyprus[101] recognized the authenticity of the leaks the fi st week after they came out.

According to a technical analysis by "ilv", a Tor Project developer, the government targeted judges, members of the national electoral council, political parties and political movements.[102] On August 4, 2015, Ecuador Transparente made public 31 secret documents from SENAIN corresponding to intelligence gathered between 2012 and 2014. Among the targets were Mauricio Rodas, mayor of Quito; politicians Alvaro Noboa, Gilmar Gutiérrez, Dalo Bucarám, Mery Zamora and Andrés Páez; environmentalists Matt Finer, Joke Baert, Sigmund Thies and Kevin Koenig; cartoonist Xavier Bonilla; and journalists María Josefa Coronel and Carlos Vera. Grassroots environmentalist organizations, like Pachamama and Yasunidos, were also targeted. Both groups, apparently, had their telephone calls and emails intercepted.[103]

As shown in the documents leaked by Ecuador Transparente, SENAIN also made use of information gathered by public agencies and stored in the government platform www.datoseguro.gob.ec. This website, administered by the National Directorate of Public Data Registry, claims that their data is encrypted in transit and on its servers.[104] Public entities, however, are legally obliged to provide any information required by SENAIN as long as this request has been communicated to the president.[105] While President Rafael Correa has stated that everything done by the Intelligence Agency is within the rule of law,[106] it is unclear whether interception was authorized by a judge, since the president later declared that "any use of SENAIN equipment for national security purposes" is authorized by the district attorney.[107]

The National Secretariat of Intelligence is accountable to the executive power and to a specialized

97 Andreína Laines, "Lourdes Tibán asegura que sí existió relación entre la Senain y Hacking Team," [Lourdes Tibán assures that there is a relation between Senain and Hacking Team], Ecuavisa, July 30, 2015, http://bit.ly/1UlK2y8 .

98 Rebeca Morla, "Ecuadorian Websites Report on Hacking Team, Get Taken Down," *PanamPost*, July 13, 2015, http://bit.ly/1oebLCI.

99 Associated Press, "APNewsBreak: Leaked Hacking Team emails suggest Ecuador illegally spied on opposition," *Fox Business*, August 6, 2015, http://fxn.ws/1Rmaa9M.

100 Carlos Gutiérrez, "Chile confi ma la compra de software a Hacking Team," [Chile confi ms software acquisition from Hacking Team], FayerWayer, July 7, 2015, http://bit.ly/22Qp7EZ.

101 Cale Guthrie Weissman, "The Hacking Team fallout continues, as the head of intelligence for Cyprus steps down," *Business Insider*, July 13, 2015, http://read.bi/1MsWwS3.

102 Ilv, "Hacking Team, Chile & Ecuador," July 11, 2015, http://bit.ly/1PxVA9x.

103 Associated Whistleblowing Press, "Ecuadorian intelligence agency spied systematically on politicians and activists," August 4, 2015, http://bit.ly/1MsYGRI.

104 Dirección Nacional de Registro de Datos Públicos, "Preguntas Frecuentes," [FAQ], March 26, 2016, http://bit.ly/1pDBXrr.

105 Law of Public and State Security, Article 17.

106 Article 22 of Law of Public and State Security states that it is prohibited to gather information, produce intelligence or store data on individuals because of "ethnicity, sexual orientation, religion, private actions, political preference or adhesion or membership to partisan organizations."

107 The Criminal Code provides in Article 5.10 that "everyone is entitled to their personal and family privacy and records and searches cannot be done (…) except by order of the competent judge." The Telecommunications Act provides in Article 77 that interception of data and messages can only be done "when there is an express order of a competent judge, as part of an investigation of a crime or for reasons of public security and the state, according to those established by law and following due process." On the other hand, Article 470 of the Criminal Code states that personal communications to third parties cannot be recorded without their knowledge and authorization, except as expressly stated in the law and previous court order. As for the interception of computer data, Article 476 of the Criminal Code allows it, as part of a judicial process only. See: ANDES, "President Rafael Correa denies that Secretary of Intelligence hired Italian Company Hacking Team," July 17, 2015, http://bit.ly/1PxXRS6.

committee of the National Assembly, where they present a report every three months in reserved sessions. Nevertheless, the legal representative of SENAIN is not required to answer every question asked.[108] The Comptroller General may also investigate SENAIN in the area of competence. Besides the abovementioned mechanisms, there is no oversight body in place to guard against abusive use of surveillance technology. Content intercepted during internet surveillance is admissible in court and can be used to convict criminals under Articles 476 and 528 of the Criminal Code.

There have been several indications of government monitoring of blogs, social media and websites. The contract between Emerging MC and SENAIN, made public by *Buzzfeed*, requires the company to "predict, anticipate and eliminate" material on social media.[109] In previous reports from 2013, "marketing company" Illuminati Lab displayed monitoring of Ecuadorian social media as a success story of their company.[110] In April 2016, SENAIN published a press release threatening legal action in light of "unfounded publications made by (...) some Twitter users" related to the Panama Papers leak.[111]

In 2011, SENAIN signed a nondisclosure agreement with the Chinese fi m Huawei.[112] The company is a partner of state-owned CNT and their technology is widely available in the country. Additionally, under the rules of the telecommunications law, ISPs are obliged by ARCOTEL to "provide technical, economic, financial, legal documents, and in general, any fo m or request for information" and to "allow inspections to facilities and systems."[113] Finally, the Subsystem for Interception of Communications or Computer Data (SICOM) of the General Attorney requested Hacking Team's assistance to build a country-wide monitoring center to access PCs, laptops, cellphones and tablets.[114] The system currently allows interception of voice calls and text messages (SMS) of criminal suspects.[115]

Neither anonymous nor encrypted communications are prohibited in Ecuador. Registration of cell phones and SIM cards, however, is mandatory for every citizen.[116] News sites are also required to prove the identity of commentators, or are otherwise liable for the latter's wrongdoing. ISPs are required to submit the IP addresses of their clients without a judicial order on request by Arcotel.[117] Finally, mobile operators were required to implement technology that would automatically provide the physical location of cellphone users for emergency purposes, within an accuracy range of 50 meters.[118]

108 "Rommy Vallejo acudió a la Asamblea Nacional para presentar su declaración trimestral de cuentas," [Rommy Vallejo attended the National Assembly to present its quarterly statement], *El Comercio*, August 5, 2015, http://bit.ly/1SQSeq3.

109 James Ball & Paul Hamilos, "Ecuador's President Used Millions Of Dollars Of Public Funds To Censor Critical Online Videos," *BuzzFeed,* September 24, 2015, http://bzfd.it/1Lu6kee.

110 Mónica Almeida, "Illuminati destaca como su 'caso de éxito' a campaña de Rafael Correa en redes," [Illuminati highlights as "success case" their Rafael Correa campaign in networks], Dec. 10, 2013, http://bit.ly/1iu99pX .

111 Secretaría Nacional de Inteligencia, "Comunicado de Prensa," [Press Release], April 4, 2016, http://bit.ly/1TP9NYp.

112 Secretaría Nacional de Inteligencia, "Convenio de Confidencialidad" [Nondisclosure agreement], June 30, 2011, http://bit.ly/1VPadNd.

113 Presidencia de la República del Ecuador, Executive Decree 864, January 25, 2016, http://bit.ly/25rkkvZ.

114 Plan V, "Los secretos del nuevo Proyecto Galileo," [The secrets of the new Galileo Project], July 8, 2015, http://bit.ly/22FDFKW.

115 Fiscalía General del Estado, "La interceptación de llamadas se hace solo bajo la autorización de un juez," [Call interception is done only under the authorization of a judge], July 21, 2015, http://bit.ly/1Mu8c70.

116 Derechos Digitales, "Freedom of Expression, Encryption and Anonymity, Civil Society and Private Sector Perceptions," May 21, 2015, http://bit.ly/1UvKTN4.

117 See Article 29.9, ARCOTEL, "Reglamento para abonados de los servicios de telecomunicaciones y valor agregado," [Telecommunication Service Subscribers and Added Value Regulation], July 20, 2012, http://bit.ly/25rl1W4.

118 Servicio Integrado de Seguridad ECU 911, "Informe de Gestión Anual 2015," [Annual Report 2015], February 19, 2016, http://bit.ly/1MuS6Kp, and Ecu 911, "Geolocalización," [Geolocation], http://bit.ly/2e3vfsH.

Intimidation and Violence

Social media influence s in Ecuador often face harassment, both online and offline. On July 29, 2015, a bouquet of flo ers was thrown at activist Paulina Muñoz by an unknown man on the street. She also disclosed that her Facebook page and email had been compromised and used to threaten her.[119] Similarly, a Twitter user critical of the government received what was labeled as a "Christmas gift" from two unidentified sende s. When he opened it, he found a box representing a coffin, a disemboweled cat, pictures of his wife and children, and a message that "granted" him 24 hours to close his Facebook and Twitter accounts.[120] Previous victims of harassment have also received offline threats because of their online activities, such as Gabriel Gonzalez, creator of the satire page Crudo Ecuador,[121] and journalists Betty Escobar[122] and Andrés Mendoza.[123]

Online threats are also a common occurrence, especially fueled by the heated atmosphere amplified by the president's weekly speeches calling on supporters to dox and prosecute dissidents.[124] In January 2016, President Correa called for the public to "use the law" against his critics on social media.[125] Days later, several Twitter accounts critical of the government were suspended. Most of them were reactivated without any explanation as to why they were sanctioned.[126] Correa also has encouraged his followers to find and elease personal information about users who insult him[127] as well as investigative journalists, like those reporting on the Panama Papers.[128]

Privacy activists Rafael Bonifaz and Alfredo Velasco denounced threats to their families as an aftermath of their follow-up on the Hacking Team scandal.[129] Andrés Delgado, who broke the story on the online magazine Gkillcity.com, lost internet access and received threats via WhatsApp.[130] Other victims include lawyer Silvia Buendía, who was threatened with having her limbs amputated; news outlet *La República Digital*, which received a message stating "I hope someone burns your facilities with all of you inside"; and Pamela Aguirre, a member of the ruling party who also received death threats for her activity promoting President Correa's reelection.[131]

119 Fundamedios, "Activist gets bouquet as threat and reports she is the victim of harassment," July 29, 2015, http://bit.ly/1RBDbx5.

120 "Tuitero denuncia amenazas de muerte," [Twitter user denounces death threats], *La República,* December 25, 2015, http://bit.ly/1NSyqv0.

121 Silvia Viñas, "What Happened When I Joked About the President of Ecuador," *The New York Times*, May 1, 2015, http://nyti.ms/1E2DoiV.

122 Marcela Estrada, "Ecuador: Censorship Beyond Borders Draws Human-Rights Condemnation," *PanamPost,* May 16, 2014, http://bit.ly/21PxsGH.

123 Fundamedios, "Journalist receives several messages threatening him to death," May 17, 2015, http://bit.ly/1ZGSyYe.

124 Fundamedios, "President calls for revealing Twitter user's identity and prosecute those who respond to his challenge in social networks," January 11, 2016, http://bit.ly/1VBGsiW.

125 Fundamedios, "President calls for revealing Twitter user's identity and prosecute those who respond to his challenge in social networks," January 11, 2016, http://bit.ly/1VBGsiW

126 Fundamedios, "Twitter keeps suspending accounts from users that are critical with the government," January 19, 2016, http://bit.ly/1o53eC7.

127 Usuarios Digitales, "Presidente pide identificar tui eros que 'insulten' en internet," [President asks to identify twitter users who insult on the internet], June 7, 2016 http://bit.ly/1QdQJ4y.

128 Paola Navarrete, "Latin American journalists investigating the Panama Papers suffer criticism and retaliation," Journalism in the Americas, April 27, 2016, http://bit.ly/21hq2Nr.

129 Fundamedios, "Digital rights activists threatened through Twitter," July 14, 2015, http://bit.ly/1qbZqAE.

130 Andrés Delgado, "El miedo de vigilar a los vigilantes," [The fear of watching the watchers], Blog Post, January 15, 2016, https://eff.org/r.xdr2.

131 Fundamedios, "The activist Silvia Buendía was threatened on Twitter," February 8, 2016, http://bit.ly/1RC1Wcx, "News portal receives threats of arson through social networks," November 18, 2015, http://bit.ly/1UqYdCf, Redacción elcomercio.com, "José Serrano anuncia que investigará las amenazas a Pamela Aguirre," [José Serrano says he will investigate threats to Pamela Aguirre], March 13, 2016, http://bit.ly/1URK6pf.

Technical Attacks

The year 2015 saw an extensive campaign of phishing and malware attacks targeting civil society and public figu es in the country. Ecuador is the fourth country with the highest number phishing attacks in the world.[132]

In December 2015, Citizen Lab revealed an analysis of a series of malware attacks in Ecuador and other countries. High-profile jou nalists working on domestic and regional politics, like Janeth Hinostroza; civil society organizations, activists and politicians working on environmental issues and freedom of expression, like César Ricaurte; and members of the parliament were known targets of the so-called Packrat malware.[133]

Journalist José María León reported that one day after the publication of the Hacking Team leaks, Gkillcity.com had its Twitter account hacked and deleted and their office in ernet access was interrupted. "One month before, we immediately remembered, someone hacked our Facebook account." Gkillcity, along with Milhojas.is and Planv.com; all received distributed-denial of service (DDoS) attacks after publishing articles detailing the links between SENAIN and Hacking Team.[134]

Four different media sites reported attacks while providing live coverage of antigovernment protests.[135] The website censuracom.ec was inaccessible for several days due to DDoS attacks, as reported by Fundamedios, a freedom of expression watchdog, which had its website attacked at the same time.[136] Several social media accounts criticizing the government had also been suspended.[137]

In August 2015, Mil Hojas Foundation published a document linking previous attacks against Bananaleaks.com (a website that published information against the government) and its associated Twitter account to "Eye Watch," a registered trademark of Emerging MC, the company allegedly hired by SENAIN for US$ 4.69 million.[138]

Ecuador has the fourth-highest number of phishing attacks in the world.[139] Between January 2015 and October 2015, there were 1,254 allegations of cybercrimes in Ecuador, according to the Attorney General, of which 800 (63 percent) were for misappropriation of money or information through electronic means. The most common type of financial malwa e were SMS trojans (67 percent), followed

132 Maria Vergelis, Tatyana Shcherbakova, Nadezhda Demidova, Darya Gudkova, "Kaspersky Security Bulletin, El spam en 2015," [Kaspersky Security Bulletin, spam in 2015], February 5, 2016, http://bit.ly/1MuS6Kp.

133 John Scott-Railton, Morgan Marquis-Boire, Claudio Guarnieri, and Marion Marschalek, "Packrat: Seven Years of a South American Threat Actor," Munk School of Global Affairs, University of Toronto, December 8, 2015, http://bit.ly/1U3dFkI.

134 José María León, "El día que tuvimos miedo," [The day we were afraid], Gkillcity.com, July 13, 2015, http://bit.ly/25t7ygw.

135 Teresa Mioli, "Cyberattacks push Ecuadoran [SIC] news sites offline during p otest coverage," Journalism in the Americas, June 12, 2015, http://bit.ly/1SfU8KT.

136 "El reporte sobre la censura que fue censurado a las 48 horas," [The censorship report that was censored after 48 hours], Plan V, January 25, 2016, http://bit.ly/1JBmxgK.

137 Fundamedios, "Social networks continue suspending accounts and critical content against the Ecuadorian government," January 28, 2016, http://bit.ly/1REFFaP.

138 Fundación 1000 hojas, "Operación Walkiria: Así censuraron a Bananaleaks," [Walkiria Operation: This is how they censored bananaleaks], August 28, 2015, http://bit.ly/1URRe52; See also: James Ball & Paul Hamilos, "Ecuador's President Used Millions Of Dollars Of Public Funds To Censor Critical Online Videos," *BuzzFeed,* September 24, 2015, http://bzfd.it/1Lu6kee The trademark was registered by I3 Ventures in 2015, however it remains under the same registrant of Illuminati Lab company http://bit.ly/1ZHkawo.

139 Maria Vergelis, Tatyana Shcherbakova, Nadezhda Demidova, Darya Gudkova, "Kaspersky Security Bulletin, El spam en 2015," [Kaspersky Security Bulletin, spam in 2015], February 5, 2016, http://bit.ly/1MuS6Kp.

by spyware (23 percent). The province of Guayas registered 49 percent of all malware attacks in the country, followed by Pichincha with 43 percent.[140]

The Counter-Intelligence and Strategic Technological Operations Center of SENAIN handles the technical aspects of the country's cybersecurity, and EcuCERT, has been in operation since 2014.[141] In early 2016, Ecuadorian police created a special unit to deal with cybercrime with a team of 200 agents working in research and intelligence.[142]

140 Dmitry Bestuzhev (@dimitribest), Twitter posts on October 30 2015, http://bit.ly/1VPBXRO.

141 Inter-American Development Bank (IDB); Organization of American States, "Cybersecurity: Are We Ready in Latin America and the Caribbean?" March 2016, http://bit.ly/1qatSLC.

142 ANDES, "Ecuador crea unidad especial para enfrentar ciberdelitos," [Ecuador creates special unity against cybercrime], February 3, 2016, http://bit.ly/1MM284J.

Freedom House

Egypt

	2015	2016
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	14	15
Limits on Content (0-35)	13	15
Violations of User Rights (0-40)	34	33
TOTAL* (0-100)	**61**	**63**

* 0=most free, 100=least free

Population:	**91.5 million**
Internet Penetration 2015 (ITU):	**36 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- Voice over Internet Protocol (VoIP) calling services were blocked over most mobile connections in October 2015 (See **Restrictions on Connectivity**).
- *Al-Araby al-Jadeed* and *The New Arab* were blocked in December 2015, days after Saudi Arabia and the United Arab Emirates censored the Qatari news sites. This was the first reported time Egypt has engaged in politically motivated blocking since 2011 (see **Blocking and Filtering**).
- A new antiterrorism law and a proposed cybercrime bill contain disproportionate penalties for nonviolent online speech (see **Legal Environment**).
- A 22-year-old was handed a three-year prison term for Facebook posts deemed insulting to President Abdel Fattah el-Sisi, including a photo of the president with Mickey Mouse ears (see **Prosecutions and Detentions for Online Activities**).
- Four Christian teenagers were sentenced to five years in prison for making a video mocking the so-called Islamic State. All four fled the country to seek asylum (see **Prosecutions and Detentions for Online Activities**).

Introduction

Restrictions on Voice over Internet Protocol (VoIP) and the unprecedented blocking of news sites led to a decline in internet freedom in Egypt over the past year.

Internet penetration has improved very slowly in the country, which has been plagued by political uncertainty and economic strife since the 2011 revolution that ousted longtime president Hosni Mubarak. Space for political opposition has dwindled both under former Islamist president Mohamed Morsi, as well as under President Abdel Fattah el-Sisi, who as defense minister and head of the armed forces removed Morsi from power in June 2013. A new constitution was passed by referendum in January 2014, and presidential elections that May brought el-Sisi to power with over 90 percent of votes.[1] Parliamentary elections in late 2015, boycotted by opposition groups, had a voter turnout of only 10 percent. Within only 15 days, the new parliament approved all but one of the 342 laws that the president had passed through decrees issued in the previous year and a half.[2]

Despite the existence of nominal guarantees in the constitution, the legal environment has tightened following the 2013 coup. Restrictions on freedom of assembly were passed in November 2013,[3] and in September 2014, a new law made it a potentially capital offence to accept funding from foreign countries in order to commit an act "harmful to the national interest, or compromising the country's sovereignty," a broad term that activists and journalists worried could apply to critical reporting or online campaigns against human rights abuses. Nongovernmental organizations (NGOs) also face increasing pressure under strict laws requiring them to register with the authorities and obtaining approval for receiving foreign funding.[4] In addition, new cybercrime and antiterrorism legislation included harsh penalties for broadly worded crimes applicable to online activities, such as setting up websites that could be construed as being related to terrorism.[5] The antiterrorism law was passed in August 2015, despite fervent criticism from local activists and the international human rights NGOs.

As the president stepped up the prosecution of opposition and human rights defenders, his detractors find sati e a potent outlet for their frustration, particularly online. After a speech where the president stated he would have readily "sold himself" for the country's benefit, pranks ers put him up for sale on eBay.[6] However, tolerance for comedy and satire has been slim. A famous YouTube comedy group was arrested on serious charges for satirical videos, while fi e teens were sentenced to fi e years on charges of insulting religion for making a mock execution video in the style of the Islamic State militant group. Several individuals were jailed for online videos that were deemed to have insulted the honor or image of Egyptian women.

1 "Egypt election: Sisi secures landslide win," BBC News, May 29, 2014, http://www.bbc.com/news/world-middle-east-27614776.

2 "100 days on, Egypt's parliament has seen few achievements, much controversy," *Al Monitor*, April 26, 2016, www.al-monitor.com/pulse/originals/2016/04/egypt-parliament-100-days-controversy-sisi-acheivement.html, and "Egypt's hollow parliament," Al Jazeera, January 12, 2016, http://www.aljazeera.com/indepth/opinion/2016/01/egypt-hollow-parliament-160112071640089.html.

3 David D. Kirkpatrick, "New law in Egypt effectively bans street protests," *The New York Times*, November 25, 2013, http://nyti.ms/1EY7Lyi.

4 David D. Kirkpatrick, "Human Rights Groups in Egypt Brace for Crackdown Under New Law," *The New York Times*, December 26, 2014, http://www.nytimes.com/2014/12/27/world/middleeast/human-rights-groups-in-egypt-brace-for-crackdown-under-new-law.html?_r=0.

5 Amira Al Hussaini, "Egypt's Anti-Terrorism Law to Target Internet," *Global Voices,* January 31, 2014, http://bit.ly/1VaZPgS.

6 "Egypt's Sisi 'put up for sale' on eBay after speech," Al Jazeera, February 25, 2016, www.aljazeera.com/news/2016/02/egypt-sisi-mocked-offering-sell-160225045549263.html.

Obstacles to Access

Poor telecommunications infrastructure and relatively high costs continue to pose obstacles to universal internet access in Egypt. The government's control over the internet backbone dampens market competition and centralizes control over the internet. Although the privately held mobile internet market is more diverse, VoIP services continue to be restricted over mobile broadband networks.

Availability and Ease of Access

The development of Egypt's information and communications technology (ICT) sector has been a strategic priority since 1999, when former president Hosni Mubarak created the Ministry of Communications and Information Technology (MCIT) to lead Egypt's transition into the information age.[7] Since then, ICT use has increased rapidly, with internet penetration growing from 21.6 percent in 2010 to 35.9 percent by the end of 2015, according to figu es from the International Telecommunication Union.[8] Mobile internet users via mobile phones or USB modems accounted for roughly 46 percent of all internet use, with ADSL use at around 34 percent. Egypt's mobile phone penetration rate was 108.2 percent in April 2016,[9] amounting to over 95 million mobile subscriptions, as well as 26.08 million mobile internet subscriptions.[10] Although these figu es are promising, there are a number of obstacles hindering access to ICTs, including an adult literacy rate of only 74 percent, poor telecommunications infrastructure in rural areas and urban slums, and flagging economic conditions [11]

Broadband prices have been slowly decreasing, despite the existence of a dominant state-owned internet provider, with increased competition from mobile providers. While a basic capped subscription costs around US$ 5.60, an unlimited 1 Mbps connection costs around US$ 16 (EGP 140) per month. Moreover, most providers implement a cap on high-speed internet, even on so called "unlimited" connections, under what has been marketed since 2007 as a "fair use policy."

Furthermore, the overall poverty of Egyptian households naturally impedes access to broadband internet.[12] Telephone lines are not universal, with large segments of the country unconnected to the landline telephone grid. Even when they are, the phone infrastructure, based on antiquated underground copper lines, frequently does not allow for speeds above 1 Mbps. In the ITU's ICT Development Index, a composite index which compares developments in ICT across countries, Egypt ranked 100 out of 167 countries in 2015, 11 spots lower than in the previous year.[13]

7 Ministry of Communications and Information Technology (MCIT), "Telecommunications," 2015, http://bit.ly/1F9U4w6.

8 "Percentage of Individuals Using the Internet" International Telecommunication Union, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

9 MCIT, "Key Indicators Viewer," July 2016. http://www.new.egyptictindicators.gov.eg/en/Indicators/_layouts/KeyIndicatorsViewer.aspx.

10 MCIT, "ICT Indicators in Brief," May 2016, http://www.egyptictindicators.gov.eg/en/Publications/PublicationsDoc/ICT%20Indicators%20(May%202016)%20English.pdf, and
The World Bank, "Literacy rate, adult total (% of people ages 15 and above)," 2012, http://bit.ly/1BUA0pA.

11 The World Bank, "Literacy rate, adult total (% of people ages 15 and above)," 2012, http://bit.ly/1BUA0pA.

12 World Bank, "Egypt, Arab Republic," http://data.worldbank.org/country/egypt-arab-republic?display=default.

13 International Telecommunication Union, *Measuring the Information Society Report 2015*, 2015, https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-ES-E.pdf.

Restrictions on Connectivity

The Egyptian government has centralized internet infrastructure and fibe -optic cables into highly controllable "chokepoints."[14] In addition, virtually all of Egypt's telecommunications infrastructure is owned by Telecom Egypt, a state-owned company. The arrangement makes it easy to suspend internet access or decrease speeds, as was the case during the 2011 revolution. From January 27 to February 2, 2011,[15] authorities disabled the country's Border Gateway Protocol Routes, shutting down all internet traffic in less than one hou .[16] Telecommunications companies were then ordered to cut mobile internet and text-messaging services under the terms of strict agreements they had signed with regulators. At the time, state intelligence agencies claimed that "foreign intelligence [was] using communication technologies to plan terrorist actions."[17]

In October 2015, operators confi med news reports that the National Telecommunications Regulatory Authority (NTRA) had blocked VoIP services on mobile networks, although they were denied by the regulator.[18] It is technically prohibited to make international calls from mobile networks under Article 72 of the 2003 Telecommunications Law, which forbids the "by-passing [of] international telephone calls by any means whatsoever."[19] Periodic blockages of VoIP traffic o er mobile networks were found as early as 2010.[20] The debate over VoIP had fla ed up in June 2013 after the NTRA announced the establishment of a committee to "monitor" communications on free messaging apps WhatsApp and Viber, pending a potential decision to block or restrict them. The NTRA stated the rationale was economic.[21] On November 3, 2013, responding to one newspaper's allegations, the NTRA denied that it was considering imposing charges for Viber and WhatsApp use.[22]

ICT Market

The Egyptian mobile phone market is divided between three companies. Vodafone Egypt, which is 55 percent owned by the private company Vodafone, enjoys the greatest market share with 40.5 percent. Mobinil was recently rebranded "Orange Egypt" in March 2016 and has a market share of 33 percent. It is almost 99 percent owned by its French parent company.[23] Finally, Etisalat Misr has a 24 percent market share. The company is 66 percent owned by Etisalat, an Emirati company with strong ties to that country's rulers.[24] The state-owned company, Telecom Egypt, obtained a license to establish a new mobile telephone company in April 2014 but has yet to launch services.

14 James Glanz and John Markoff, "Egypt Leaders Found 'Off' Switch for Internet," *The New York Times*, February 15, 2011, http://nyti.ms/nTX2HK.

15 Erica Chenoweth, "Backfi e in the Arab Spring," Middle East Institute, September 1, 2011, http://bit.ly/1W8Refh.

16 Iljitsch van Beijnum, "How Egypt did (and your government could) shut down the internet," *Ars Technica*, January 30, 2011, http://bit.ly/1i2l5qS.

17 Ameera Fouad, "Saying no to mobile phones," *Ahram Online*, February 2-8, 2012, http://bit.ly/1NIfDWi.

18 "The national regulator responds to the blocking of free calls," *Dot Masr*, October 5, 2015, http://bit.ly/2f0zd2C.

19 Telecommunication Regulation Law No. 10 of February 2003, www.tra.gov.eg/uploads/law/law_en.pdf.

20 "Confusion reigns over the status of Internet calling apps," *Mada Masr*, October 6, 2015, www.madamasr.com/news/confusion-reigns-over-status-internet-calling-apps.

21 "Egypt considers banning Viber, WhatsApp," *Ahram Online*, June 8, 2013, http://bit.ly/1KO112u. x.

22 "NTRA: Viber, WhatsApp, BBM are free and cannot be priced," *Al Masry al Youm*, November 3, 2013, http://bit.ly/1KaMFeZ.

23 "Are you Orange?" *Mada Masr*, March 14, 2016, www.madamasr.com/news/economy/are-you-orange.

24 Etisalat Group, "Results Q4 2015" investor presentation, March 10, 2016, www.etisalat.com/en/system/docs/12-4-2013/Q4-2015-ResultsPresentation.pdf.

In the fi ed-broadband market, Telecom Egypt (under the banner TE Data) controls 63 percent of the ADSL market.[25] Egypt's main internet service providers (ISPs), also known as "Class A" ISPs, are Etisalat Egypt, LINKdotNET, and Vodafone data. These companies lease lines from TE Data and resell bandwidth to over 200 smaller ISPs.

Regulatory Bodies

Mobile service providers and ISPs are regulated by the National Telecommunications Regulatory Authority (NTRA) and governed by the 2003 Telecommunication Regulation Law. The NTRA's board is chaired by the ICT minister and includes representatives from the defense, finance, and in erior ministries; the state security council; the presidency; workers' unions; as well as public figu es, experts, and other military figu es.[26] Officiall , the NTRA is responsible for regulating the telecommunications industry[27] and furthering ICT development through projects like the "eMisr" National Broadband Plan outlined in late 2011.[28] The NTRA also conducts analysis of the telecommunication market and publishes research to encourage investment.

Limits on Content

Egypt blocked two Qatari-owned news sites during the coverage period, marking the first time the authorities had ever used this method of censorship. While one lawsuit to ban Facebook was rejected, another has sprung up, and Facebook's Free Basics service was banned two months after it was instituted. Digital activism has waned amid widespread fear and self-censorship around political organizing, although Egyptians have used satire and comedy to push the boundaries on sensitive issues.

Blocking and Filtering

In an unprecedented move, authorities blocked access to two news sites over the coverage period, signaling a new willingness to engage in politically motivated blocking. Following similar moves by Saudi Arabia and the UAE,[29] in December 2015 Egypt blocked the Qatari-owned news site *al-Araby al-Jadeed* and its English-language equivalent *The New Arab*.[30] The Egyptian government did not acknowledge any decision to block the website. The move may have come under pressure from Saudi and Emirati leaders, given the recent rapprochement between Egypt and the Gulf Arab countries. It also came shortly before the fi th anniversary of the January 25 revolution. As of mid-2016, it remained blocked on most ISPs.

Generally speaking, Egypt rarely blocks political, social, or religious content online. YouTube, Facebook, Twitter and blog-hosting services are freely available, despite numerous attempts to ban them. In August 2015, a court rejected a lawsuit stemming from May 2014 in which a lawyer pressed charges against the prime minister and the minister of telecommunications, arguing that Facebook

25 International Telecommunication Union, "Telecom Egypt Data S.A.E. (TE Data)," accessed July 2015, http://bit.ly/1MmT7TF.
26 National Telecom Regulatory Authority, "Board Members," accessed April 16, 2013, http://bit.ly/1LcI2TJ.
27 National Telecom Regulatory Authority, "NTRA Function and Role," accessed April 16, 2013, http://bit.ly/1URa4oH.
28 National Telecom Regulatory Authority and MCIT, "eMisr National Broadband Plan," 2011, http://bit.ly/1JfcaI7.
29 "Egyptian authorities block access to The New Arab," *The New Arab*, December 31, 2015. https://www.alaraby.co.uk/english/news/2015/12/31/the-new-arab-blocked-in-egypt.
30 "Saudi Arabia, UAE and Egypt block access to Qatari-owned news website," *The Guardian,* January 5, 2016. https://www.theguardian.com/media/2016/jan/05/saudi-arabia-uae-egypt-block-access-qatari-news-website.

is used to spread immorality, rumors, and false news detrimental to the state. The State Litigation Authority argued that blocking Facebook would impede on citizens' constitutional rights, pointing out that millions use the website to share photos and express their opinions. It also added that even repressive countries like Saudi Arabia had not blocked the site. In ultimately rejecting the lawsuit, the court pointed out that the right to access information was a part of citizens' development rights. However, the court added that the state should block content threatening to national security.[31] In January 2016, a similar lawsuit emerged to ban Facebook and its mobile app "for its grave danger to national security and societal peace." As of July 2016, the verdict had had been thrice postponed.[32]

Egyptian courts have consistently ruled to ban pornographic websites.[33] Rulings by administrative courts in 2015 and 2009 were not implemented; a separate court case from 2013 decided against a ban on online pornography.[34] Previously, the ban was estimated to cost as much as EGP 100 million (US$ 14 million),[35] with a significant effect on in ernet speeds. Civil society organizations have objected to the threat of a ban, both on grounds of freedom of expression but also because of the high expense. Nevertheless, several ISPs have implemented the court's decision on a voluntarily basis, offering a "safe internet service" to subscribers.

Content Removal

According to the most recent transparency reports published by Facebook, Google, and Twitter, Egypt has not requested these companies remove user-generated content on their platforms over the past year. Instances of direct government pressure on news sites to remove content are rare, but online journalists did report receiving a directive to refrain from reporting on an event in August 2014. A public prosecutor reportedly issued a gag order targeting news websites regarding the killing of four people by the police on the northern Alamein desert highway.[36] This was the fi st instance of a media gag order that applied to online media alongside print. The Egyptian president has also met occasionally with the editors-in-chief of the main news outlets to admonish them for not towing the line.

Media, Diversity, and Content Manipulation

At a time when traditional media is suffering from what several independent newspaper editors have referred to as unseen level of homogeneity, online media is also struggling to maintain its independence.[37] A survey by researchers at Northwestern University in Qatar found that only 25 percent of Egyptians agreed in 2015 that "The media can report the news independently without interference from officials" down from 27 percent in 2013. Egypt ranked lower than Lebanon, Qatar, Saudi Arabia,

31 "The administrative court merits on the rejection of the lawsuit to ban Facebook in Egypt," *Youm7,* August 25, 2015, http://bit.ly/2ek4jSP.

32 "Today, the court considers a lawsuit to ban Facebook in Egypt for threatening national security," *Youm7,* May 15, 2016, http://bit.ly/2eWfN0n.

33 "Egypt's court orders ban on porn websites," *Ahram Online*, May 20, 2015, http://bit.ly/1Oqs61j.

34 "Egypt prosecutor orders Internet porn ban," *Daily News Egypt*, November 8, 2012, http://bit.ly/1KihwTP.

35 "New case on banning porn websites in Egypt adjourned," *Ahram Online*, June 1, 2013, http://bit.ly/1Oqs61j.

36 Mohamed El Dahshan and Rayna Stamboliyska, *Egypt: News Websites and Alternative Voices*, Article 19 and Heliopolis Institute, 2014, http://www.article19.org/data/files/medialibra y/37780/Egypt-Report-for-Web.pdf.

37 Mohamed El Dahshan and Rayna Stamboliyska, *Egypt: News Websites and Alternative Voices*, Article 19 and Heliopolis Institute, (London: Free World Centre, 2014) http://bit.ly/1KramwE.

Tunisia, and the UAE. Similarly, the amount of people who agreed that "It is okay to express unpopular ideas on the internet" fell from 48 to 45 percent.[38]

Online journalists are often reluctant to cross red lines on sensitive topics, which include sectarian tensions, sexual liberty, the Muslim Brotherhood, detainees, military operations in the Sinai, and the military's outsized role in the national economy. A provision in the August 2015 antiterrorism law criminalizes the publication of any information regarding militant attacks that contradicts official government statements, punishable by two years in prison.[39] Those working for English-language outlets enjoy greater editorial freedom, while Arabic-language reporters fear that critical reports will affect their long-term professional prospects. Many experience online harassment from paid commentators. Those working for outlets affilia ed or aligned with the Muslim Brotherhood face heavy prison sentences and several have been accused of supporting a terrorist organization.[40]

The Egyptian blogosphere has lost much of its vitality over the past few years. Attacks against bloggers have had a chilling effect; the increased popularity of Facebook and Twitter in the aftermath of the 2011 revolution has also led many key writers to focus their attention and content creation there. Registering a local .eg domain requires the submission of personal data and copies of a national ID, as well as a commercial registry for top level domains. Online-only news websites are not recognized by the state as news outlets, unless connected to a print newspaper, making it tough to obtain press credentials, gain access to sources or fact-check information with officials.

The economic viability of independent news websites is constantly under threat, as exemplified by the string of closures and financial difficulties experienced by most. The landscape is domin ed by the online versions of state-owned newspapers or those benefiting f om the backing of government-connected financie s.[41] The most widely read news outlets, per the most recent Alexa ranking, are primarily tabloids, news portals aligned with the government, and sports websites.[42]

Facebook launched its "Free Basics" service in October 2015, which allowed users on the Etisalat mobile network to access certain internet websites and platforms for free. The service was suspended in December, weeks before the fi th anniversary of the January 25 protests, apparently over a licensing issue.[43] However, Reuters later reported that the government may have suspended Free Basics "after the U.S. company refused to give the Egyptian government the ability to spy on users."[44]

Digital Activism

Digital activism and political organizing have been largely subdued over the past several years due to fears of arrest, harsh jail sentences, and even murder by police forces while attending protests. A November 2013 law has effectively banned protest and given free rein to police in cracking down

38 Northwestern University in Qatar, "Media Use in the Middle East, 2015 - A six-nation survey", April 2015, http://bit.ly/1Y41J5f.

39 "Draft Terrorism Law (full text)," [in Arabic] *Al Masry Al Youm*, July 4, 2015, www.almasryalyoum.com/news/details/768074.

40 Mohamed El Dahshan and Rayna Stamboliyska, *Egypt: News Websites and Alternative Voices*, Article 19 and Heliopolis Institute, (London: Free World Centre, 2014) http://bit.ly/1KramwE.

41 Leslie T Chang, "The news website that's keeping press freedom alive in Egypt," *The Guardian*, January 27, 2015, http://bit.ly/1BuOn6k.

42 Alexa, "Top Sites in Egypt," accessed July 18 2016, http://www.alexa.com/topsites/countries/EG.

43 Leila Fadel, "Egypt Cracks Down on Free Facebook Service," National Public Radio, January 3, 2016, http://www.npr.org/2016/01/03/461843931/egypt-cracks-down-on-free-facebook-service

44 "Exclusive: Egypt blocked Facebook Internet service over surveillance – sources," Reuters, April 1, 2016, www.reuters.com/article/us-facebook-egypt-idUSKCN0WY3JZ.

on demonstrations.[45] Given the strong overlap of online and offline activism, especially for political activists, the chilling effect and the overall political disappointments that many have endured since 2011 have led to a decrease in political engagement, both on the streets and in writing. For instance, the website WikiThawra, the most reliable resource tracking numbers of imprisoned protesters, stopped operating in mid-2014, largely due to the organizers' disappointment in the current political situation.[46]

However, some daring Egyptians have used satire and comedy to push the boundaries on political, social, and religious issues. On January 25, 2016, the anniversary of the Egyptian revolution, television comedian Shady Hussein and actor Ahmed Malek recorded and published a prank video in which they distributed "balloons" made of condoms to police recruits on the street. Both Hussein and Malek had been critically injured in revolutionary protests. The video amassed upwards of a million views in one day and resulted in death and legal threats against the two creators.[47]

Violations of User Rights

Several new laws threaten free expression online. An antiterrorism law was passed in August 2015, and a cybercrime law is under consideration. Both laws include harsh penalties for online activities, which activists and observers warn could be used to prosecute dissidents and opposition political parties. Several users have been arrested or imprisoned over the coverage period for laws related to insulting the president, inciting debauchery, or contempt of religion. The monitoring of cyberspace by the authorities remains a high concern.

Legal Environment

Egypt's constitution, amended on January 18, 2014,[48] contains articles that address and nominally guarantee freedom of the press, stating that Egyptians "have the right to own and issue newspapers and establish visual, audio and digital media outlets." According to Article 70, "the law shall regulate ownership and establishment procedures for visual and radio broadcast stations in addition to online newspapers." This wording implies that even online sources of information could be regulated and their owners may be required to seek government approval in order to operate, as is currently the case with newspapers. Article 71 states that censorship is forbidden "in any way" and no individuals should be punished for publications. However, exceptions are made for "times of war or general

45 David D. Kirkpatrick, "New law in Egypt effectively bans street protests," *The New York Times*, November 25, 2013, http://nyti.ms/1EY7Lyi.

46 Thomas Hughes and Emad Mubarak, "Censorship in Egypt: Online and offline" *Mada Masr*, November 30, 2014, http://bit.ly/1P0Jrju.

47 "Egypt TV Personalities Face Arrest for 'Condom Balloons Police Prank' Amid Calls for Boycott," *Egyptian Streets,* January 26, 2016, http://egyptianstreets.com/2016/01/26/egypt-tv-personalities-face-arrest-for-condom-balloons-police-prank-amid-calls-for-boycott/.

48 Draft Constitution of The Arab Republic of Egypt, December 2, 2013, Trans. by International IDEA, http://bit.ly/1eLPdiF.

mobilization," with crimes delineated for "incitement to violence," "discrimination amongst citizens, or impugning the honor of individuals."[49]

Article 211 outlines the establishment of a "National Media Council" tasked with regulating "the affairs of radio, television, and printed and digital press, among others" (Article 211) and ensuring that the press maintains a commitment to "professional and ethical standards, as well as national security needs." Furthermore, Article 57 states that private communications "may only be confisca ed, examined or monitored by causal judicial order, for a limited period of time, and in cases specified by the law." Judicial warrants are needed in order to enter, search, monitor, private property such as homes as specified in A ticle 58. However, the constitution continues to permit the trial of civilians under military courts, to the anger of political activists.[50]

In August 2015, a new antiterrorism law was ratified by the p esident.[51] The bill had been set for changes after criticism from the international community, [52] but was rushed through after the assassination of Prosecutor General Hisham Barakat on June 29, 2015.[53] The antiterrorism legislation classifies a la ger number of crimes as terrorism and provides for the establishment of a "Terrorism Prosecutor's Office" which would likely be subject to fewer checks and appeal provisions than normal civilian courts. One provision would allow the police to monitor internet traffic and social media activity to "prevent their use for terrorist purposes."[54] Furthermore, Article 27 calls for a minimum sentence of fi e years in prison for "setting up a website with the goal of promoting ideas or beliefs inciting to the use of violence, broadcasting information to mislead the police or judicial authorities on terrorism cases, or exchanging messages and issuing orders between terrorist groups or organizations."[55] Setting up a group with the intention of "advocating by any means the obstruction of provisions of the constitution or laws" is punishable by life imprisonment or the death penalty, a charge that, activists pointed out, could apply to any peaceful political party or advocacy group.[56] Finally, journalists face heavy fines for disputing fficial accounts f attacks by militants.

Previously, President el-Sisi issued a separate law in February 2015 broadening the definition f "terrorist entities" to include anyone who threatens public order "by any means," and allowing the state to draw up lists of alleged terrorists or terrorist organizations.[57] The law was met with wide skepticism from legal and rights activists, who criticized that the loose wording of the law could allow the

49 The full text reads, "It is prohibited to censor, confisca e, suspend or shut down Egyptian newspapers and media outlets in any way. Exception may be made for limited censorship in time of war or general mobilization. No custodial sanction shall be imposed for crimes committed by way of publication or the public nature thereof. Punishments for crimes connected with incitement to violence or discrimination amongst citizens, or impugning the honor of individuals are specified by la ." Miriam Rizk and Osman El Sharnoubi, "Egypt's constitution 2013 vs. 2012: A comparison," *Ahram Online*, December 12, 2013, http://bit.ly/1boZjtj.

50 "Egypt panel approves 'conditional military trials of civilians'," *Ahram Online*, November 21, 2013, http://bit.ly/1EY7StE.

51 "Egypt's al-Sisi imposes strict anti-terrorism laws," BBC News, August 17, 2015, http://www.bbc.com/news/world-middle-east-33955894.

52 José Gonzalez, "Egyptian draft anti-terror laws pose a threat to freedom of expression," Canadian Journalists for Free Expression, May 5, 2014, https://cjfe.org/resources/features/egyptian-draft-anti-terror-laws-pose-threat-free-expression; Erin Cunningham, "Egyptian draft laws to widen 'terror' definition drawing fi ce criticism," *The Washington Post,* April 22, 2014, http://wapo.st/1QAuyBA.

53 Mai El-Sadany, "Yet Another Terrorism Law," The Tahrir Institute for Middle East Policy, July 6, 2015, http://bit.ly/1KO98Cb.

54 Al Hussaini,"Egypt's Anti-Terrorism Law to Target Internet."

55 Al Hussaini,"Egypt's Anti-Terrorism Law to Target Internet."

56 Cairo Institute for Human Rights Studies, "Egypt's draft anti-terrorism laws constitute greatest threat to civil liberties in 37 years," IFEX, April 30, 2014, http://bit.ly/1KraMDe.

57 Sarah El Deeb, "Egyptian president issues new anti-terrorism law," *Yahoo News,* 24 February 2015, http://yhoo.it/1Kid3k9.

state to consider political parties, student unions, political movements, and human rights organizations as terrorist organizations.[58]

A new cybercrime law was approved by the Council of Ministers in April 2015, approved by parliament in May 2016 and as of mid-2016 awaited ratification by the president. The harbinger of this law was the 2014 constitution itself, which stated in Article 34 that "The security of cyberspace is an integral part of the economic system and national security. The State shall take the necessary measures to preserve it, as regulated by Law," which led free speech activists at the time to warn of a potential crackdown on online freedom of expression. The draft law outlined penalties for incitement, terrorism, religious intimidation, and the use of personal photos and videos for blackmail. It also allows law enforcement agencies to submit requests to block websites deemed to threaten national security, a term that has traditionally been used as an excuse to enforce censorship on political opponents, journalists, and activists.[59] The law also gives empowers "Security authorities (the Presidency – the armed forces – the ministry of interior – the intelligence services)" to confisca e equipment, censor content, and arrest individuals.[60]

Prosecutions and Detentions for Online Activities

Egyptians continue to face stark penalties for their online activities. In previous years, the government had mainly targeted members of organized opposition movements, such as the Muslim Brotherhood or April 6 Movement. This year authorities went after dancers, comedians, teenagers, and cartoonists with the same prosecutorial zeal.

- In October 2015, a military court sentenced 22-year-old Amr Nohan to three years in prison for several posts on social media, including a picture of President Sisi with "Mickey Mouse ears" added to his head. He was finishing compulso y military duty at the time of his arrest. During the trial, investigators admitted to monitoring and tampering with his Facebook account.[61]

- In May 2016, the police arrested all six members of the satirical comedy group "The Street Children" and charged them with "inciting people against the authorities, forming a group that stands against state principles, and attempting to topple the regime." Earlier that month, the group had uploaded two satirical videos that had criticized President Sisi.[62] Their arrest was widely condemned by Egyptian media, including some prominent supporters of the president. An online petition was drafted calling for their release. They were detained some 150 days and faced sentences of three to fi e years in prison for insulting the president.[63]

58 Enas Hammad,"Egypt's terrorism law whittles down opposition," *Al Monitor*, March 2, 2015, http://bit.ly/1KlYSig.

59 Ragab Saad, "Egypt's Draft Cybercrime Law Undermines Freedom of Expression", Atlantic Council, April 24, 2015, http://bit.ly/1Eofymq; For the full text of the law, see "Al-Watan publishes the text of the draft cybercrime law submitted to the parliament," [in Arabic] *Al-Watan*, May 11, 2016. http://bit.ly/2dA6svQ.

60 AFTE, *Technical Hostility*, June 2016. http://eipr.org/sites/default/files/ eports/pdf/cybercrime.pdf.

61 Imogen Calderwood, "Egyptian law student, 22, jailed for three years after posting image of President Sisi wearing Mickey Mouse ears on Facebook," *The Daily Mail*, December 19, 2015, http://www.dailymail.co.uk/news/article-3367182/Egyptian-law-student-22-jailed-three-years-posting-image-President-Sisi-wearing-Mickey-Mouse-ears-Facebook.html#ixzz4OQLT0sJY.

62 "'Street Children' band members released," *Daily News Egypt*, September 7, 2016. www.dailynewsegypt.com/2016/09/07/street-children-band-members-released/.

63 George Mikhail, "Satire leads Egypt youth troupe to prison," *Al Monitor,* May 18, 2016, http://www.al-monitor.com/pulse/originals/2016/05/egypt-arrest-satire-troupe-street-children-sisi-charges.html.

Several individuals were jailed for online videos that were deemed to have insulted the honor or image of Egyptian women.

- On September 3, 2015, two belly dancers were each sentenced to six months in prison for "inciting debauchery" through their music videos uploaded to YouTube. Suha Mohammed Ali and Dalia Kamal Youssef, known by their stage names of Shakira and Bardis, were arrested following lawsuits filed against them by law ers who claimed the two women constituted an "outrage to public morality and harmed the image of Egyptian women."[64]

- On March 13, 2016, Taymour el-Sobki, the son of a TV director and the administrator of a misogynist Facebook page, was sentenced to three years for "insulting Egypt's women." He was targeted for stating that "most women are prone to adultery" on a television interview broadcasted in 2015. Although the interview did not spark any outrage at the time, a short clip from the episode went viral on social media and prompted a lawsuit against el-Sobki.[65]

Egyptians were targeted for addressing religious taboos. For example:

- In February 2016, four teenagers—Moller Yasa, Albir Shehata, and Bassem Younan, and Klenton Faragalla were sentenced to fi e years in prison for a YouTube video mocking the so-called Islamic State, including a fake execution. All four are Christian and had been accused by neighbors of insulting Islam in their video. They were detained for two months, released on bail, and went into self-imposed exile in Turkey, and later, Switzerland where they were seeking asylum as of September 2016.[66] Their teacher, Gad Youssef Younan, was also sentenced to three years.[67]

- In March 2016, al-Sayed Youssef el-Naggar was arrested for a Facebook post calling for the burning of Islamic jurisprudence books he perceived as supporting extremism. He was arrested in front of al-Azhar mosque, where he had planned to burn the books,[68] and sentenced to one year in prison. His appeal case was rejected in September 2016.[69]

- In January 2016, prominent poet and columnist Fatima Naoot was sentenced to three years in prison for "contempt of religion" for a Facebook post in which she criticized the tradition of slaughtering sheep for the annual religious holiday of Eid El Adha.[70] She

64 "Egyptian belly dancers jailed for 'inciting debauchery," BBC, September 3, 2015. www.bbc.co.uk/news/world-middle-east-34140406.

65 "Taymour El Sobki sentenced to three years for "insulting Egypt's women," *Al Masry al Youm,* March 13, 2016, http://today.almasryalyoum.com/article2.aspx?ArticleID=497630&IssueID=3899.

66 Luiz Sanchez, "Coptic teenagers accused of insulting religion seek asylum in Switzerland," *Mada Masr*, September 6, 2016, http://www.madamasr.com/en/2016/09/06/feature/politics/coptic-teenagers-accused-of-insulting-religion-seek-asylum-in-switzerland/.

67 "Egypt sentences 4 Coptic students to 5 years in jail for contempt of Islamic religion," *Ahram Online*, February 25, 2016. http://english.ahram.org.eg/NewsContent/1/64/188505/Egypt/Politics-/UPDATED-Egypt-sentences--Coptic-students-to--years.aspx.

68 Association for Freedom of Thought and Expression, "Renewal of detention of a citizen for calling to burn the Al-Bukhari book," March 7, 2016, http://afteegypt.org/uncategorized/2016/03/07/11905-afteegypt.html.

69 "Confi mation of the detention of a citizen accused of attempting to burn Al Bukhari's compendium," *Cairo Live*, September 21, 2016, http://zahma.cairolive.com/?p=59434.

70 "Egyptian writer Fatima Naoot sentenced to 3 years in jail for 'contempt of religion'," *Ahram Online*, January 26, 2016. http://english.ahram.org.eg/NewsContent/1/64/185963/Egypt/Politics-/Egyptian-writer-Fatima-Naoot-sentenced-to--years-i.aspx.

had originally posted the comment in October 2014 and was on trial for approximately one year. The decision was being appealed by Naoot.[71]

Authorities used technology to entrap sexual and gender minorities accused of performing illegal acts.

- On April 13, 2016, the "Vice Police" engaged in online conversations with a homosexual man who allegedly offered sex in exchange for money. The man was later arrested for "inciting debauchery."[72]
- Similarly, police announced the arrest of a transsexual woman in May 2016 on charges of prostitution. Police reportedly set up a meeting with the accused via Facebook and she was promptly arrested. In national coverage, the accused was called an offensive epithet.[73]

Several prominent digital activists and online journalists remain in prison on serious charges. In many cases, individuals faced charges unrelated to their online activities, although the intentions of the authorities were clear. For example, Alaa Abdel Fattah, a prominent blogger and leading figure in the 2011 revolution, was sentenced to five years in prison on February 23, 2015 along with 24 other defendants for a brief protest on November 26, 2013. The demonstrators were taking a stand against newly passed legislation that effectively criminalized any protests without government permission.[74] In June 2016, the UN Working Group on Arbitrary Detention issued a legal opinion[75] stating that Abdel Fattah was being detained arbitrarily and calling on the Egyptian government to immediately release him.[76]

Surveillance, Privacy, and Anonymity

Surveillance and monitoring are a wide concern in the country, given the tense environment in which numerous users have been arrested for their online activities. In July 2015, Italian surveillance software manufacturer Hacking Team was hacked, and a 400 GB trove of company emails and emails was dumped online. The emails confirmed what some experts had already reported,[77] namely that Egypt had acquired Hacking Team's "Remote Control System" (RCS), a spyware technology marketed as "the hacking suite for governmental interception" and can capture data on the target's computer; monitor encrypted internet communications; record Skype calls, emails, messages, and passwords typed into a browser; and remotely turn on a device's webcam and microphone.[78] The leak produced

71 "Appeal against Fatima Naoot sentence dropped, another appeal to be filed soon" *Mada Masr*, March 31, 2016, http://www.madamasr.com/en/2016/03/31/news/u/appeal-against-fatima-naoot-sentence-dropped-another-appeal-to-be-filed soon/.

72 "Vice police entraps a sexual deviant on the internet" *Youm7*, April 13, 2016, http://bit.ly/2f0PMez.

73 "The Arrest of Facebook's most famous shemale in a wig and a dress in Sheikh Zayed," *Youm7*, May 2, 2016, http://bit.ly/2eNQg8v.

74 "Alaa Abdel Fattah: Egypt jails activist-blogger for five years," *BBC News*, February 23, 2015, http://bbc.in/17MgxiI.

75 United Nations Human Rights Council, "Opinion No. 6/2016 concerning Alaa Ahmed Seif al Islam Abd El Fattah (Arab Republic of Egypt)", 6 June 2016. www.ohchr.org/Documents/Issues/Detention/Opinions/Session75/Opinion_2016_6_Egypt.pdf.

76 EFF", Alaa Abd El Fattah Must Be Released, Says UN Working Group on Arbitrary Detention," July 5, 2016, https://www.eff.org/deeplinks/2016/07/alaa-abd-el-fattah-must-be-released-says-un-working-group-arbitrary-detention.

77 Bill Marczak, et al., "Mapping Hacking Team's 'Untraceable' Software," Citizen Lab, February 17, 2014, http://bit.ly/1kPDo0Y.

78 Cora Currier, Morgan Marquis-Boire, "A detailed look at Hacking Team's Emails about its repressive clients," *The Intercept*, July 7, 2015. https://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/.

invoices showing that the Egyptian Ministry of Defense, and possibly other institutions, paid EUR 737,500 (US$ 845,000) to the company through a third-party intermediary.[79] In addition, a February 2016 report by Privacy International concluded that a branch of the Egyptian security apparatus, the "Technical Research Department," had also purchased surveillance equipment from Nokia Siemens Network (NSN) in the past through various joint ventures and subsidiaries.[80]

Several regulations on SIM card registration or the use of anonymizers restrict the ability of Egyptians to use the internet anonymously. Mobile phone customers must provide their National ID numbers to their providers.

After some 13 million phone lines had been shut off as part of a campaign to disconnect service from all unregistered SIM cards in 2014 and 2015,[81] the NTRA issued a regulation in May 2015 limiting the sale of SIM cards to the official branches f the three mobile operators and imposed even stricter registration requirements[82] in a bid to prevent reselling of SIM cards.[83] In February, the NTRA announced that it had finalized the dra t for a "Unified Contract" for the sale f SIM cards by all three companies, which is yet to be implemented.[84]

Encryption is also restricted within the country. According to the Egyptian Telecommunications Law, "telecommunication services operators, providers, their employees and users of such services shall not use any Telecommunication Services encryption equipment except after obtaining a written consent from each of the NTRA, the Armed Forces and National Security Entities, and this shall not apply to encryption equipment of radio and television broadcasting."[85]

Cooperation between private companies and the government in handing over user data is thought to be extensive. ISPs and mobile operators are obliged to maintain a database of their customers and allow government access to their databases. In the past, details emerged that mobile operators Vodafone, Mobinil, and Etisalat had to sign terms of agreement that bound them to cooperate with government officials when equested to tap any conversation or monitor any discussion. In an interview, Mobinil founder Naguib Sawiris stated that under the company's terms of agreement, the government had the right to cancel any or all mobile services in the absence of cooperation.[86]

Intimidation and Violence

Amid sectarian tensions in the country, individuals have been attacked in retribution for Facebook posts deemed to insult religion. The perpetrators of this type of violence are rarely held accountable,

79 Emir Nader, "Egypt's purchase of hacking software documented in new leaks," *Daily News Egypt*, July 6, 2015, http://bit.ly/1J1X35m.

80 J.M. Porup, "European spy tech sold to ultra-secret branch of Egyptian gov't, claims new report," *Ars Technica*, February 25, 2016, http://arstechnica.co.uk/security/2016/02/european-spy-tech-sold-to-secret-branch-of-egyptian-intelligence-claims-new-report/.

81 "The NTRA extends the bad on selling mobile lines outside of main stores for two months," *Youm7*, November 17, 2015, http://bit.ly/2eYL0zC.

82 "The legislation preventing the sale of mobile lines outside of company branches enters in force tomorrow," *Sada El Balad*, May 19, 2015, http://www.elbalad.news/1540046.

83 "The ban on mobile lines sales costs vendors 125 million pounds of losses," *Al Borsa*, October 14, 2015, http://bit.ly/1Lv1j2C.

84 "The NTRA plans on renewing the regulation limiting the sale of mobile lines", *Al Mal*, February 2, 2015. www.almalnews.com/Pages/StoryDetails.aspx?ID=268557.

85 Telecommunication Regulation Law No. 10.

86 Stephanie Baker and Mahmoud Kassem, "Billionaire Facing Death Threats Says Egypt Risks Becoming Iran," *Bloomberg Markets* (blog), *Bloomberg Business*, October 26, 2011, http://bloom.bg/rXPGQE.

with the police or judiciary turning a blind eye and sometimes targeting victims rather than aggressors. For example, in late May 2015, 18 members of 5 Christian families from a village in Upper Egypt were expelled from their homes after one man allegedly published a Facebook post insulting the prophet Mohamed. Groups of villagers gathered outside their houses and demanded they leave the village, all under the approval of security forces. According to the TV presenter who broke the story nationally, the man accused of writing the post is in fact illiterate.[87]

Students also suffer administrative consequences for their online posts. On March 8, 2016, the University of Mansoura suspended a student and announced it will investigate nine others over Facebook comments criticizing the university and some of its professors. Abdallah Azmy Ismail, an engineering student, was suspended for a full semester for comments made during an online discussion. The school's student union issued a statement condemning the university, pointing out that the school's arbitrary treatment of the students "has reached the point of utilizing personal disagreements between students on social media which would have occurred outside of the university campus to take action against them inside the school."[88]

Technical Attacks

Technical violence is not widespread, with only a few instances of hacking and defacement reported during the past year. On August 14, 2015, during the second anniversary of the dispersal of the pro-Mohamed Morsi sit-in in the squares of al-Nahda and Raba'a al-Adaweya that left at least 817 dead, the website of Cairo Airport was hacked.[89] On October 22, the official ebsite of the cabinet, as well as that of the Information and Decision Support Centre (IDSC), a government think-tank, were briefly defaced. The attack was claimed by a g oup called "Anonymous R4bia Team," in reference to Raba'a al-Adaweya.[90] In May 2016, an information sharing service for airlines reported that Egypt had notified airlines f attempts to jam the GPS signal around Cairo airport, possibly by hackers.[91]

87 "Host: 5 Christian families forced from homes over after member accused of insulting Prophet Mohamed," *Egypt Independent,* June 1, 2015, http://bit.ly/1FlnhUP.

88 "School of Engineering of Mansoura suspends a student and investigates nine others for criticizing the school on Facebook," *Youm7*, March 12, 2016, http://bit.ly/2fwHE9W.

89 "Cairo airport website hacked as Egyptians mark massacre," Al Jazeera, August 14, 2015, www.aljazeera.com/news/2015/08/cairo-airport-website-hacked-egyptians-mark-massacre-150814095238267.html.

90 "Egypt's official cabinet ebsite hacked," *Ahram Online,* October 22, 2015, http://english.ahram.org.eg/NewsContent/1/64/161573/Egypt/Politics-/Egypts-official-cabine -website-hacked-.aspx.

91 India Ashok, "Egypt warns of hackers jamming GPS signals in Cairo airport," *International Business Times*, May 30, 2016, www.ibtimes.co.uk/egypt-warns-hackers-jamming-gps-signals-cairo-airport-1562693.

Freedom House

Estonia

	2015	2016
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	1	0
Limits on Content (0-35)	3	3
Violations of User Rights (0-40)	3	3
TOTAL* (0-100)	**7**	**6**

* 0=most free, 100=least free

Population:	**1.3 million**
Internet Penetration 2015 (ITU):	**88 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2016 Status:	**Free**

Key Developments: June 2015 – May 2016

- Estonia continues to be one of the most digitally advanced countries in the world. The Estonian Internet Foundation has consolidated its role in raising awareness about key concerns surrounding digital trends and governance of the free internet (see **Availability and Ease of Access** and **Regulatory Bodies**).
- In June 2015, the European Court of Human Rights upheld an Estonian Supreme Court decision from 2009, stating that content hosts may be held legally liable for third-party comments made on their websites. Since then, major online media publications have removed the functionality for anonymous comments on their websites and continued active moderation to limit hate speech (see **Content Removal**).

Introduction

Estonia's advanced internet freedom environment continued to make gains thanks to increased internet access and online participation among citizens.

Estonia in one of the most wired and technologically advanced countries in the world. With a high internet penetration rate, widespread e-commerce, and e-government services embedded into the daily lives of individuals and organizations, Estonia has become a model for free and open internet access as a development engine for society. When the country regained independence in 1991 after nearly 50 years of Soviet rule, its infrastructure was in a disastrous condition. The country's new leadership, however, perceived the expansion of information and communication technologies (ICTs) as a key to sustained economic growth and invested heavily in their development. This progress has continued with support of all following governments.

After the first internet connections in the country were introduced in 1992 at academic facilities in Tallinn and Tartu, the government further worked with private and academic entities to initiate a program in 1996 called Tiger Leap, which aimed to establish computers and internet connections in all Estonian schools by 2000. This program helped build a general level of technological competence and awareness of ICTs among Estonians. Today, with a high level of computer literacy and connectivity already established, the program's focus has shifted from basic concerns such as access, quality, and cost of internet services to discussions about security, anonymity, the protection of private information, and citizens' rights on the internet. In addition, the majority of users conduct business and e-government transactions over the internet: in 2016, 99.6 percent of banking transactions were done with e-banking services, and 96 percent of people declared their income electronically.[1]

With regard to freedom of expression online, recent court rulings on intermediary liability in Estonia have posed some concerns. On June 16, 2015, the Grand Chamber of the European Court of Human Rights (ECtHR) issued a ruling that reaffirmed an earlier Estonian Supreme Court decision regarding the legal liability of content hosts for third-party comments. The Grand Chamber of the ECtHR found that a company's legal liability for comments posted by its users did not sufficiently interfere with the freedom of expression guarantees enshrined in the European Convention on Human Rights; therefore, intermediaries could be held responsible for third-party content published on their website or forum, even if they delete the content upon notification.[2] Since February 2016, several major media companies have removed anonymous comments functions from their online portals.

Over the past couple of years, the issue of privacy for individual users on the internet has become a widely debated topic in Estonia, with a particular focus on the privacy policies of global service providers. The Digital Agenda 2020 for Estonia, established by the Ministry of Economic Affairs and Communications, outlines how both technological and organizational conditions will be developed to ensure that people will always know and be able to decide when, by whom, and for what purpose their personal data is being used in the public sector.[3] The same agenda also launched an "e-residency" program to offer its secure and convenient online services to the citizens of other countries. Services include digital authentication, digital signatures, encrypted transmission of documents

1 Estonian Information System's Authority, "Facts about e-Estonia," accessed June 2, 2016, http://bit.ly/2cjJcTH
2 European Court of Human Rights, Case of Delfi AS v. Estonia, Judgement, June 16, 2015, http://bit.ly/1hu6nIr.
3 Digital agenda 2020 for Estonia, accessed June 11, 2016, http://bit.ly/2dENc0n

and other electronic communications, and access to all Estonian public and private sector online services.[4]

Obstacles to Access

Estonia continues to be one of the most connected countries in the world with regard to internet access, and Estonian internet users face very few obstacles when it comes to accessing the internet.

Availability and Ease of Access

The number of internet and mobile telephone users in Estonia has grown rapidly in the past 20 years. According to statistics from the International Telecommunication Union (ITU), internet penetration in Estonia reached 88.4 percent in 2015, compared to 84 percent in 2014 and 79 percent in 2013.[5] There were also nearly 2 million mobile phone subscriptions in 2015, translating to a mobile phone penetration rate of 148 percent.[6] This figu e is commonly attributed to the widespread use of internet-enabled mobile devices, the growing popularity of machine-to-machine (M2M) services, and the use of more than one mobile phone by individual Estonians.

The fi st public Wi-Fi area was launched in 2001, and since then, the country has developed a system of mobile data networks that enable widespread wireless broadband access. In 2011, the country had over 2,440 free, certified Wi-Fi a eas meant for public use, including at cafes, hotels, hospitals, schools, and gas stations, and the government has continued to invest in public Wi-Fi.[7] In addition, a countrywide wireless internet service based on CDMA technology has been deployed and is priced to compete with fi ed broadband access. Three mobile operators cover the country with mobile 3G and 3.5G services, and as of April 2016, 4G services covered over 98 percent of Estonian territory.[8] Municipalities in rural areas have been subsidizing local fiber and wi eless internet deployment efforts, and the country's regulatory framework presents low barriers to market entry, enabling local startups to proliferate.

Estonians use a large variety of internet applications, including search engines (85 percent of users), email (83 percent of users), local online media, news portals, social-networking sites, instant messaging, and Voice over Internet Protocol (VoIP) services.[9] Estonian Public Broadcasting delivers all radio channels and its own TV production services, including news in real time over the internet; it also offers archives of its radio and television programs at no charge to users.

4 "What is e-Residency?" e-estonia.com, accessed June 22, 2016, http://bit.ly/2dEOWqz

5 International Telecommunication Union (ITU), "Percentage of individuals using the Internet 2000-2015," accessed October 10, 2016, http://bit.ly/1cblxxY.

6 International Telecommunication Union (ITU), "Mobile-cellular subscriptions 2000-2015," accessed October 10, 2016, http://bit.ly/1cblxxY.

7 Public Wi-Fi Hotspot database in Estonia, accessed June 15, 2016, http://wifi.ee/leviala/

8 Annual report of the Estonian Technical Regulatory Authority 2015, accessed June 25, 2016 http://bit.ly/2eJ8EAf.

9 Pille Pruulmann-Vengerfeldt, Margit Keller, and Kristina Reinsalu, "1.1.4 Quality of Life and Civic Involvement in Information Society," *Information Society Yearbook 2009* (Tallinn: Ministry of Economic Affairs and Communications, 2010), http://bit.ly/2eofxJA.

Restrictions on Connectivity

There were no government-imposed restrictions or disruptions to internet access during the past years.

ICT Market

The Estonian Electronic Communications Act was passed in late 2004 and has been bolstered by a number of amendments added to help develop and promote a free market and fair competition in electronic communications services.[10] Today, there are over 200 operators offering such services, including six mobile operators and numerous internet service providers (ISPs). ISPs and other communications companies are required to register with the Estonian Technical Regulatory Authority, a branch of the Ministry of Economic Affairs and Communications, though there is no registration fee.[11]

Regulatory Bodies

The main bodies in charge of regulatory issues in the telecommunications sector include the Technical Regulatory Authority and the Estonian Competition Authority. There have been no recent known cases of government interference with the telecommunications sector through regulatory bodies, or of regulators abusing their powers.

The Estonian Internet Foundation has taken an increasingly larger role in discussions and awareness-building surrounding key concerns about digital trends and governance of the free internet, notably by organizing "Internet Day" annual conferences since 2015.[12] The foundation was established in 2009 to manage Estonia's top level domain, ".ee."[13] With its multi-stakeholder foundation, the organization represents the Estonian internet community internationally and has succeeded in overseeing various internet governance issues such as the domain name registration process. In February 2012, the Estonian Internet Foundation was admitted to the Council of European National Top Level Domain Registries (CENTR). During last three years the domain registration and annual fees have dropped from a €20 annual fee to a €7 annual fee, together with a 40 percent decrease in the registrar's deposit, a decrease in the registrar's service fees, and an unlimited number of domains for each user.[14]

Limits on Content

Estonians have access to a wide range of content online, and very few resources are blocked or filtered by the government. However, a 2009 court ruling on intermediary liability for third-party comments was upheld by several European Court of Human Rights decisions, including most recently in June

10 "Electronic Communications Act," Ministry of Economic Affairs and Communications, accessed October 11, 2016, http://bit.ly/2eoeKbB.

11 Technical Regulatory Authority, "Commencement of Provision of Communications Service," accessed February 15, 2015, http://bit.ly/2dSKMtP.

12 Interneti Päev, accessed June 2, 2016, http://päev.internet.ee/2016.

13 Estonian Internet Foundation, accessed June 30, 2016, http://www.internet.ee/en/.

14 ".ee domain price to drop to 7 euros", Estonian Internet Foundation, accessed June 1, 2016, http://bit.ly/2dSKCTf.

2015, which may increase censorship or content removal, particularly on forums or other websites with public comment sections.

Blocking and Filtering

There are very few restrictions on internet content and communications in Estonia. YouTube, Facebook, Twitter, LinkedIn and many other international video-sharing and social-networking sites are widely available and popular. Estonians use the internet for uploading and sharing original content such as photographs, music, and text—a higher percentage of people in Estonia (32 percent) use the internet to publically share self-created content than do people in any other country in Europe.[15]

A 2010 law on online gambling requires all domestic and foreign gambling sites to obtain a special license or face access restrictions. As of February 2016, the Estonian Tax and Customs Board had over 1,000 websites on its list of illegal online gambling sites that Estonian ISPs are required to block.[16] The list of blocked sites is transparent and available to the public.

Content Removal

There have been some instances of content removal related to online communications. Most of these cases involve civil court orders to remove inappropriate or off-topic reader comments from online news sites. Comments are also sometimes removed from online discussion forums and other sites. Generally, users are informed about a given website's privacy policy and rules for commenting, which they are expected to follow. Most of the popular online services have established policies that outline a code of conduct for the responsible and ethical use of their services and have enforcement policies in place.

In June 2015, the Grand Chamber of the European Court of Human Rights (ECtHR) upheld a 2009 Estonian Supreme Court decision establishing intermediary liability over third-party comments on internet news portals.[17] The debate began in 2008 when the victim of unflat ering and largely anonymous comments on a news story filed suit against the popular Es onian news site *Delfi*, claiming that the web portal must be held responsible for defamatory reader comments and screen them before they become public.[18] In 2009, the Estonian Supreme Court upheld the rulings of lower courts, stating that *Delfi* was not a passive intermediary since the site already exerted control over its comments section by removing those that violate their own rules; therefore, it could be held liable for defamatory or otherwise illegal content prior to publication. Website owners argued that they did not have the capacity to monitor and edit all comments made on their sites.

The Estonian Supreme Court ruling was previously upheld in October 2013 by the European Court of Human Rights, which stated that the company's liability for defamatory comments was not a "disproportionate interference" with Article 10 of the European Convention on Human Rights guaranteeing

15 "Individuals Using the Internet for Uploading Self-Created Content to Any Website to Be Shared," Eurostat, accessed June 11, 2015,http://bit.ly/2dItUGb.

16 The list of restricted websites can be found on the Estonian Tax and Customs Board website: "Ebaseadusliku kaughasartmängu serverite domeeninimed" [Illegal gaming servers, domain names], Tax and Customs Board, accessed June 10, 2016, http://bit.ly/2d56Gw1.

17 "CASE OF DELFI AS v. ESTONIA", Grand Chamber judgment, accessed June 18, 2015, http://bit.ly/1hu6nIr.

18 Kaja Koovit, "Big Businessman Goes to War Against Web Portals," Baltic Business News, March 18, 2008, http://bit.ly/2dND70r.

freedom of expression.[19] The case was then referred to the Grand Chamber of the European Court of Human Rights, which also upheld the decision June 2015.

Beginning in February 2016, one of the major independent media companies, Postimees Grupp, discontinued the possibility for anonymous comments on its online portals in February 2016. The public broadcasting ERR followed suit, while the independent media house Ekspress Group added a registration system for its online comments section. As a result, the number of comments on online outlets has reportedly declined.[20]

Media, Diversity, and Content Manipulation

Estonians have access to a wide array of content online, and there are few economic or political barriers to posting diverse types of content, including different types of news and opinions.

Additionally, Estonia has the largest functioning public-key infrastructure[21] in Europe, based on the use of electronic certifica es maintained on the national identification (ID) ca d. More than 1.2 million active ID cards are in use, which enable both electronic authentication and digital signing, and over 40 percent of active ID cards have been used for these purposes.[22] The Digital Signature Act, adopted in 2000,[23] gives an individual's digital signature the same weight as a handwritten one and requires public authorities to accept digitally-signed documents. Estonian ID cards were used to facilitate electronic voting during the parliamentary elections in 2007 and were used again in the 2009 municipal and European Parliament elections. During parliamentary elections in March 2015, 176,491 votes were cast over the internet, representing over 30 percent of all votes from Estonia.[24] In 2016, 96 percent of citizens filed their ta es online, making the web services offered by the tax department the most popular public e-service. Over 63 percent of internet users regularly use e-government services, and 77 percent of these users have indicated their satisfaction with such services.[25]

Digital Activism

Social media use in Estonia is fairly widespread, and Estonians often make use of such sites to share news and information and generate public discussion about current political debates. In addition to discussions, netizens also actively participate in online petitions that can be initiated by anybody and joined for free.[26]

19 "European Court strikes serious blow to free speech," ARTICLE 19, October 14, 2013, http://bit.ly/1Bf9pcV.

20 Postimees, "Hate speech a security threat," Eurotopics.net, January 4, 2016, http://bit.ly/2d8kYrf.

21 A public-key infrastructure (PKI) is a system for the creation, storage, and distribution of digital certificates, which are used to verify that a particular public key belongs to a certain entity. The PKI creates digital certificates that map public keys to entities, securely stores these certificates in a central repository, and revokes them if needed.

22 See the web portal for the ID-card system, http://id.ee/?lang=en.

23 "Digitaalallkirja seadus" [Digital Signature Act], Riigi Teataja, accessed May 21, 2013, http://bit.ly/2di154f.

24 Vabariigi Valimiskomisjon (Electoral Commission), "Statistics about Internet Voting in Estonia," accessed October 11, 2016 http://bit.ly/2e3L9Qz.

25 Kristina Randver, *Kodanike rahulolu riigi poolt pakutavate avalike e-teenustega, Jaanuar 2010* [Citizens' Satisfaction with the Provision of Public E-Services, January 2010] (Tallinn: TNS Emor, 2010), http://bit.ly/2da2nL8.

26 Petitsioon [Petitions], accessed October 11, 2016, http://petitsioon.ee

Violations of User Rights

Freedom of speech and freedom of expression are protected by Estonia's constitution and by the country's obligations as a member state of the European Union. Anonymity is unrestricted, and there have been extensive public discussions on anonymity and the respectful use of the internet. Internet access at public access points can be obtained without prior registration. Over the past few years, the government has succeeded in reducing the number and severity of cyberattacks against its infrastructure.

Legal Environment

According to the constitution of Estonia, everyone has the right to freely obtain information and to freely disseminate ideas, opinions, beliefs, and other information. In addition, everyone has the right to the confidentiality of messages sent or received. In general, these rights are well protected. Any restrictions on these rights must be necessary in a democratic society and shall not distort the nature of the rights and freedoms restricted.[27]

Narrow limits on freedom of expression relate to the incitement of national, racial, religious or political hatred, violence, or discrimination, which are prohibited and punishable by law. Estonia is currently in the process of amending the penal code to establish a framework on hate speech criminalization in the country and thereby comply with the European Council Framework Decision 2008/913/JHA,[28] issued November 28, 2008, on "combating certain forms and expressions of racism and xenophobia by means of criminal law." In July 2012, the Ministry of Justice initiated proceedings to amend sections 151 and 152 of the penal code, which would lead to a new legal norm regarding hate speech-related legislation in Estonia.[29] This process was previously a topic of significant public debate within the country, but the present government has taken more cautious positions on proceeding with this initiative.

Prosecutions and Detentions for Online Activities

There were no cases of prosecutions or detentions for online activities during the coverage period.

Surveillance, Privacy, and Anonymity

Estonia has strong privacy protections for its citizens. The Personal Data Protection Act (PDPA), first passed in 1996 and updated in 2008,[30] restricts the collection and public dissemination of an individual's personal data. No personal information that is considered sensitive—such as political opinions, religious or philosophical beliefs, ethnic or racial origin, sexual behavior, health, or criminal convictions—can be processed without the consent of the individual. The Data Protection Inspectorate

27 Constitution of the Republic of Estonia [English translation], June 28, 1992, http://bit.ly/2dIm4MT.

28 EUR-Lex, "Access to European Union Law," accessed May 5, 2013, http://bit.ly/2d4YKuV.

29 Office of the High Commissioner for Human Rights, "Tenth and Eleventh Periodic Report on the implementation of the International Convention on the Elimination of all forms of Racial Discrimination in Estonia," January 2013, http://bit.ly/2e6xqtx.

30 Estonian Data Protection Inspectorate, "Inspectorate," March 14, 2015, http://bit.ly/2dYLoNz.

(DPI) is the supervisory authority for the PDPA, tasked with "state supervision of the processing of personal data, management of databases, and access to public information."[31]

In 2015, the Chancellor of Justice (Ombudsman) processed several cases related to online privacy and data protection.[32] The Ombudsman is an independent official whose duties a e to ensure that legislation in Estonia complies with the constitution, and that the fundamental rights and freedoms of the Estonian people are protected. In three cases during the spring of 2015, the Chancellor strongly and clearly argued for the users' right to privacy with regard to the protection of private data in public databases. The Chancellor of Justice's office has ta en a leading role in interpreting the constitution in cases related to privacy and private information on the internet in Estonia, establishing new standards for the protection of user rights online.

Data retention practices established under the 2005 Electronic Communications Act,[33] which aligned with EU legislation, were thrown into doubt by the Court of Justice of the European Union (CJEU) in April 2014, when the court found the European Data Retention Directive (2006/24/EC) to be invalid and in contravention of articles 7, 8, and 52(1) of the European Convention on Human Rights.[34] The ruling was lauded among privacy proponents who had long argued that requirements for the blanket retention of data constituted mass surveillance and far exceeded what was necessary for law enforcement purposes. However, the decision has also prompted debate among legal experts and different reactions by governments, with some member states now suspending their national implementations of the European directive, while others are drafting new data retention laws in order to compel internet service providers to continue to store user data.[35]

According to a report by the Estonian Parliament Security Authorities Surveillance Select Committee, which oversees the practices of surveillance agencies and security agencies, there were over 2,700 cases of information requests based on court orders in 2014, a decrease of 4 percent from the previous year.[36] The select committee was established to exercise supervision over the legality of surveillance and the activities of the Security Police.[37] The committee monitors the activities of the Security Police Board to ensure conformity with the constitution, the Surveillance Act, and other regulations on security agencies.

Intimidation and Violence

There have been no physical attacks against bloggers or online journalists in Estonia, though online discussions are sometimes inflamma ory.

31 Electronic Privacy Information Center (EPIC) and Privacy International, "Republic of Estonia," in *Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments* (Washington: EPIC, 2007), http://bit.ly/2e38qaI.

32 "Tasks and jurisdiction of the Chancellor of Justice," accessed June 2, 2015, http://bit.ly/2dYL956,

33 Electronic Communications Act, translation to English, http://bit.ly/2eccx3T.

34 The ECJ court ruling pertained to the cases *Digital Rights Ireland Ltd (*C-293/12) and Kärntner Landesregierung (C-594/12) and is available at http://bit.ly/1yF25p3.

35 Martin Husovec, "First European Constitutional Court Suspends Data Retention After the Decision of the Court of Justice of EU," The Center for Internet and Society at Stanford Law School, April 28, 2015, http://stanford.io/2dGBfaF.

36 Overview of Parliament Select Committe activities, http://bit.ly/2e6wLbo.

37 "Security Authorities Surveillance Select Committee," Riigikogu: The Parliament of Estonia, June 16, 2016, http://bit.ly/2dGCGpr.

Technical Attacks

Awareness of the importance of ICT security in both private and business use has increased significantly since a series of cyberattacks against Estonian websites and government organizations in the spring of 2007. To protect the country from future attacks, the government adopted a fi e-year Cyber Security Strategy in 2008 that focused on the development and implementation of security measures that would increase competence in cyber security, improve the legal framework, bolster international cooperation, and raise public awareness.[38] Estonia's cybersecurity strategy is built on strong private-public collaboration and a unique voluntary structure through the National Cyber Defense League.[39] With more than 150 experts participating, the league has simulated different security threat scenarios as defense exercises that have served to improve the technical resilience of Estonia's telecommunication networks and other critical infrastructure over the past few years.

Also in 2008, the North Atlantic Treaty Organization (NATO) established a joint cyber defense center in Estonia to improve cyber defense interoperability and provide security support for all NATO members. Since its founding, the center has supported awareness campaigns and academic research on the topic and hosted several high-profile confe ences, among other activities.[40] From 2009, the NATO Cooperative Cyber Defense Centre of Excellence has organized an annual International Conference on Cyber Conflict, or CyCon, bringing ogether international experts from governments, the private sector, and academia. CyCon has focused on international cooperation and the legal, regulatory, military, and paramilitary aspects of cybersecurity, with the goal of ensuring the development of a free and secure internet.

38 Cyber Security Strategy Committee, *Cyber Security Strategy* (Tallinn: Ministry of Defence, 2008), http://bit.ly/2e6v2my; See also: Ministry of Economic Affairs and Communication, "Cyber Security Strategy 2014-2017," accessed October 11, 2016, http://bit.ly/2fdtquG.

39 "Estonian Defense League's Cyber Unit," Kaitseliit [Defence League], accessed October 11, 2016, http://bit.ly/2dhXTFC.

40 "Cyber Security Conferences," Cooperative Cyber Defense Centre of Excellence (CCD COE), accessed October 11, 2016, http://bit.ly/2dIPzSy.

Freedom House

Ethiopia

	2015	2016
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	23	23
Limits on Content (0-35)	28	28
Violations of User Rights (0-40)	31	32
TOTAL* (0-100)	**82**	**83**

* 0=most free, 100=least free

Population:	**99.3 million**
Internet Penetration 2015 (ITU):	**12 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- Internet and mobile phone networks were repeatedly disrupted around the country, particularly in the Oromia region during antigovernment protests that began in November 2015 (see **Restrictions on Connectivity**).
- Social media and communications platforms were temporarily blocked several times to restrict information about antigovernment protests and police brutality (see **Blocking and Filtering**).
- News websites were newly blocked for reporting on the Oromo protests and a severe drought, adding to a growing blacklist (see **Blocking and Filtering**).
- In May 2016, blogger Zelalem Workagenehu was sentenced to over fi e years in prison for leading a digital security course (see **Prosecutions and Arrests for Online Activities**).
- Prosecutors challenged the release of members of the Zone 9 blogging collective, after they were acquitted of terrorism charges in 2015 (see **Prosecutions and Arrests for Online Activities**).

Introduction

Internet freedom declined in the past year as the government cracked down on antigovernment protests and the digital tools citizens used to organize them.

Starting in the Oromo region in November 2015 as a protest against the authoritarian government's plan to infringe on land belonging to the marginalized Oromia people, the movement spread across the country in the subsequent months, turning into unprecedented demonstrations seeking regime change and democratic reform.

In a heavy-handed response, the authorities frequently shutdown local and national internet and mobile phone networks to prevent citizens from communicating about the protests. Social media platforms and communications apps such as Facebook, Twitter, Skype, and IMO were also temporarily blocked at different times. In October 2016, the government imposed a six-month state of emergency on October 17, resulting in another internet shutdown lasting several days. Under the state of emergency, accessing or posting content related to the protests on social media and efforts to communicate with "outside forces" are criminal offenses.

News websites and blogs reporting on the protests were permanently blocked in 2015 and 2016. Separately, critical news about the current drought—the worst the country has experienced in 50 years—was systematically censored. Meanwhile, the authorities arrested and prosecuted several bloggers, sentencing blogger Zelalem Workagenehu to fi e years in prison in May 2016. He was convicted of conspiring to overthrow the government for facilitating a course on digital security. The government's persecution of the Zone 9 bloggers continued. Though four of the bloggers were acquitted in October 2015, the prosecutor appealed their release to the Supreme Court, and they were repeatedly summoned throughout the year.

The legal environment for internet freedom became more restrictive under the Computer Crime Proclamation enacted in June 2016, which criminalizes defamation and incitement. The proclamation also strengthens the government's surveillance capabilities by enabling real-time monitoring or interception of communications.

Obstacles to Access

Internet and mobile phone networks were deliberately disrupted in many parts of the country throughout the year, particularly in the Oromia region during largescale antigovernment protests that erupted in November 2015. Meanwhile, poor infrastructure, obstructionist telecom policies, and a government monopoly on the ICT sector make ICT services prohibitively expensive for the majority of the population.

Availability and Ease of Access

Ethiopia is one of the least connected countries in the world with an internet penetration rate of only 12 percent, according to 2015 data from the International Telecommunications Union (ITU).[1] Mobile

1 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1cblxxY

phone penetration is also poor at 43 percent, up from just 32 percent in 2014.[2] Low penetration rates stem from underdeveloped telecommunications infrastructure, which is almost entirely absent from rural areas, where about 85 percent of the population resides. A handful of signal stations service the entire country, resulting in network congestion and frequent disconnection.[3] In a typical small town, individuals often hike to the top of the nearest hill to find a mobile phone signal

Access to ICT services remains prohibitively expensive for most Ethiopians, largely due to the government's monopoly over the telecom sector, which provides consumers with few options. Prices are set by state-controlled EthioTelecom and kept artificially high [4] Price cuts announced in February 2016 mitigated some of the financial strain [5] bringing mobile internet prices to ETB 5 (US$ 0.25) per day for 25 MB of data or ETB 3,000 (US$ 140) per month for 30 GB. Nonetheless, the lower cost 25 MB package is extremely limited considering a standard Google search uses up to 79 KB alone. Regularly loading websites containing 1 GB of multimedia content could cost US$ 9 a day. William Davison, Bloomberg's Ethiopia correspondent, described the issue on Facebook in March 2016: "It cost me 44 birr ($2.05) to watch Al Jazeera's latest 3-minute dispatch on Oromo protests using 4G network on my phone, which is not that much less than the average daily wage of a daily laborer in Ethiopia."[6] Ethiopians can spend an average of US$85 per month for limited mobile or fi ed wireless internet access. Better quality services in neighboring Kenya and Uganda cost less than US$30 a month.

Telecommunication devices, connection fees and other related costs are also beyond the means of many Ethiopians. As a result, Ethiopia has among the lowest smartphone ownership rates in the world at only 4 percent according to a recent Pew survey.[7] In April 2016, EthioTelecom proposed a new pricing scheme to charge more for the use of popular Voice-over-IP (VoIP) platforms such as Viber and Facebook Messenger on mobile devices.[8] This would make smartphone usage even more expensive.

Consequently, the majority of internet users still rely on cybercafés for internet access. A typical internet user in Addis Ababa pays between ETB 5 and 7 (US$ 0.25 to 0.35) for an hour of access. Because of the scarcity of internet cafes outside urban areas, however, rates in rural cybercafés are higher. In addition, digital literacy rates are generally low.

For the few Ethiopians who can access the internet, connection speeds have been painstakingly slow for years, despite the rapid technological advances improving service quality in other countries. In a test conducted in the capital Addis Ababa,[9] the average connection speed during one week

2 International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions, 2000-2015," http://bit.ly/1cblxxY

3 Endalk Chala, "When blogging is held hostage of Ethiopia's telecom policy," in "GV Advocacy Awards Essays on Internet Censorship from Iran, Venezuela, Ethiopia," Global Voices (blog), February 3, 2015, http://bit.ly/1OpDvzz

4 *Ethiopia – Telecoms, Mobile, Broadband and Forecasts*, Paul Budde Communication Pty Ltd.: June 2014, http://bit.ly/1ji15Rn

5 Misak Workneh, "Ethio Telecom announces new mobile internet packages, tariff revisions," *Addis Fortune*, February 23, 2016, http://addisfortune.net/articles/ethio-telecom-announces-new-mobile-internet-packages-tariff-revisions/

6 William Davison's Facebook post, March 26, 2016, https://www.facebook.com/william.davison.33/posts/10153956834545792?pnref=story

7 Jacob Poushter, "Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies," Pew Research Center, February 22, 2016, http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/

8 Eskedar Kifle, "Ethio elecom may charge for VoIP apps," Capital Ethiopia, April 6, 2016, http://mereja.com/news/1149276.

9 Test conducted by Freedom House researcher in March 2016. While the speed test should not be interpreted as a standard speed for the entire EthioTelecom network speeds, the data we gathered from a repeated speed tests over a span of a week from March 16 to March 21, 2016 suggest that Ethiopia's average speed lags behind the average speed of the region. Nearly same figu es were reported by speed-test services such as http://testmy.net and http://www.dospeedtest.com.

in March 2016 was 1.2 Mbps—fi e times slower than the average 5.5 Mbps connection speed in Kenya. According to Akamai, the average connection speed in Ethiopia was 3 Mbps in the fi st quarter of 2016, significantly lo er than the global average of 6.3 Mbps (Kenya's average speed was documented at 7.3 Mbps in the same period).[10]

In practice, such speeds result in extremely sluggish download times, even of simple images. Logging into an email account and opening a single message can take as long as fi e minutes at a standard cybercafé with broadband in the capital city, while attaching documents or images to an email can take eight minutes or more.[11] On mobile connections, Akamai found Ethiopia had the world's slowest average load time, at 8.5 seconds.[12]

Compounding Ethiopia's onerous access issues, severe drought in 2015 and 2016 has had a negative impact on the country's hydroelectric electricity production,[13] resulting in frequent and extended power outages that limit users' ability to access the internet even further.[14]

Restrictions on Connectivity

The Ethiopian government's monopolistic control over the country's telecommunications infrastructure via EthioTelecom enables it to restrict information flows and access o internet and mobile phone services. In 2015–16, the flow f online traffic in o, within, and out of Ethiopia registered a significant decline, li ely as a result of network throttling, repeated internet shutdowns, and increased blocking.

As a landlocked country, Ethiopia has no direct access to submarine cable landing stations; thus, it connects to the international internet via satellite, a fibe -optic cable that passes through Sudan and connects to its international gateway, and the SEACOM cable that connects through Djibouti to an international undersea cable. All connections to the international internet are completely centralized via EthioTelecom, enabling the government to cut off the internet at will.

Internet and mobile phone networks were disrupted in many parts of the country throughout the year. Oromia, the largest of the federal republic's nine regional states, has experienced frequent telecom network since November 2015 saw the start of largescale demonstrations against the government's plan to appropriate Oromia territory.[15] The protest movement escalated and remained ongoing in late 2016, leading the government to declare a six-month state of emergency and shut down mobile internet services nationwide for several days in October.[16]

10 Akamai, "Average Connection Speed," map visualization, *The State of the Internet*, Q1 2016, accessed August 1, 2016, http://akamai.me/1LiS6KD

11 According to tests by Freedom House consultant in 2016.

12 Akamai, "State of the Internet, Q1 2016 Report," https://goo.gl/TQH7L7.

13 William Davison, "Ethiopia Sees Nationwide Power Cuts While Drought Dries Dams," Bloomberg, December 1, 2015, http://www.bloomberg.com/news/articles/2015-12-01/ethiopia-sees-nationwide-power-cuts-while-drought-dries-dams

14 Mengisteab Teshome, "Ethiopia: Power Outage Taken as 'Business As Usual' – Residents," The Ethiopian Herald, September 4, 2015, http://allafrica.com/stories/201509040955.html

15 Endalk Chala, "Ethiopia Locks Down Digital Communications in Wake of #OromoProtests," Global Voices (blog), July 14, 2016, https://globalvoices.org/2016/07/14/ethiopia-locks-down-digital-communications-in-wake-of-oromoprotests; Moses Karanja et al., "Ethiopia: Internet Shutdown Amidst Recent Protests?" OONI, August 10, 2016, https://ooni.torproject.org/post/ethiopia-internet-shutdown-amidst-recent-protests/

16 Stephanie Busari, "Ethiopia declares state of emergency after months of protests," CNN, October 11, 2016, http://www.cnn.com/2016/10/09/africa/ethiopia-oromo-state-emergency/; Endalk Chala, "Ethiopian authorities shut down mobile internet and major social media sites," Global Voices (blog), October 11, 2016, https://globalvoices.org/2016/10/11/ethiopian-authorities-shut-down-mobile-internet-and-major-social-media-sites/

In an incident unrelated to the protests, internet services on computers and mobile devices were shut down for 24 hours in July 2016, ostensibly to prevent students from cheating during national university exams.[17]

The ICT shutdowns have been costly. Network disruptions between July 1, 2015 and June 30, 2016 cost Ethiopia's economy over US$ 8.5 million, according to the Brookings Institution.[18]

ICT Market

The space for independent initiatives in the ICT sector, entrepreneurial or otherwise, is extremely limited,[19] with state-owned EthioTelecom holding a fi m monopoly over internet and mobile phone services as the country's sole telecommunications service provider. Despite repeated international pressure to liberalize telecommunications in Ethiopia, the government refuses to ease its grip on the sector.[20]

China is a key investor in Ethiopia's telecommunications industry,[21] with Zhongxing Telecommunication Corporation (ZTE) and Huawei currently serving as contractors to upgrade broadband networks to 4G in Addis Ababa and expand 3G networks elsewhere.[22] The partnership has enabled Ethiopia's authoritarian leaders to maintain their hold over the telecom sector,[23] though the networks built by the Chinese fi ms have been criticized for their high cost and poor service.[24] Furthermore, the contracts have led to increasing fears that the Chinese may also be assisting the authorities in developing more robust ICT censorship and surveillance capacities (see Surveillance, Privacy, and Anonymity).[25] In December 2014, the Swedish telecom group Ericsson also partnered with the government to improve and repair the mobile network infrastructure,[26] though ZTE remains the sector's largest investor.

Onerous government regulations also stymie other aspects of the Ethiopian ICT market. For one, imported ICT items are tariffed at the same high rate as luxury items, unlike other imported goods such as construction materials and heavy duty machinery, which are given duty-free import privileges to encourage investments in infrastructure.[27] Ethiopians are required register their laptops and tablets at the airport with the Ethiopian customs authority before they travel out of the country,

17 Paul Schemm, "Ethiopia shuts down social media to keep from 'distracting' students," Washington Post, July 13, 2016, https://www.washingtonpost.com/news/worldviews/wp/2016/07/13/ethiopia-shuts-down-social-media-to-keep-from-distracting-students/

18 Darrell M. West, "Internet shutdowns cost countries $2.4 billion last year," Brookings Institute, Center for Technology Innovation, October 2016, https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf

19 Al Shiferaw, "Connecting Telecentres: An Ethiopian Perspective," Telecentre Magazine, September 2008, http://bit.ly/1ji348h.

20 "Ethio Telecom to remain monopoly for now," TeleGeography, June 28, 2013, http://bit.ly/1huyjf7

21 Paul Chapman, "New report explores the Ethiopian – telecoms, mobile and broadband – market insights, statistics and forecasts," *WhatTech*, May 1, 2015, http://bit.ly/1L46Awu.

22 "Out of reach," *The Economist*, August 24, 2013, http://econ.st/1l1UvJO.

23 "Out of reach," *The Economist*.

24 Matthew Dalton, "Telecom Deal by China's ZTE, Huawei in Ethiopia Faces Criticism," *The Wall Street Journal*, January 6, 2014, http://on.wsj.com/1LtSCkD.

25 Based on allegations that the Chinese authorities have provided the Ethiopian government with technology that can be used for political repression—such as surveillance cameras and satellite jamming equipment—in the past. See: *Addis Neger*, "Ethiopia: China Involved in ESAT Jamming," *ECADAF Ethiopian news & Opinion,* June 23, 2010, http://bit.ly/1LtSYI9; Gary Sands, "Ethiopia's Broadband Network – A Chinese Trojan Horse?" *Foreign Policy Blogs*, Foreign Policy Association, September 6, 2013, http://bit.ly/1FWG8X1.

26 ENA, "Ericsson to take part in telecom expansion in Ethiopia," *Dire Tube*, December 18, 2014, http://bit.ly/1PkZfvA.

27 The Embassy of the United Stated, "Doing Business in Ethiopia," http://1.usa.gov/1LtTExh.

ostensibly to prevent individuals from illegally importing electronic devices, though observers believe the requirement enables officials o monitor citizens' ICT activities by accessing the devices without consent.[28]

Local software companies also suffer from heavy-handed government regulations, which do not have fair, open, or transparent ways of evaluating and awarding bids for new software projects.[29] Government companies are given priority for every kind of project, while smaller entrepreneurial software companies are completely overlooked, leaving few opportunities for local technology companies to thrive.

Cybercafés are subject to burdensome operating requirements under the 2002 Telecommunications (Amendment) Proclamation,[30] which prohibit them from providing Voice-over-IP (VoIP) services, and mandate that owners obtain a license from EthioTelecom via an opaque process that can take months. In the past few years, EthioTelecom began enforcing its licensing requirements more strictly in response to the increasing spread of cybercafés, reportedly penalizing Muslim cafe owners more harshly. Violations of the requirements entail criminal liability, though no cases have been reported.[31]

Regulatory Bodies

Since the emergence of the internet in Ethiopia, the Ethiopian Telecommunications Agency (ETA) has been the primary regulatory body overseeing the telecommunications sector. In practice, government executives have complete control over ICT policy and sector regulation.[32] The Information Network Security Agency (INSA), a government agency established in 2011 and controlled by individuals with strong ties to the ruling regime,[33] also has significant po er in regulating the internet under the mandate of protecting the communications infrastructure and preventing cybercrime.

Limits on Content

News websites known for their reporting on the Oromo protests joined Ethiopia's growing list of blocked content, while social media and communications platforms were blocked for periods of time throughout the coverage period for their role in disseminating information about the demonstrations and police brutality. The government manipulates online content, disseminating propaganda to convince Ethiopians that social media is a dangerous tool co-opted by opposition groups to spread hate and violence.

28 World Intellectual Property Organization, "Ethiopia Custom Regulation: No 622/2009," http://bit.ly/1NveoeB.

29 Mignote Kassa, "Why Ethiopia's Software Industry Falters," *Addis Fortune* 14, no. 700 (September 29, 2013), http://bit.ly/1VJiIWC.

30 "Proclamation No. 281/2002, Telecommunications (Amendment Proclamation," *Federal Negarit Gazeta* No. 28, July 2, 2002, http://bit.ly/1snLgsc.

31 Ethiopian Telecommunication Agency, "License Directive for Resale and Telecenter in Telecommunication Services No. 1/2002," November 8, 2002, accessed October 20, 2014, http://bit.ly/1pUtpWh.

32 Dr. Lishan Adam, "Understanding what is happening in ICT in Ethiopia," (policy paper, Research ICT Africa, 2012) http://bit.ly/1LDPyJ5.

33 Halefom Abraha, "THE STATE OF CYBERCRIME GOVERNANCE IN ETHIOPIA," (paper) http://bit.ly/1huzP0S.

Blocking and Filtering

One of the first African countries to censor the internet,[34] Ethiopia has a nationwide, politically motivated internet blocking and filtering regime that is reinforced during sensitive political events. More websites were newly blocked during the Oromia protests that began in November 2015. Targets included the websites of US-based diaspora satellite television stations such as Ethiopian Satellite Television (ESAT) and the Oromo Media Network (OMN), which provided wall-to-wall coverage of the antigovernment protests. Ayyantuu.net and Opride.com, prominent websites also known for their reporting on the protests, were also blocked.[35]

In an apparent attempt to restrict news about the protests from spreading, social media and file sharing platforms such as Facebook, Twitter, WhatsApp, and Dropbox were repeatedly blocked for periods of time throughout the protests.[36] The blocks on social media first impacted networks in the Oromia region but later spread to other regions,[37] and eventually manifested in a shutdown of entire internet and mobile networks for days a time (see Restrictions on Connectivity).

Unrelated to the protests, the authorities blocked access to social media and communications platforms, including Facebook, Twitter, Instagram, Viber, IMO, and Google+, to prevent cheating during university examinations on July 9 and 10, 2016.[38] The blocks followed a 24-hour internet blackout for the same reason (see Restrictions on Connectivity). A government spokesperson stated that blocking social media during the exam would help students concentrate. However, some progovernment media organizations and commentators seemed to have exclusive access to social media during the block,[39] which reinforced the belief that the government imposes restrictions on citizens while keeping the web open for its own advantage. Viber and IMO, two popular voice-over-IP applications, remained blocked until July 20, according to local sources.[40]

Separately, coverage of a severe drought—the worst the country has experienced in 50 years—was systematically censored in the past year, with news websites and blogs blocked for reporting on the impact of the disaster that strayed from the government's official narrative.[41]

In total, over one hundred websites are inaccessible in Ethiopia.[42] A manual test conducted on the ground in mid-2016 confirmed that a large number of the websites tested by Freedom House each

34 Rebecca Wanjiku, "Study: Ethiopia only sub-Saharan Africa nation to filter net," IDG News Service, October 8, 2009, http://bit.ly/1Lbi3s9.

35 "Ayyaantuu website blocked in Ethiopia," Ayyaantuu News, March 3, 2016, http://www.ayyaantuu.net/ayyaantuu-website-blocked-in-ethiopia/

36 Felix Horne, "Deafening silence from Ethiopia," Foreign Policy in Focus, April 12, 2016, http://fpif.org/deafening-silence-ethiopia/; Endalk Chala, "Ethiopia locks down digital communications in wake of #OromoProtests," Global Voices (blog), July 14, 2016, https://advox.globalvoices.org/2016/07/14/ethiopia-locks-down-digital-communications-in-wake-of-oromoprotests/

37 William Davison, "Twitter, WhatsApp Down in Ethiopia Oromia Area After Unrest," Bloomberg, April 12, 2016, http://www.bloomberg.com/news/articles/2016-04-12/twitter-whatsapp-offline-in-ethiopia-s-oromia-area-after-unrest

38 Nicole Orttung, "Why did Ethiopia block social media," Christian Science Monitor, July 12, 2016, http://www.csmonitor.com/World/2016/0712/Why-did-Ethiopia-block-social-media?cmpid=gigya-tw

39 According to activists who were able to circumvent the blocks and observe the social media activities of progoverment users.

40 @befeqadu Twitter post, July 17, 2016, https://twitter.com/befeqadu/status/754725025610104833

41 Christabel Ligami, "Defying censorship, hunger stories emerge from Ethiopia," Equal Times, April 29, 2016, http://www.equaltimes.org/defying-censorship-hunger-stories?lang=en#.WBJZxMmFs6E; "Ethiopian police detain journalists reporting on drought, escort them back to capital," Committee to Protect Journalists, August 17, 2016, https://cpj.org/2016/08/ethiopian-police-detain-journalists-reporting-on-d.php

42 Test conducted by an anonymous researcher contracted by Freedom House, March 2015. During the test, some websites opened at the first attempt but were inaccessible when refreshed.

year since 2012 remained blocked. Blocked sites include Ethiopian news websites, political party websites, and the websites of international digital rights organizations, such as the Electronic Frontier Foundation and Tactical Technology Collective. Select tools such as text messaging apps and services on Google's Android operating system on smartphones were also inaccessible, but at irregular intervals and for unclear reasons.[43]

Notably, several websites that hadn't been updated for years and appeared abandoned became accessible again in 2016, likely because the authorities deemed them no longer threatening. The social media curation tool Storify—first blocked in July 2012[44]—was also newly accessible during the coverage period,[45] in addition to the URL shortening tool Bit.ly.[46]

To filter the internet, specific internet protocol (IP) addresses or domain names are generally blocked at the level of the EthioTelecom-controlled international gateway. Deep-packet inspection (DPI) is also employed, which blocks websites based on a keyword in the content of a website or communication (such as email).[47]

Digital security tools are also pervasively blocked in Ethiopia, including Tor, the circumvention tool that enables users to browse anonymously, which been blocked since May 2012.[48] As social media platforms were blocked in the past year, diaspora-based activists publicized virtual private networks (VPNs) to circumvent the censorship, but certain VPNs were also subsequently blocked.[49] Local sources suspected progovernment commenters were flagging the same tools to be blocked by the authorities. The Amharic translation of the Electronic Frontier Foundations' "Surveillance Self-Defense" web guide was blocked two weeks after it was published in October 2015.[50] One source reported that key terms such as "proxy" yield no search results on unencrypted search engines,[51] reflecting the government's efforts to limit users' access to circumvention tools and strategies.

Some restrictions are also placed on content transmitted via mobile phones. Text messages to more than ten recipients require prior approval from EthioTelecom.[52] A bulk text message sent without prior approval is automatically blocked, irrespective of the content.

---

43 @AtnafB Twitter post, July 17, 2016, https://twitter.com/AtnafB/status/754711725967024131

44 Mohammed Ademo, Twitter post, July 25, 2012, 1:08 p.m., https://twitter.com/OPride/status/228159700489879552.

45 Mohammed Ademo, "Media Restrictions Tighten in Ethiopia," *Columbia Journalism Review*, August 13, 2012, http://bit.ly/1Lm2npk.

46 Ory Okolloh Mwangi, Twitter post, November 6, 2013, 9:20 a.m., https://twitter.com/kenyanpundit/status/398077421926514688.

47 Daniel Berhane, "Ethiopia's web filtering: advanced technology, hypocritical criticisms, bleeding constitution," *Horns Affairs*, January 16, 2011, http://bit.ly/1jTyrH1

48 "Tor and Orbot not working in Ethiopia," Tor Stack Exchange, message board, April 12, 2016, http://tor.stackexchange.com/questions/10148/tor-and-orbot-not-working-in-ethiopia; "Ethiopia Introduces Deep Packet Inspection," Tor (blog), May 31, 2012, http://bit.ly/1A0YRdc; Warwick Ashford, "Ethiopian government blocks Tor network online anonymity," *Computer Weekly*, June 28, 2012, http://bit.ly/1LDQ5L2.

49 Ismail Akwei, "Ethiopia blocks social media to prevent university exam leakage," Africa News, July 10, 2016, http://www.africanews.com/2016/07/10/ethiopia-blocks-social-media-to-prevent-university-exam-leakage/

50 Endalk Chala, "Defending against overreaching surveillance in Ethiopia: Surveillance Self-Defense now availabile in Amharic," Electronic Frontier Foundation, October 1, 2015, https://www.eff.org/deeplinks/2015/09/defending-against-overreaching-surveillance-ethiopia-surveillance-self-defense-n-0

51 A 2014 report from Human Rights Watch also noted that the term "aljazeera" was unsearchable on Google while the news site was blocked from August 2012 to mid-March 2013. According to HRW research, the keywords "OLF" and "ONLF" (acronyms of Ethiopian opposition groups) are not searchable on the unencrypted version of Google (http://) and other popular search engines. Human Rights Watch, "They Know Everything We Do," March 25, 2014, 56, 58, http://bit.ly/1Nviu6r.

52 Interview with individuals working in the telecom sector, as well as a test conducted by a Freedom House consultant who found it was not possible for an ordinary user to send out a bulk text message.

There are no procedures for determining which websites are blocked or why, precluding any avenues for appeal. There are no published lists of blocked websites or publicly available criteria for how such decisions are made, and users are met with an error message when trying to access blocked content. The decision-making process does not appear to be controlled by a single entity, as various government bodies—including the Information Network Security Agency (INSA), EthioTelecom, and the ICT ministry—seem to be implementing their own lists, contributing to a phenomenon of inconsistent blocking. This lack of transparency is exacerbated by the government's continued denial of its censorship efforts. Government officials flatly deny the blocking f websites or jamming of international satellite operations while also stating that the government has a legal and a moral responsibility to protect the Ethiopian public from extremist content.

Content Removal

Politically objectionable content is often targeted for removal, often by way of threats from security officials who pe sonally seek out users and bloggers to instruct them to take down certain content, particularly critical content on Facebook. The growing practice suggests that at least some voices within Ethiopia's small online community are being closely monitored. For instance, during the various legal proceedings involving the Zone 9 bloggers in 2015, friends and reporters who posted pictures and accounts of the trials on social media were briefly detained and as ed to remove the posts.[53] During protests in Oromia, activists who wrote messages of solidarity for the protestors on Facebook were also asked to delete their posts.[54]

Media, Diversity, and Content Manipulation

Lack of adequate funding is a significant challenge for independent online media in Ethiopia, as fear of government pressure dissuades local businesses from advertising with politically critical websites. A 2012 Advertising Proclamation also prohibits advertisements from fi ms "whose capital is shared by foreign nationals."[55] The process for launching a website on the local .et domain is expensive and demanding,[56] requiring a business license from the Ministry of Trade and Industry and a permit from an authorized body.[57] While the domestic Ethiopian blogosphere has been expanding, most blogs are hosted on international platforms or published by members of the diaspora community.

Despite Ethiopia's extremely low levels of internet access, the government employs an army of trolls to distort Ethiopia's online information landscape.[58] Opposition groups, journalists, and dissidents use the contemptuous Amharic colloquial term, "Kokas," to describe the progovernment commentators.[59] Observers say the Kokas regularly discuss Ethiopia's economic growth in favorable

53 Reporters prevented from reporting on the trial of Zone9 Bloggers. See, Trial Tracker Blog, http://trialtrackerblog.org/home/ .

54 Kevin Mwanza, "Is Ethiopia restricting access to social media in Oromia region?" Afk Insider, April 13, 2016, http://afkinsider.com/123180/ethiopia-restricting-access-social-media-oromia-region/

55 Exemptions are made for foreign nationals of Ethiopian origin. See, Abrham Yohannes, "Advertisement Proclamation No. 759/2012," Ethiopian Legal Brief (blog), September 27, 2012, http://bit.ly/1LDQf5c.

56 "Proclamation No. 686/2010 Commercial Registration and Business Licensing," *Federal Negarit Gazeta*, July 24, 2010, http://bit.ly/1P3PoLy; World Bank Group, *Doing Business 2015: Going Beyond Efficiency, Economy Profile 2015, Ethiopia*, 2014, http://bit.ly/1L49tO6.

57 Chala, "When blogging is held hostage of Ethiopia's telecom policy."

58 "Ethiopia Trains Bloggers to attack its opposition," *ECADF Ethiopian News & Opinions*, June 7, 2014, http://bit.ly/1QemZjl.

59 The term "Koka" is a blend of two words: Kotatam and cadre. Kotatam is a contemptuous Amharic word used to imply that someone is a sellout who does not have a respect for himself or herself.

terms and post uncomplimentary comments about Ethiopian journalists and opposition groups on Facebook and Twitter. In return, they are known to receive benefits such as mone , land, and employment promotions.

The government also manipulates online content through propaganda that aims to convince Ethiopians that social media is a dangerous tool co-opted by opposition groups to spread hate and violence.[60] That characterization has been debunked by research. The University of Oxford and Addis Ababa University analyzed thousands of comments made by Ethiopians on Facebook during general election in 2015, finding that ha e speech was a marginal proportion of the total comments assessed.[61]

Meanwhile, increasing repression against journalists and bloggers has had a major chilling effect on expression online, particularly in response to the spate of blogger arrests that have increased in the past few years (see Prosecutions and Detentions for Online Activities). Many bloggers publish anonymously to avoid reprisals.[62] Fear of pervasive surveillance has also led to widespread self-censorship. Local newspapers and web outlets primarily publish reporting by regime critics and opposition organizations in the diaspora. Few independent local journalists will write for either domestic or overseas online outlets due to the threat of repercussions.

Digital Activism

Despite oppressive conditions caused by poor access and the hostile legal environment, online activism has gained considerable momentum and influence in the ast year, particularly as traditional media coverage of current events has become increasingly narrow and dominated by pro-government voices. Notably, social media and communications platforms helped tech-savvy Ethiopians launch the widespread antigovernment protests in the Oromia region in November 2015. Online tools have been essential to the #OromoProtests movement, enabling activists to post information about the demonstrations and disseminate news about police brutality as the government cracked down on protesters.[63] The use of such tools to fuel the protest movement led the government to block access to several platforms throughout the year, and shut down internet and mobile networks altogether (see Blocking and Filtering and Restrictions on Connectivity).

Violations of User Rights

The new Computer Crime Proclamation enacted in June 2016 criminalizes defamation and incitement; observers say it could be invoked to suppress digital mobilization. The proclamation also strengthens the government's surveillance capabilities by enabling real-time monitoring or interception of communications. Several bloggers were arrested and prosecuted, with one blogger sentenced to five years in prison, while prosecutors challenged the acquittal of the Zone 9 bloggers.

60 Endalk Chala, "Ethiopia protest videos show state brutality, despite tech barriers," Global Voices (blog), January 6, 2016, https://advox.globalvoices.org/2016/01/06/ethiopia-protest-videos-show-state-brutality-despite-tech-barriers/

61 Iginio Gagliardone et al., "Mechachal: Online debates and elections in Ethiopia. Report One: A preliminary assessment of online debates in Ethiopia," working paper, October 2, 2015, http://bit.ly/2eOLFCH

62 Markos Lemma, "Disconnected Ethiopian Netizens," Digital Development Debates (blog),November 2012, http://bit.ly/1Ml9Nu3.

63 Jacey Fortin, "The ugly side of Ethiopia's economic boom," Foreign Policy, March 23, 2016, http://foreignpolicy.com/2016/03/23/no-one-feels-like-they-have-any-right-to-speak-at-all-ethiopia-oromo-protests/

Legal Environment

Fundamental freedoms are guaranteed for Ethiopian internet users on paper, but the guarantees are routinely flou ed in practice. The 1995 Ethiopian constitution provides for freedom of expression, freedom of the press, and access to information, while also prohibiting censorship.[64] These constitutional guarantees are affi med in the 2008 Mass Media and Freedom of Information Proclamation, known as the press law, which governs the print media.[65] Nevertheless, the press law also includes problematic provisions that contradict constitutional protections and restrict free expression, such as complex registration processes for media outlets and high fines for defamation [66] The Criminal Code also penalizes defamation with a fine or up o one year in prison.[67]

Meanwhile, several laws are designed to restrict and penalize legitimate online activities and speech.

Most alarmingly, the 2012 Telecom Fraud Offences Law extends the violations and penalties defined in the 2009 Anti-Terrorism Proclamation and criminal code to electronic communications, which explicitly include both mobile phone and internet services.[68] The antiterrorism legislation prescribes prison sentences of up to 20 years for the publication of statements that can be understood as a direct or indirect encouragement of terrorism, which is vaguely defined [69] The law also bans Voice over Internet Protocol (VoIP) services such as Skype[70] and requires all individuals to register their telecommunications equipment—including smartphones—with the government, which security officials typically enfo ce at security checkpoints by confiscating ICT equipment if the owner cannot produce a registration permit, according to sources in the country.

In June 2016, the Ethiopian government passed a new Computer Crime Proclamation that criminalized an array of online activities.[71] Civil society expressed concern that the law would be used to further crackdown on critical commentary, political opposition, and social unrest.[72] For example, content that "incites fear, violence, chaos or conflict among people" can be punished with up o three years in prison, which could be abused to suppress digital campaigns.[73] Other problematic provisions ban the dissemination of defamatory content, which can be penalized with up to 10 years

64 Constitution of the Federal Democratic Republic of Ethiopia (1995), art. 26 and 29, accessed, August 24, 2010, http://www.ethiopar.net/constitution.

65 Freedom of the Mass Media and Access to Information Proclamation No. 590/2008, *Federal Negarit Gazeta* No. 64, December 4, 2008.

66 Article 19, *The Legal Framework for Freedom of Expression in Ethiopia*, accessed September 10, 2014, http://bit.ly/1Pl0f33.

67 Criminal Code, art. 613, http://bit.ly/1OpHE6F.

68 Article 19, "Ethiopia: Proclamation on Telecom Fraud Offences,"legal analysis, August 6, 2012, http://bit.ly/1Lbonjm.

69 "Anti-Terrorism Proclamation No. 652/2009," *Federal Negarit Gazeta* No. 57, August 28, 2009.

70 The government fi st instituted the ban on VoIP in 2002 after it gained popularity as a less expensive means of communication and began draining revenue from the traditional telephone business belonging to the state-owned EthioTelecom. In response to widespread criticisms, the government claimed that VoIP applications such as Skype would not be considered under the new law, though the proclamation's language still enables the authorities to interpret it broadly at whim.

71 "Ethiopia Computer Crime Proclamation Text Draft," Addis Insight, May 9, 2016, http://www.addisinsight.com/2016/05/09/ethiopia-computer-crime-proclamation-text-draft/

72 Kimberly Carlson, "Ethiopia's new Cybercrime Law allows for more efficient and sys ematic prosecution of online speech," Electronic Frontier Foundation, June 9, 2016, https://www.eff.org/deeplinks/2016/06/ethiopias-new-cybercrime-law-allows-more-efficien -and-systematic-prosecution-online; Tinishu Soloman, "New Ethiopian law targets online crime," The Africa Report, June 9, 2016, http://www.theafricareport.com/East-Horn-Africa/new-ethiopian-law-targets-online-crime.html

73 Article 14, "Crimes against Public Security," Computer Crime Proclamation, draft text at http://www.addisinsight.com/2016/05/09/ethiopia-computer-crime-proclamation-text-draft/, http://hornaffairs.com/en/2016/05/09/ethiopia-computer-crime-proclamation/

in prison,[74] and the distribution of unsolicited messages to multiple emails (spam), which carries up to fi e years in prison.[75]

To quell escalating antigovernment protests that began in the Oromia region in November 2015, the government imposed a six-month state of emergency on October 17, 2016 that included restrictions on certain online activities.[76] In addition to shutting down the internet for several days, the authorities criminalized the access and posting of content related to the protests on social media, as well as efforts to communicate with "terrorist" groups, a category that includes exiled dissidents. Penalties for violating the state of emergency include prison terms of three to fi e years.[77]

Prosecutions and Detentions for Online Activities

In the past few years, the authorities have intensified their crac down against bloggers and online journalists, using harsh laws to arrest and prosecute individuals for their online activities and silence dissent. The most high-profile p osecutions were against six bloggers from the critical Zone 9 blogging collective, who were arrested in April 2014,[78] and charged with terrorism under the harsh Anti-Terrorism Proclamation in July.[79] The bloggers were accused of intent to overthrow the government, an offense under the criminal code, by encrypting their communications to disseminate seditious writings.[80]

Despite widespread international condemnation, the detainees were denied bail and brought to court dozens of times for over a year,[81] until two of them were unexpectedly released without charge in early July 2015, immediately before U.S. President Obama visited Ethiopia. The four remaining Zone 9 bloggers were acquitted in October 2015,[82] though they were barred from leaving the country.[83] The prosecutor contested their acquittal and appealed to the Supreme Court, and the four were summoned in December 2015 and in October 2016.[84] They were scheduled to return to court in November 2016.[85]

Several other bloggers were arrested and prosecuted in the past year, including Getachew

74 Article 13, "Crimes against Liberty and Reputation of Persons," Computer Crime Proclamation.

75 Article 15, "Dissemination of Spam," Computer Crime Proclamation,

76 "Seven things banned under Ethiopia's state of emergency," BBC News, October 17, 2016, http://www.bbc.com/news/world-africa-37679165

77 "Social media blackout in Ethiopia," Jacarandafm, October 17, 2016, https://www.jacarandafm.com/news-sport/news/social-media-blackout-in-ethiopia/

78 "Six members of Zone Nine, group of bloggers and activists are arrested," [in Amharic] Zone9 (blog), April 25, 2014, http://bit.ly/1VJn6ow.

79 "Federal High Court Lideta Criminal Bench court, Addis Ababa," http://1drv.ms/1OqAjlC.

80 Endalk Chala, "What You Need to Know About Ethiopia v. Zone9 Bloggers: Verdict Expected July 20," Global Voices (blog), July 17, 2015, http://bit.ly/1jTDO9b.

81 Ellery Roberts Biddle, Endalk Chala, Guardian Africa network, "One year on, jailed Ethiopian bloggers are still awaiting trial," *The Guardian*, April 24, 2015, http://gu.com/p/47ktv/stw; "Nine Journalists and Bloggers Still Held Arbitrarily," Reporters Without Borders, "Nine Journalists and Bloggers Still Held Arbitrarily," August 21, 2014, http://bit.ly/1P3TW4I.

82 Committee to Protect Journalists, "In Ethiopia, Zone 9 bloggers acquitted of terrorism charges," news statement, October 16, 2015, https://www.cpj.org/2015/10/in-ethiopia-zone-9-bloggers-acquitted-of-terrorism.php.

83 Gregory Warner, "Freed from prison, Ethiopian bloggers still can't leave the country," NPR, May 31, 2016, http://www.npr.org/sections/parallels/2016/05/31/480100349/freed-from-prison-ethiopian-bloggers-still-cant-leave-the-country

84 "Netizen Report: Ethiopia's Zone9 Bloggers Go Back to Court," Global Voices (blog), March 30, 2016, https://advox.globalvoices.org/2016/03/30/netizen-report-ethiopias-zone9-bloggers-go-back-to-court/

85 "Netizen Report: As Protests Rage in Ethiopia, Zone9 Bloggers Return to Court," Global Voices (blog), October 21, 2016, https://globalvoices.org/2016/10/21/netizen-report-as-protests-rage-in-ethiopia-zone9-bloggers-return-to-court/

Shiferaw, editor-in-chief of the online newspaper *Negere Ethiopia*, in December 2015.[86] *Negere Ethiopia* is known for its affiliation with the opposition as ell as its coverage of the Zone 9 trials. Shiferaw remained in pretrial detention in mid-2016.[87]

The prominent opposition member Yonatan Tesfaye was arrested in December 2015 and charged with terrorism based on Facebook posts that criticized the government's handling of the Oromia protests.[88] He remained in prison in mid-2016 and faces the death sentence if convicted.[89] Tesfaye's Twitter handle has been active during his detention, leading to suspicions that the officials ha e been using his account to bait potential dissidents.[90]

In April 2016, blogger Zelalem Workagenehu was found guilty of terrorism and sentenced to over fi e years in prison in May.[91] He was fi st arrested in July 2014 on charges of conspiring to overthrow the government after he facilitated a course on digital security. In the same trial, bloggers Yonatan Wolde and Bahiru Degu were acquitted after spending nearly two years in detention on terrorism charges; they were also arrested in July 2014 for applying to participate in Workaegnehu's digital security course.[92] Workagenehu has appealed to the Supreme Court.[93]

The ongoing antigovernment protest movement has also led to numerous arrests, some for digital activities, including posting or "liking" social media content about the protests. In October 2016, police arrested Seyoum Teshome, a well-known academic and blogger for the Ethiothinktank.com website who had published an article about the Oromia protest movement in *The New York Times*.[94]

Meanwhile, the well-known dissident journalist and blogger Eskinder Nega is serving an 18-year prison sentence handed down in July 2012 under the draconian anti-terrorism law for criticizing the law itself in an online article.[95]

Surveillance, Privacy, and Anonymity

Government surveillance of online and mobile phone communications is pervasive in Ethiopia

86 "Ethiopia arrests second journalist in a week, summons Zone9 bloggers," Committee to Protect Journalists, press release, December 27, 2015, https://www.cpj.org/2015/12/ethiopia-arrests-second-journalist-in-a-week-summo.php

87 "Getachew Shiferaw – The Price of Freedom of Expression in Ethiopia," Ethiopian Human Rights Project, May 3, 2016, http://ehrp.org/getachew-shiferaw-the-price-of-freedom-of-expression-in-ethiopia/

88 Salem Soloman, "Ethiopia's Anti-terrorism Law: Security or Silencing Dissent?" VOA News, May 31, 2016, http://www.voanews.com/a/ethiopia-anti-terrorism-law-security-silencing-dissent/3356633.html

89 "Ethiopia: Release opposition politician held for Facebook posts," Amnesty International, press release, May 6, 2016, https://www.amnesty.org/en/latest/news/2016/05/ethiopia-release-opposition-politician-held-for-facebook-posts/; "Facebook post leads to serious charges for Ethiopian politician," Enca, May 6, 2016, http://bit.ly/2ewu9SU

90 @befeqadu Twitter post, April 12, 2016, https://twitter.com/befeqadu/status/719963259911188480/photo/1

91 Tedla D. Tekle, "Ethiopian blogger and activist sentences to fi e years and four months," Global Voices (blog), May 16, 2016, https://advox.globalvoices.org/2016/05/16/ethiopian-blogger-and-activist-sentenced-to-fi e-years-and-four-months/

92 Tedla D. Tekle, "'I was forced to drink my own urine,': 'Freedom' for netizen after 647 days locked up, but not for all," Global Voices (blog), May 2, 2016, http://bit.ly/2fxUWPs

93 "Co-blogger Zelalem Workagegnehu's appeal heard, appointed to tomorrow," De Birhan (blog), July 20, 2016, http://debirhan.com/?p=10035

94 "Oromo protests: Ethiopia arrests blogger Seyoum Teshome," Al Jazeera, October 5, 2016, http://www.aljazeera.com/news/2016/10/oromo-protests-ethiopia-arrests-blogger-seyoum-teshome-161005071925586.html

95 Such trumped-up charges were based on an online column Nega had published criticizing the government's use of the Anti-Terrorism Proclamation to silence political dissent and calling for greater political freedom in Ethiopia. Nega is also the 2011 recipient of the PEN/Barbara Goldsmith Freedom to Write Award."That Bravest and Most Admirable of Writers: PEN Salutes Eskinder Nega," PEN American Center (blog), April 13, 2012, http://bit.ly/1Lm89Y7; See also, Markos Lemma, "Ethiopia: Online Reactions to Prison Sentence for Dissident Blogger," *Global Voices*, July 15, 2012, http://bit.ly/1OpKaKf; Endalk Chala, "Ethiopia: Freedom of Expression in Jeopardy," *Global Voices Advocacy*, February 3, 2012, http://bit.ly/1jfIEO3.

and was strengthened under the new Computer Crime Proclamation enacted in June 2016, which enables real-time monitoring or interception of communications authorized by the Minister of Justice and obliges service providers to store records of all communications and metadata for at least a year.[96]

There are strong indications that the government has deployed a centralized monitoring system developed by the Chinese telecommunications fi m ZTE to monitor mobile phone networks and the internet, according to a 2015 Human Rights Watch report.[97] Known for its use by repressive regimes in Libya and Iran, the monitoring system enables deep packet inspection (DPI) of internet traffic across the EthioTelecom network and has the ability to intercept emails and web chats.

Another ZTE technology, known as ZSmart, is a customer management database installed at EthioTelecom that provides the government with full access to user information and the ability to intercept SMS text messages and record phone conversations.[98] ZSmart also allows security officials to locate targeted individuals through real-time geolocation tracking of mobile phones.[99] While the extent to which the government has made use of the full range of ZTE's sophisticated surveillance systems is unclear, the authorities frequently present intercepted emails and phone calls as evidence during trials against journalists and bloggers or during interrogations as a scare tactic.[100]

Meanwhile, exiled dissidents have been targeted by surveillance malware. Citizen Lab research published in March 2015 said Remote Control System (RCS) spyware had been used against two employees of Ethiopian Satellite Television Service (ESAT) in November and December 2014. ESAT is a diaspora-run independent satellite television, radio, and online news media outlet, based in Alexandria, Virginia.[101] Made by the Italian company Hacking Team, RCS spyware is advertised as "offensive technology" sold exclusively to law enforcement and intelligence agencies around the world, and has the ability to steal files and asswords and intercept Skype calls and chats.[102]

While Hacking Team has said that the company does not deal with "repressive regimes,"[103] the social engineering tactics used to bait the two ESAT employees made it clear that the attack was targeted. Moreover, analysis of the RCS attacks uncovered credible links to the Ethiopian government, with the spyware's servers registered at an EthioTelecom address under the name "INSA-PC," referring to the Information Network Security Agency (INSA), the body established in 2011 to preside over the security of the country's critical communications infrastructure.[104] INSA was already known to be using the commercial toolkit FinFisher to target dissidents and supposed national security threats. FinFisher can secretly monitor computers by turning on webcams, record everything a user types with a key logger, and intercept Skype calls.[105]

96 Article 23, "Retention of Computer Data" and Article 24, "Real-time Collection of Computer Data," http://hornaffairs.com/en/2016/05/09/ethiopia-computer-crime-proclamation/

97 Human Rights Watch, "They Know Everything We Do," 62.

98 Human Rights Watch, "They Know Everything We Do," 67.

99 Ibid, 52.

100 Committee to Protect Journalists, "Ethiopian Blogger, Journalists Convicted of Terrorism," January 19, 2012, http://cpj.org/x/47b9.

101 Bill Marczak et al., *Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware,* Citizen Lab, March 9, 2015, http://bit.ly/1Ryogmr.

102 Hacking Team,"Customer Policy," accessed February 13, 2014, http://hackingteam.it/index.php/customer-policy.

103 Declan McCullagh, "Meet the 'Corporate Enemies of the Internet' for 2013," *CNET*, March 11, 2013, accessed February 13, 2014, http://cnet.co/1fo6jJZ.

104 Marczak et al., *Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware.*

105 Fahmida Y. Rashid, "FinFisher 'Lawful Interception' Spyware Found in Ten Countries, Including the U.S.," *Security Week*, August 8, 2012, http://bit.ly/1WRPuap.

Given the high degree of online repression in Ethiopia, political commentators use proxy servers and anonymizing tools to hide their identities when publishing online and to circumvent fil ering, though the tools are also subject to blocking (see Blocking and Filtering).

Anonymity is further compromised by strict SIM card registration requirements. Upon purchase of a SIM card through EthioTelecom or an authorized reseller, individuals must provide their full name, address, government-issued identification numbe , and a passport-sized photograph. EthioTelecom's database of SIM registrants enables the government to terminate individuals' SIM cads and restrict them from registering for new ones. Internet subscribers are also required to register their personal details, including their home address, with the government. During the antigovernment protests in 2016, state-owned ICT provider EthioTelecom announced plans to require mobile phones to be purchased from Ethiopian companies and to create a tracking system for all mobile devices in Ethiopia. Observers believe the plan aims to allow the government to track and identify all communications from subscribers on its network.[106]

While the government's stronghold over the Ethiopian ICT sector enables it to proactively monitor users, its access is less direct at cybercafés. For a period following the 2005 elections, cybercafé owners were required to keep a register of their clients, but the requirement has not been enforced since mid-2010.[107] Nevertheless, some cybercafé operators have reported that they are required to report "unusual behavior" to security officials, who also visit cybe cafés (sometimes in plainclothes) to ask questions about individuals or monitor activity themselves.[108]

Intimidation and Violence

Government security agents frequently harass and intimidate bloggers, online journalists, and ordinary users for their online activities. Independent bloggers are often summoned by the authorities to be warned against discussing certain topics online, while activists report that they are regularly threatened by state security agents.[109] Ethiopian journalists in the diaspora have also been targeted for harassment.[110]

Amidst escalating antigovernment protests in 2015 and 2016, the authorities reportedly harassed, detained, and abused several people who used their mobile phones to record footage of demonstrations.

Meanwhile, imprisoned bloggers reported being held in degrading conditions and tortured by prison guards seeking to extract false confessions.[111] Yonatan Wolde and Bahiru Degu were re-arrested shortly after their acquittal in April 2016 and released the next day, reporting that officials had threatened their lives.[112]

106 Endalk Chala, "Ethiopia Locks Down Digital Communications in Wake of #OromoProtests."

107 Groum Abate, "Internet Cafes Start Registering Users," *The Capital* republished *Nazret* (blog), December 27, 2006, http://bit.ly/1Lm98aX.

108 Human Rights Watch, "They Know Everything We Do," 67.

109 SIMEGNISH (LILY) MENGESHA, "CRAWLING TO DEATH OF EXPRESSION – RESTRICTED ONLINE MEDIA IN ETHIOPIA," Center for International Media Assistance (blog), April 8, 2015, http://bit.ly/1IbxFie.

110 "ክንፉ አሰፋ በስለላ ከሦሳንድ የተባረረው የጋዜጣኛውን አንነት አቆርጣለሁ አለ," *ECADAF Ethiopian News & Opinion*, April 12, 2015, http://ecadforum.com/Amharic/archives/14790/.

111 Tedla D. Tekle, "'I was forced to drink my own urine,': 'Freedom' for netizen after 647 days locked up, but not for all."

112 Tedla D. Tekle, "'I was forced to drink my own urine,': 'Freedom' for netizen after 647 days locked up, but not for all."

Technical Attacks

Opposition critics and independent voices face frequent technical attacks, even when based abroad. Independent research has found that Ethiopian authorities have used sophisticated surveillance malware and spyware, such as FinFisher's FinSpy and Hacking Team's Remote Control Servers (RCS), to target exiled dissidents.[113]

There were no reports of technical attacks against human rights defenders or dissidents during the coverage period, though hacktivists launched attacks on government websites, including the Ministry of Defense, as a form of digital protest alongside the largescale Oromo demonstrations.[114] Meanwhile, the Information Network Security Agency (INSA) reported that they had foiled at least 155 cyberattacks in 2015. Critics said they used the data to justify cracking down on the internet.[115]

113 Marczak et al., *Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware.*

114 Kinfemicheal Yilma, "Hacktivism: A New Front of Dissent, Regulation," Addis Fortune, February 14, 2016, http://addisfortune.net/columns/hacktivism-a-new-front-of-dissent-regulation/

115 "Ethiopia: The cyber attack that probably never was," Zehabesha, July 13, 2016,http://www.zehabesha.com/ethiopia-the-cyber-attack-that-probably-never-was/

Freedom House

France

	2015	2016
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	3	3
Limits on Content (0-35)	6	6
Violations of User Rights (0-40)	15	16
TOTAL* (0-100)	**24**	**25**

* 0=most free, 100=least free

Population:	**66.8 million**
Internet Penetration 2015 (ITU):	**85 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2016 Status:	**Free**

Key Developments: June 2015 – May 2016

- The prolonged state of emergency initiated by President Hollande after the Paris terrorist attacks on November 13, 2015 significantly ex anded the powers of authorities to conduct house arrests, raids, and searches of electronic devices, without prior judicial authorization (see **Legal Environment** and **Surveillance, Privacy, and Anonymity**).
- The Paris attacks impacted the number of requests to take down pro-terrorism content, as administrative measures enabled the blocking and de-indexing of infringing websites without authorization from a judge. State of emergency legislation in turn empowered the interior minister to take any measures to interrupt online public communications services inciting or glorifying terrorist acts (see **Blocking and Filtering** and **Content Removal**).
- New legislation has also bolstered the state's surveillance apparatus. In July 2015, the French Constitutional Council approved almost all provisions of a new intelligence law which requires internet service providers to install devices to monitor users' "suspicious behavior" and provide access to intelligence agencies (see **Legal Environment** and **Surveillance, Privacy, and Anonymity**).
- Parliament adopted a law to fight against o ganized crime, terrorism, and their financing in May 2016, enabling prosecutors to eavesdrop as part of their investigations, and establishing criminal sanctions for frequently visiting sites glorifying or inciting terrorist acts (see **Legal Environment** and **Surveillance, Privacy, and Anonymity**).

Introduction

Measures to address terrorist threats have impacted France's internet freedom environment by expanding government surveillance powers and limiting judicial oversight.

As France continued to reel from the horrific *Charlie Hebdo* attack in January 2015, a series of coordinated attacks stunned Paris on the night of November 13, 2015. Islamic State (IS) gunmen and suicide bombers targeted restaurants, bars, a major stadium, and a concert hall, killing 130 people and injuring hundreds more. The attacks prompted hundreds of raids throughout the country.[1] The suspected ringleader, Abdelhamid Abaaoud, a Belgian national, was killed after a long gun battle during a police raid in the Paris suburb of Saint-Denis just a few days after the events.[2]

The Paris attacks triggered draconian measures from the government, with the declaration of a state of emergency on November 13, 2015. Extended for a third time through the end of July 2016, and again for six months following a deadly terrorist attack in Nice on July 14, these emergency measures significantly ex anded authorities' powers, such as allowing house arrests and searches without judicial oversight. Provisions on electronic searches allowed authorities to access and copy user data without clarifying safeguards concerning the use of this data, even when no wrongdoing has been uncovered. State of emergency legislation also granted powers to the interior minister to immediately interrupt online communication services deemed to "incite or glorify terrorist acts."[3] In this context, United Nations human rights experts raised concerns about "excessive and disproportionate restrictions on fundamental freedoms" in France, including "the lack of clarity and precision of several provisions of the state of emergency and surveillance laws."[4]

A series of legislative changes to address threats to national security sought to expand government surveillance powers and introduce stricter measures to tackle terrorist content online. The antiterrorism law passed in November 2014 outlined prison sentences for the broad offense of "apology for terrorism" online. In early 2015, two decrees outlining administrative measures for the blocking and de-indexing of websites for terrorist content were harshly criticized by free speech advocates. Parliament also adopted a new intelligence law on June 24, 2015, granting intelligence agencies the power to intercept electronic communications in real-time and request the immediate handover of user data from ISPs, without prior court approval. The French Constitutional Council subsequently declared three of the law's provisions unconstitutional in July 2015, including one that would have allowed interception of all international electronic communications. However, following the November 2015 terrorist attacks and the declaration of the state of emergency, an amended proposal related to the monitoring and surveillance of international electronic communications was adopted.[5]

While France has traditionally maintained a relatively open and accessible internet, several actions on the part of successive administrations have raised concerns from internet freedom groups and free speech activists. During this coverage period, the controversial law on the distribution and protection of creative works on the internet, known as HADOPI, received renewed criticism after the

1 "Paris Attacks: What Happened on the Night," *BBC News*, December 9, 2015, http://bbc.in/1MEFrPj.

2 "Paris Attacks: Who were the attackers?" *BBC News*, January 19, 2016, http://bbc.in/1j9Ynx8.

3 Human Rights Watch, "France: New Emergency Powers Threaten Rights," November 24, 2015, http://bit.ly/1P8yL1Q; See also: La Quadrature du Net, "A Police State to Avoid Any Critical Evaluation?" November 19, 2015, http://bit.ly/2cFVLoh.

4 OHCHR, "UN rights experts urge France to protect fundamental freedoms while countering terrorism," January 19, 2016, http://bit.ly/20e9Jkh.

5 Law 2015-1556, November 30, 2015, http://bit.ly/2eWT2N1.

French Senate released a report recommending more drastic sanctions against piracy and fewer "educational measures."

Obstacles to Access

France's internet penetration continued to increase, reaching nearly 85 percent in 2015. The current ICT market is open, highly competitive, and has benefited from the privatization of the state-owned company France Telecom.

Availability and Ease of Access

Committed to providing widespread access to high-speed broadband, the French government has been has been implementing an ambitious national plan to deploy high-speed broadband throughout France by 2022, mobilizing public and private investments totaling 20 billion euros (US$22 billion) over 10 years.[6] The government predicts its plan will benefit 50 pe cent of the population by the end of 2016.[7] In April 2015, the French parliament approved an amendment to the telecoms component of France's economic reform law, known as the Loi Macron, requiring telecom operators to improve mobile coverage throughout the country. The law will ensure that residents of an estimated 170 municipalities, which currently have no access to mobile services, will be covered by mobile networks by 2017. Failure to comply with the obligations can result in sanctions from the telecoms regulator.[8]

In 2015, the International Telecommunication Union (ITU) estimated an internet penetration rate of 84.7 percent.[9] Fixed broadband penetration also increased, from 40.1 percent in 2014 to 41.3 percent in 2015, with almost 27 million subscriptions.[10] Wireless broadband subscriptions reached 48.8 million subscriptions in December 2015.[11] Nonetheless, some demographic disparities in internet usage still persist: for example, mobile penetration ranged from 65.3 percent in the Paris area to 42.7 percent in urban areas with less than 50,000 inhabitants.[12] Most at-home users have access to broadband connections, while the remaining households are connected either through dial-up or satellite services, usually due to their rural location.[13]

The average monthly cost of broadband internet access in France is approximately EUR 30 (USD $43), for both ADSL, and fibe -optic connections, which is fairly affordable for a large percentage of the population whose average net monthly income is 2,202 euros (USD $2,400).[14] Companies such as Free Telecom offer cheap internet access and mobile contracts through bundled deals. Speeds are fast, with Akamai data reporting connection speeds of 8.9 Mbps peak connection speeds of 43.2

6 "Plan France Très Haut Débit," official ebsite, accessed September 22, 2016, http://www.francethd.fr.

7 "Le Plan France Très Haut Débit," gouvernement.fr, September 8, 2016, http://bit.ly/21kmjzc.

8 International Telecommunications Union (ITU), "French government approves amendment mandating rural mobile expansion," April 21, 2015, http://bit.ly/1VSNxbn.

9 ITU, "Percentage of Individuals using the Internet (2000-2015)," accessed September 22, 2016, http://bit.ly/1cblxxY.

10 ITU, "Fixed-broadband subscriptions, 2000-2015," accessed September 22, 2016, http://bit.ly/1cblxxY.

11 OECD, "Total fi ed and wireless broadband subscriptions by country," accessed September 22, 2016, http://bit.ly/1cP4RGV.

12 Statista, "Mobile internet usage penetration in France from 2010 to 2014, by urban area size," March 21, 2013, accessed February 11, 2016, http://bit.ly/2eku0Fs.

13 Ariase, "L'ADSL et la fib e optique en France" [ADSL and Broadband Access in France], accessed February 12, 2016, http://bit.ly/2eHNZft.

14 "Les salariés français gagnent en moyenne 2202 euros net par mois," [French employees earn on average 2,202 Euros a month], *Le Figaro*, September 16, 2015, http://bit.ly/1P0QG6W.

Mbps at the end of 2015.[15]

According to the ITU, mobile penetration in 2015 reached 102.6 percent in 2015, up from 97.4 percent in 2012.[16] Recent figu es show that in 2015, 54.7 percent of the population accessed the internet via mobile, projecting 65.2 percent in 2017.[17]

Restrictions on Connectivity

There were no restrictions on connectivity reported during the coverage period. There is no central internet backbone, and ISPs are not required to lease bandwidth from a monopoly holder. Instead, the backbone consists of several interconnected networks run by ISPs and shared through peering or transit agreements. There are also a number of Internet Exchange Points (IXPs) in France,[18] which contribute to improved access and lower consumer prices.[19]

ICT Market

There are no significant business hu dles to providing access to digital technologies in France. The main ISPs are Orange, Free, Bouygues Telecom, and Numericable-SFR (SFR was a division of Vivendi that was sold to Numericable).[20] Others such as NRJ Mobile, Virgin Mobile, Cofidis Mobile, and Da ty make use of the main ISPs' networks, reselling the services.[21]

Numericable, after beating Bouygues' bid to acquire SFR, showed further interest in expanding its market presence by offering to buy Bouygues, its smaller loss-making rival, for 10 billion euros. The owner, Martin Bouygues, rejected the bid. Both the Economy Minister Emmanuel Macron and the Budget Minister Christian Eckert were against the deal, believing that consolidation was not the best move for the sector.[22] In the wake of their loss of SFR to Numericable and the buyout offer, Bouygues has been keen to prove they are a growing concern and accused Numericable of breach of contract.[23] Most recently, Orange showed interest in purchasing Bouygues for the same price, but negotiations failed in April 2016.[24]

Regulatory Bodies

The telecommunications industry in France is regulated by the Regulatory Authority for Electronic and Postal Communication (ARCEP),[25] while competition is regulated by France's Competition

15 Akamai, The State of the Internet, Q4, 2015 Report, accessed September 22, 2016, http://akamai.me/2b5MgzU.

16 ITU, "Mobile-cellular subscriptions 2000-2015," accessed September 22, 2016, http://bit.ly/1cblxxY.

17 Statista, "Mobile phone internet user penetration in France from 2014 to 2017," accessed February 12, 2016, http://bit.ly/2eHPKcE.

18 Internet Exchange Points, Data Centre Map, accessed February 12 2016, http://bit.ly/2dzlzY4.

19 "Internet Service Providers and Peering v3.0," DrPeering International, accessed February 12, 2016 http://bit.ly/1joJCaC.

20 Ruth Bender, "Vivendi Accepts Altice Offer to Buy 20% Numericable-SFR Stake," *Wall Street Journal,* February 27, 2015, http://on.wsj.com/2f5YxrP.

21 Jerome Tranie, «Fastest ISPs 2014: France," *PC Mag*, June 19, 2014, http://bit.ly/2euIzHk.

22 Leila Abboud and Dominique Vidalon, "France's Numericable SFR makes fresh bid for Bouygues Telecom – sources," June 21, 2015, http://reut.rs/2eyefKt.

23 Elsa Bembaron, "Bouygues Telecom sues Numericable," August 26, 2015, http://bit.ly/1he450b.

24 Geraldine Amiel , Marie Mawad , and Francois De Beaupuy, "Orange-Bouygues Deal Collapse Ends Months of Tense Diplomacy," *Bloomberg,* April 4, 2016, http://bloom.bg/2dABccT.

25 ARCEP, "Autorité de Régulation des Communications Électroniques et des Postes," http://bit.ly/1RImAXo.

Authority and, more broadly, by the European Commission (EC).[26] The commissioner of ARCEP is appointed by the government, but as an EU Member State, France must ensure the independence of its national telecommunications regulator. Given that the French state is the main shareholder in Orange, the country's leading telecom company, the EC stated that it would closely monitor the situation in France to ensure that European regulations were being met.[27] The EC has previously stepped in when the independence of national telecommunications regulators seemed under threat, notably in Romania, Latvia, Lithuania, and Slovenia.[28] ARCEP remains an independent and impartial body and decisions made by the regulator are usually seen as fair.

Net neutrality was in the news when the new European Regulation related to net neutrality was adopted in November 2015 and came into effect in April 2016.[29] In September, ARCEP, working with European counterparts (the Body of European Regulators of Electronic Communications), released four factsheets regarding the implementation of the new regulations concerning net neutrality. The factsheets summarized key points in four areas: traffic management, comme cial practices, optimized services that are distinct from internet access, and the quality of internet access services.[30] ARCEP will be in charge of overseeing the application of net neutrality in France, with strengthened transparency obligations of operators and ISP commercial practices (bundling, zero-rating, and sponsored data) under particularly scrutiny.

Limits on Content

In the wake of deadly terrorist attacks in France, attention over mechanisms to counter pro-terrorist content online reached new levels during this period of coverage. Expanded state of emergency legislation enabled the interior minister to immediately censor any website deemed to promote terrorism or incite acts of terrorism. The HADOPI anti-piracy law was also back in the news due to a proposed update to its tenets, prompting criticism from internet rights watchdogs.

Blocking and Filtering

France does not generally engage in any politically motivated blocking of websites. YouTube, Facebook, Twitter and international blog-hosting services as a whole are freely available. However, since the *Charlie Hebdo* and November 2015 attacks in Paris, the government has released statements suggesting that limiting fundamental rights of citizens would serve public safety,[31] and terrorist-related content has been subject to censorship.

A decree issued in February 2015 outlined administrative measures to block websites containing materials that incite or condone terrorism, as well as sites that display child pornography.[32] The decree implemented article 6-1 of the Law on Confidence in the Digital Economy (CEN), passed in 2004, as

26 "Autorité de la concurrence," accessed February 12, 2016, http://bit.ly/1frpn7J.

27 "ARCEP must remain independent vis-a-vis government – EC," *Telecompaper,* January 14, 2011, http://bit.ly/1k5gzJe.

28 Arjan Geveke, "Improving Implementation by National Regulatory Authorities," European Institute of Public Administration, 2003, accessed February 12, 2016, http://bit.ly/2dAAlJ2.

29 EU Regulation 2015/2120, November 25, 2015, http://bit.ly/2efzIeu.

30 ARCEP, "Net Neutrality," September 2015, accessed February 12, 2016, http://bit.ly/1NDlZIP.

31 "Valls : «La sécurité est la première des libertés" [Valls : Security is the fi st of liberties], *La Depeche*, January 7, 2016, http://bit.ly/2eydvoA.

32 Decree 2015-125 of February 5, 2015, http://bit.ly/2cqSoRr.

well as article 12 of new antiterrorism law passed in November 2014.[33] The administrative authority, in this case the Central Office for the Fight against Crime elated to Information and Communication Technology (OCLCTIC), is in charge of creating a blacklist of sites containing infringing materials, and must review the list every four months to ensure that blacklisted sites continue to contravene French law. OCLCTIC can request editors or hosts to remove the content, and after a 24 hour period it can request ISPs to block the site.[34] Users trying to access those pages are redirected to a website from the Ministry of Interior indicating why the site was blocked and avenues for appeal. Shortly after the decree was announced, fi e websites were blocked with no judicial or public oversight under suspicion of containing terrorism-related information.[35]

A fi st activity report covering the period between March 2015 and February 2016 noted that French authorities made 312 requests to block sites (some of them were made available again after the removal of infringing content). Administrative blocking requests for terrorist content targeted 68 sites, compared to 244 sites displaying child pornography. The Paris attacks in November 2015 significantly impacted the number of overall requests to censor content linked to terrorism (see also Content Removal).[36]

Meanwhile, under the extended state of emergency legislation fi st adopted in November 2015, the interior minister was given the power to block websites and social media, taking "any measure to ensure the interruption of any public communication service online that glorifies or inci es acts of terrorism."[37] Although the National Commission on Informatics and Liberty (CNIL) noted in its April 2016 report that the "implementation methods of this measure have not been specified, and o date, the Minister of Interior has not resorted to it."[38]

While no "over blocking" was reported during this period, a chief concern remains the lack of judicial oversight in the blocking of websites that incite or promote terrorist acts. The procedure is supervised by the CNIL, the data protection agency. As an administrative authority, CNIL can also refer requests to the administrative court should they be unhappy with any action taken by the OCLCTIC. Some commentators have lamented that while CNIL was founded to protect internet freedoms, it is now overseeing the restriction of those same rights.[39] Critics also question the lack of a clear definition of what constitutes problematic content, which has led to the prosecution of more than seventy people after the Charlie Hebdo attacks based on the anti-terrorism law of 2014, one of whom was a French teenager who merely posted a drawing on Facebook (see Violations of User Rights).[40]

33 "L'impossible et controversé blocage des sites Internet djihadistes," [The impossible and controversial blocking of jihadist sites], *Le Monde,* September 13, 2014, http://bit.ly/2dfofWV.

34 The blocking order can be issued immediately if the editor does not provide information stipulated under article 6-III of LCEN. See: Article 12, Law 2014-1353 of November 13, 2014, http://bit.ly/2eeaTwZ.

35 Lucie Ronfaut, "La France bloque pour la première fois des sites Web de propagande terroriste" [France blocks terrorist propaganda websites for the fi st time], *Le Figaro,* March 16, 2015, http://bit.ly/2eAyTsT.

36 "Blocages de sites web, le bilan de la Cnil," [Website blockings, CNIL's report], *Libération,* April 15, 2016, http://bit.ly/1T9zkIa; See also: Alexandre Linden, "Rapport d'activité de la personne qualifiée" [Activity eport], March 2015 – February 2016, CNIL, accessed September 1, 2016, http://bit.ly/2eAO4Ch.

37 Law 2015-1501 of November 20, 2015, http://bit.ly/1qraiKQ See also: Daniel Severson, "France's Extended State of Emergency: What New Powers Did the Government Get?" *Lawfare*, November 22, 2015, http://bit.ly/1OYBpSl; Glynn Moody, "French state of emergency allows website blocking, device search powers," *Ars Technica*, November 20, 2015, http://bit.ly/1XeWKf1.

38 Alexandre Linden, "Rapport d'activité de la personne qualifiée" [Activity eport], March 2015 – February 2016, CNIL, accessed September 1, 2016, http://bit.ly/2eAO4Ch.

39 EDRI, "France implements Internet censorship without judicial oversight," March 11, 2015, accessed February 12, 2016 http://bit.ly/1CasJYJ.

40 Julien Lausson, "Apologie du terrorisme: un ado poursuivi à cause d'un dessin sur Facebook" [Apology of terrorism: a teenager prosecuted because of a drawing on Facebook] *Numerama*, January 17, 2015, http://bit.ly/1ZDWSsl.

Content Removal

French authorities are fairly transparent about what content is prohibited and the reasons behind specific con ent removal requests. Incitement of hatred, racism, Holocaust denial, child pornography, copyright infringement, and defamation are illegal. Article R645-1 of the French criminal code outlaws the display of the emblems, uniforms, or badges of criminal organizations, under penalty of a fine [41]

As stipulated in the 2014 anti-terrorism law, the administrative authority (OCLCTIC) can request editors and hosts to remove content that incites or apologizes for terrorism, as well as sites that display child pornography; after a 24 hour period it can request ISPs to block the site (see Blocking and Filtering).[42]

A government decree issued on March 4, 2015 also allows for the delisting of online content from search results using a similar administrative procedure supervised by CNIL.[43] Under this decree, OCLCTIC submits requests to search engines, which then have 48 hours to comply. The OCLCTIC is responsible for reevaluating de-indexed websites every four months, and requesting the relisting of websites where the incriminating content has been removed. According to CNIL's report, between March 2015 and February 2016, French authorities made 855 de-indexing requests (of which 386 were for pro-terrorist content, and 469 for child pornography), as well as 1,439 removal requests (of which 1,286 were for pro-terrorist content, and 153 for child pornography content). Content was removed in 1,179 of cases.[44]

CNIL reportedly gave the green light for all of these removal and de-indexing requests, except in one case: a photo that was widely circulated on social media and blogs, showing the aftermath of the Bataclan concert hall in Paris, where gunmen claimed the lives of 90 victims on November 13, 2015.[45] CNIL argued that only the context of the photo's publication could determine whether it was inciting or glorifying terrorism. OCLCTIC subsequently followed this recommendation.

The anti-piracy law HADOPI, originally passed in June 2009[46] and supplemented by a second law in October 2009[47] was once again in the news in 2015. In July 2015, the digital rights group La Quadrature du Net (LQDN) strongly objected to a Senate report from July 2015 that proposed an extra-judicial administrative fine, giving HADOPI the right o essentially bypass the legal procedure if they so desired.[48] LQDN also pointed out that the report drew on earlier recommendations,[49] which would

41 Elissa A. Okoniewski, "Yahoo!, Inc. v. Licra: The French Challenge to Free Expression on the Internet," American University International Law Review 18, 1, 2002, http://bit.ly/1LOzaFS.

42 See Article 12, Law 2014-1353 of November 13, 2014, http://bit.ly/2eeaTwZ.

43 The decree implements modifications o the 2004 LCEN that were made under the 2011 LOPPSI 2 and the 2014 antiterrorism law. See: Decree 2015-253 of March 4, 2015, http://bit.ly/2ctwhi3.

44 Alexandre Linden, "Rapport d'activité de la personne qualifiée" [Activity eport], March 2015 – February 2016, CNIL, accessed September 1, 2016, http://bit.ly/2eAO4Ch.

45 "Le gouvernement demande à Facebook et Twitter de censurer une photo du Bataclan," [Government asks Facebook and Twitter to censor a photo of the Bataclan], *Le Figaro,* November 18, 2015, http://bit.ly/1YgahVR.

46 Law 2009-669 of June 12, 2009, http://bit.ly/2dAON3J.

47 Law 2009-1311 of October 28, 2009, http://bit.ly/2eAOvw7.

48 Loïc Hervé and Corinne Bouchoux, "Rapport d'information au nom de la commission de la culture, de l'éducation et de la communication (1) par la mission d'information sur la Hadopi" [Information report in name of the commission on culture, education and communication by the information mission on Hadopi], Senate, Extraordinary Session 2014-2015, July 8, 2015, http://bit.ly/2eHIEn8.

49 La Quadrature du Net, "Rapport MIQ : le vrai visage du SOPA à la française" [MIQ Report: the true face of the French SOPA], May 12, 2014, http://bit.ly/2eI8WqS.

mean HADOPI had the power to act as content monitors, carrying out private policing of copyright.[50] In a surprise move, parliament adopted a proposal in April 2016 to suppress HADOPI by February 2022,[51] but the Senate voted to reverse this move.[52] HADOPI functions by responding to copyright infringers with a graduated response, starting with an email warning for the fi st offense, followed by a registered letter if a second offence occurs within six months. If a third offence occurs within a year of the registered letter, the case can be referred to the court, and the offender may receive a fine as a possible sanction.[53]

The legal debate over the right to be forgotten also escalated in the past year. In June 2015, the French data protection agency CNIL ordered Google to extend the "right to be forgotten" ruling across all of its sites that can be accessed within the country, including Google.com and not just Google.fr.[54] Google raised concerns that the move would set a dangerous precedent for authoritarian governments, who could also request that Google apply national laws extraterritorially.[55] An informal appeal by Google was rejected in September 2015, and CNIL threatened to take action against Google with fines f approximately EUR 300,000 should they refuse to comply.[56] In early February 2016, Google announced that it would comply by removing certain search results across all EU domains.[57]

A ruling in early February 2016 by a Paris court established that Facebook could be sued in France for removing the account of a French user who posted an image of a 19th century painting of a naked woman by Gustave Courbet. A French court will now be entitled to hear the case, brought by the account's Parisian user. Facebook had argued that cases concerning their terms and conditions could only be heard by a Santa Clara, CA court, where its headquarters are based. This was dismissed by a Paris appeals court, which ruled that should the case involve a French user, it can be heard in France. The decision can be appealed to France's highest court.[58]

Media, Diversity, and Content Manipulation

France is home to a highly diverse online media environment. Self-censorship online is minimal, and there were no reports of the French government proactively manipulating content online. There are no recent cases of paid government commentators and discriminatory allocation of advertising.

Meanwhile, government measures to counter terrorist propaganda online have taken center stage in the wake of deadly terrorist attacks. The French government recently introduced a communication campaign against extremist radicalization aimed at preventing and tackling jihadist propaganda

50 La Quadrature du Net, "Rapport Hadopi au Sénat: le pire est devant nous!" [HADOPI Report to the Senate: the worst is ahead of us!], July 9, 2015, http://bit.ly/1MmSx4K.

51 Amaelle Guiton, "La fin d'Hadopi, une agonie politique" [The end f Hadopi, a political agony], *Libération,* April 30, 2016, http://bit.ly/1SUW2np.

52 Elsa Trujillo, "Les sénateurs sauvent la Hadopi de la disparition," [Senators vote to save Hadopi from disappearance], *Le Figaro,* May 26, 2016, http://bit.ly/1RxskAH.

53 Guillaume Champeau, "HADOPI: An FAQ to learn all," *Numerama,* February 10, 2016, http://bit.ly/2dRVwdH.

54 CNIL, "Right to delisting: Google informal appeal rejected," September 21, 2015, http://bit.ly/1NGpDz2.

55 Peter Fleischer, "Implementing a European, not global, right to be forgotten," Google Europe Blog, July 30, 2015, http://bit.ly/2dgeyHK.

56 Samuel Gibbs, "French data regulator rejects Google's right-to-be-forgotten appeal," *The Guardian*, September 21, 2015, http://bit.ly/1Kvr6nf.

57 Danielle Correa, "'Right to be forgotten' extended to all Google domains in EU," *SC Magazine UK*, February 12, 2016, http://bit.ly/2dzFTbB.

58 "Court says Facebook nude painting case can be tried in France," *Reuters,* February 12, 2016, http://reut.rs/1PKGzCL.

online[59] and has turned to the private sector to discuss plans to counter extremist discourse and terrorist propaganda.[60]

Digital Activism

French digital rights and advocacy groups, such as La Quadrature du Net (LQDN), are very active in the country, playing a significant ole in protesting the government's recent moves to expand surveillance and blocking measures without judicial oversight.[61] In the past, LQDN successfully lobbied the European Parliament for an amendment to the European Union Telecoms Package to ensure that no restrictions on internet access could be imposed without prior judicial approval. [62]

The #NuitDebout movement is a recent example of a large scale digital campaign. Launched in March 2016 to protest against newly adopted labor reforms, activists used their own online radio and TV stations and various social media channels to share information and organize large nightly assemblies at the Place de la République in Paris. The protests were subsequently replicated in other cities across the country. The movement has since broadened to include other important issues and has taken a critical stance on France's political system, calling for social and political change.[63]

Violations of User Rights

Both in the lead up and in reaction to terrorist attacks, a series of legislative changes have raised concerns among digital and human rights activists. The prolonged state of emergency initiated after the Paris terrorist attacks in November 2015 has significantly expanded the powers of authorities to conduct house arrests, raids, and searches and seizures of devices, without judicial oversight. New laws to address threats to national security have also bolstered the state's surveillance powers and introduced stricter measures to tackle terrorist propaganda online.

Legal Environment

In accordance with the 1789 Declaration of the Rights of Man,[64] France's constitution guarantees freedom of speech.[65] The European Convention on Human Rights, of which France is a signatory, provides for freedom of expression, subject to certain restrictions which are "necessary in a democratic society."[66]

59 "Stop Jihadism" website, accessed September 1, 2016, http://www.stop-djihadisme.gouv.fr/.

60 Martin Untersinger and Morgane Tual, "Contre la propagande djihadiste en ligne, le gouvernement se tourne vers le secteur privé," *Le Monde,* May 9, 2016, http://bit.ly/2cJBtdS.

61 La Quadrature du Net, "Who are we?" accessed February 15, 2016, http://bit.ly/2dzGBpm.

62 Danny O'Brien, "Blogging ACTA across the globe: the view from France," Electronic Frontier Foundation, January 2010, accessed February 15, 2016, http://bit.ly/2eXcb1u.

63 Elisabetta Ferrari, "#nuitdebout: 5 things to know about the movement that's spreading through France (and maybe Europe)," Media Activism Research Collective, April 16, 2016, http://bit.ly/1WxvCel.

64 "The free communication of ideas and opinions is one of the most precious of the rights of man. Every citizen may, accordingly, speak, write, and print with freedom, but shall be responsible for such abuses of this freedom as shall be defined by la ." See: Declaration of the Rights of Man 1789, September 1, 2016, http://bit.ly/1AgkDwp.

65 Guy Carcassonne, "The Principles of the French Constitution," published on the website of the Embassy of France in Washington, DC, November 28, 2007, http://bit.ly/1X4r11P.

66 European Court of Human Rights, European Convention on Human Rights, accessed September 1, 2016, http://bit.ly/1foTq0D.

Since November 2015, broad new powers under the state of emergency have raised concerns among human rights and digital activists.[67] While Prime Minister Manuel Valls declared on November 19 that it was a "short term response,"[68] the state of emergency was subsequently extended three times to beyond this report's coverage period.[69] The state of emergency includes provisions on electronic searches (see Surveillance, Privacy, and Anonymity).[70] The state of emergency also empowered the interior minister to take "any measure to ensure the interruption of any online public communication service that incites the commission of terrorist acts or glorifies them"[71]

Meanwhile, measures to address terrorism were already in place prior to the November 2015 state of emergency. The antiterrorism law passed in November 2014 penalizes online speech deemed as "apology for terrorism" (apologie du terrorisme) with up to seven years in prison and a EUR 100,000 (US$100,000) fine. Online penalties a e harsher than offline, which is subject o fi e years in prison and a EUR 75,000 fine [72] Another law adopted by parliament in May 2016 and enacted in June 2016 "on the fight against errorism and organized crime" also provides sentences of up to two years in prison or a EUR 30,000 fine for f equently visiting sites that glorify or incite terrorist acts, unless these consultations are done in "good faith," such as journalistic or research activities (see also Surveillance, Privacy, and Anonymity).[73]

In a positive step, following a process of public consultation, the National Assembly adopted a "Digital Republic" bill in January 2016, covering a wide range of issues such as access to public data, safeguards for net neutrality, and the protection of personal data. The bill reached the final stage f the parliamentary process in September 2016.[74]

Prosecutions and Detentions for Online Activities

During the coverage period, multiple sentences were handed down to online users for glorifying terrorism.[75]

In February 2016, police arrested the owner of a website (Darkness.su) that provides anonymous

67 "Human Rights Watch, "France: New Emergency Powers Threaten Rights," November 24, 2016, http://bit.ly/1P8yL1Q.

68 "Discours de Manuel VALLS, Premier ministre, Projet de loi sur la prorogation de l'état d'urgence, Assemblée nationale" [Speech by Manuel Valls, Prime Minister: bill on the extension of the state of emergency, National Assembly], gouvernement.fr, November 19, 2015, http://bit.ly/2duhrIJ.

69 See: Declaration of the State of Emergency, November 14, 2015; First extension of three months, Law 2016-162, February 19, 2016; Second extension of two months, Law 2016-629, May 20, 2016; Third extension of six months, Law 2016-987, July 21, 2016.

70 La Quadrature du Net, "A Police State to Avoid any Critical Evaluation?" November 19, 2015 http://bit.ly/1kNOJlk; See also: Glynn Moody, "French state of emergency allows website blocking, device search powers," *Ars Technica*, November 20, 2015, http://bit.ly/1XeWKf1.

71 Law 2015-1501 of November 20, 2015, Article 11, http://bit.ly/2evb2MQ.

72 Law 2014-1353 of November 13, 2014, http://bit.ly/1T1dzwE.

73 Law 2016-731 of June 3, 2016, http://bit.ly/2cS1zAO.

74 The bill came into force outside the period of coverage of this report, on October 7, 2016. See: Law 2016-1321 of October 7, 2016, http://bit.ly/2eAVW6D.

75 See for example: "A Nice, une Franco-Tunisienne condamnée à trois ans de prison pour apologie du terrorisme," [Franco-Tunisian woman sentenced to three years in prison in Nice for apology of terrorism] *Le Monde,* 18 June, 2016, http://bit.ly/2eIhRbJ; "Condamné pour apologie du terrorisme sur internet" [Condemned for apology of terrorism online], *La Depeche,* November 21, 2015, http://bit.ly/2dMZyU2; "Apologie du terrorisme sur Twitter : un ado condamné à 2 ans de prison ferme" [Apology of terrorism on Twitter : teenager sentenced to two years of prison], *Numerama,* December 11, 2015, http://bit.ly/2e1yaiF; Une peine record à Montpellier pour un homme accusé d'apologie du terrorisme sur internet [Record sentence in Montpellier for man accused of apology of terrorism online], *France 3 Languedoc-Roussillon,* August 31, 2016, http://bit.ly/2dAXv24.

messaging services for failing to cooperate with authorities in an investigation linked to a series of fake bomb threats against schools around the world. A group called "Ev4cuati0nSquad" had allegedly placed threatening calls using the messaging service. He was taken in for questioning after refusing to provide police with the encryption key to allow authorities access to the data.[76]

Surveillance, Privacy, and Anonymity

Surveillance has escalated in recent years, not least with the enactment of a new surveillance law in June 2015, which was passed in the wake of the attacks on *Charlie Hebdo* by armed extremists earlier that year. The *Loi Relatif au Renseignement*, or Intelligence Law,[77] allows for intelligence agencies to conduct electronic surveillance without a court order and requires ISPs to install so-called "black boxes," algorithms that analyze users' metadata for "suspicious" behavior in real time.[78] The French Constitutional Council subsequently declared three of the law's provisions unconstitutional in July 2015, including one that would have allowed the interception of all international electronic communications. However, an amendment enabling mass surveillance of electronic communications sent to or received from abroad was later adopted on November 30, 2015, shortly after the Paris attacks on November 13, for the purposes of "defending and promoting the fundamental interests of the country."[79]

Under the state of emergency established in November 2015, the authorities were granted powers to access and copy user data, with little judicial oversight and without clarifying safeguards concerning the use of this data.[80] The constitutional council struck down the provision allowing the authorities to copy user data in February 2016, citing the lack of judicial oversight.[81] A new version of this provision was reintroduced in July 2016, adding certain judicial guarantees.[82]

The newest law related to the fight against o ganized crime and terrorism, adopted by parliament in May 2016 and enacted in June 2016, has also elicited strong reactions from the public.[83] The law notably expands special investigation methods to prosecutors and investigating judges, which were previously reserved for intelligence services. This includes bugging private locations, using phone eavesdropping devices such as IMSI catchers, and night-time searches.[84]

76 Florian Reynaud and Soren Seelow, "Alertes à la bombe dans les lycées : le jeune homme placé sous le statut de témoin assisté" [Bomb alerts in high schools: young man placed under the status of an 'assisted witness'], *Le Monde, February 10, 2016,* http://bit.ly/1SIGtlg.

77 Law 2015-912 of July 24, 2015, http://bit.ly/1SMCPq3.

78 Angelique Chrisafis, "France asses new surveillance law in wake of Charlie Hebdo attack," *The Guardian*, May 5, 2015, http://bit.ly/1Qj1XAK.

79 Law 2015-1556 of November 30, 2015, http://bit.ly/2eWT2N1.

80 La Quadrature du Net, "A Police State to Avoid any Critical Evaluation?" November 19, 2015, http://bit.ly/1kNOJlk; See also: Glynn Moody, "French state of emergency allows website blocking, device search powers," *Ars Technica*, November 20, 2015, http://bit.ly/1XeWKf1.

81 Jean-Baptiste Jacquin, "Etat d'urgence : le Conseil constitutionnel censure les saisies informatiques lors des perquisitions" [State of emergency : Constitutional Council censors IT seizures during searches], *Le Monde,* February 19, 2016, http://bit.ly/2e-B8z1u.

82 Alexandre Boudet, "La version 4 de l'état d'urgence est la plus musclée depuis novembre 2015" [Version 4 of the state of emergency : the most beefed up version since November 2015], *Huffington Post,* July 27, 2016, http://huff.to/2e1B8Uz.

83 Law 2016-731 of June 3, 2016, http://bit.ly/2c7knag; See also : Jean-Baptiste Jacquin, "La France se dote de la loi antiterroriste la plus sévère d'Europe" [France gets the strictest antiterrorist law in Europe], *Le Monde,* May 12, 2016, http://bit.ly/2eB-2jqA; Donald Hebert, "Ce qui fait polémique dans le projet de loi Urvoas contre le terrorisme" [What is generating constroversy with the Urvoas bill against terrorism], *Nouvel Obs*, March 3, 2016, http://bit.ly/2dB1uLL.

84 "No Government has done more to counter terrorism to date," gouvernement.fr, July 17, 2016, http://bit.ly/2eB98bw; Laetitia Valy, "Lutte contre le terrorisme : les 3 nouveautés à ne pas manquer !" [Fight against terrorism: three novelties not to miss!], *Net-Iris*, June 13, 2016, http://bit.ly/2evOIEA.

Other recent regulations on electronic surveillance were passed in December 2013 and came into force in January 2015, as part of a routine military spending bill (the Military Programming Law, or LPM). Article 20 of the LPM significantly ex anded electronic surveillance of French residents and businesses by requiring ISPs to hand over data such as phone conversations, emails, internet activity, personal location data, and other electronic communication data to public authorities. The powers relate to the General Directorate for Internal Security (DCRI), three intelligence agencies under the Ministry of Defense, as well as anti-money-laundering and customs agencies. Under the law, these agencies can conduct surveillance without prior court approval for purposes of "national security," the protection of France's "scientific and economical po ential," and the prevention of "terrorism" or "criminality."[85] The office f the prime minister authorizes surveillance and the National Commission for Security Interception (*Commission nationale de contrôle des interceptions de sécurité*, CNCIS) must be informed within 48 hours in order to ensure its approval.[86] Critics have pointed out that the CNCIS lacks appropriate control mechanisms and independence from political interference, given that the CNCIS is composed of only three politicians.[87] On the other hand, the government argued that the law provides an improved legal framework for practices that have already been in place for years.[88]

Article 23 of LOPPSI 2, adopted in 2011, grants the police with the authority to install malware—such as keystroke logging software and Trojan horses—on a suspect's computer in the course of counter-terrorism investigations, although authorization must come from a court order.[89]

Regarding user privacy protections, a French order in February 2016 from the European Data Protection Authority ruled that Facebook was not allowed to track non-users in France or transfer personal data to U.S. servers. Facebook tracks the online movements of its users via its tracking cookies and plugins on third party websites, even if they are logged out, but this will not be legal to do to European citizens under the new order. French authorities said Facebook would be fined if they did not comply within three months.[90]

Intimidation and Violence

There were no reported physical attacks against bloggers or online journalists in France. Under the state of emergency however, human rights groups have documented abusive searches and house arrests based on suspected terrorist-related activity.[91] Regional media reported on a number of raids and seizures specifically ta geting suspects of online activism and propaganda.[92]

85 Alexandre Entraygues, "France—New 'Patriot Act' imposes surveillance obligations," Linklaters, January 31, 2014 http://bit.ly/1LOD6X5.

86 Kim Willsher, "French officials can moni or Internet users in real time under new law," *The Guardian,* December 11, 2013, http://bit.ly/18mtHm0.

87 Guillaume Champeau, "La DGSI investi du pouvoir de surveiller les communications sur internet" [The DGSI granted surveillance powers over the internet], *Numerama,* May 2, 2014, http://bit.ly/2extbqS.

88 Scott Sayare, "France broadens its surveillance power," *The New York Times,* December 14, 2013, http://nyti.ms/1MBpsFD.

89 Emilien Ercolani, "Loppsi : qui pourra installer les mouchards informatiques?" [Loppsi: Who could install spywares?], *L'informaticien,* November 7 2011, http://bit.ly/1MBpDkh.

90 Rakesh Krishnan, "French Orders Facebook to Stop Tracking Non-Users or Face Fines," *The Hacker News,* February 9, 2016, http://bit.ly/2dN6KPL.

91 Human Rights Watch, "France: Abuses under State of Emergency," February 3, 2016, http://bit.ly/1SZmwpH; Amnesty International, "France: Upturned lives: The disproportionate impact of France's state of emergency," February 4, 2016, http://bit.ly/1ZFuUeJ.

92 See for example: "Perquisition à Hérouville : «Activisme et propagande sur Internet»" [Raid in Hérouville : Activism and propaganda on the internet], *Ouest-france.fr*, November 20, 2015, http://bit.ly/2e1vAcm.

Technical Attacks

According to the Global State of Information Security Survey 2016, the number of recorded cyber-attacks in France has grown by 51 percent in the last year – which translates to approximately 21 attacks per day – compared to 38 percent globally.[93] In response, French cybersecurity budgets have increased by an average of 29 percent, compared to 24 percent globally, commensurate with the financial loss caused by the incidents (EUR 3.7 million on a erage per company).[94]

One of the main cybersecurity headlines in 2015 was the hacking of the television and online news outlet TV5Monde on April 8, 2015. Hackers claiming to belong to the Islamic State breached the company's information systems, overriding TV5Monde's broadcasted programming for more than three hours and disabling live broadcasts for a day on 11 channels. The group, which called itself "CyberCaliphate," also hacked the news company's website and social media accounts.[95] News reports suggest that the cyberattackers were able to gain access by phishing three employees of the company who clicked on an infected email in January.[96] The Twitter account of French newspaper *Le Monde* was also hacked by supporters of the Syrian government in January 2015. In the weeks after the terrorist attacks against *Charlie Hebdo*, authorities reported some 19,000 cyberattacks against French websites.[97]

93 Philippe Trouchaud, "The Global State of Information Security, Survey 2016 - Turnaround and Transformation in cybersecurity," PriceWaterhouse Coopers France, October 2015, accessed February 16, 2016, http://pwc.to/1NLowjA.

94 Elodie Gaillard, "Press Release in 2015," PriceWaterhouse Coopers France, October 15, 2015, http://pwc.to/1Phurem.

95 Angelique Chrisafis and Samuel Gibbs "French media groups to hold emergency meeting after Isis cyber-attack," *The Guardian*, April 9, 2015, http://bit.ly/1PlUUrz.

96 Jean-Paul Marthoz, "Cyberattacks rattle French, Belgian media outlets," Committee to Protect Journalists (blog), April 16, 2015, http://bit.ly/2evSI8b.

97 Aurelien Breeden and Alissa J. Rubin, "French Broadcaster TV5 Monde Recovers After Hacking," *New York Times,* April 9, 2015 http://nyti.ms/1DuINn0.

Freedom House

The Gambia

	2015	2016
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	18	18
Limits on Content (0-35)	21	22
Violations of User Rights (0-40)	26	27
TOTAL* (0-100)	**65**	**67**

* 0=most free, 100=least free

Population:	**1.99 million**
Internet Penetration 2015 (ITU):	**17 percent**
Social Media/ICT Apps Blocked:	**Yes^**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

^Occurred after coverage period until September 2016

Key Developments: June 2015 – May 2016

- Network slowdowns occurred throughout 2015 and early 2016, and an internet shutdown was reported in the Greater Banjul Area during rare anti-government protests in April 2016 (see **Restrictions on Connectivity**).
- In July 2015, a radio journalist was arrested for sending pictures that allegedly incited hatred against the president via Facebook and WhatsApp; in August, a Facebook user was arrested for sharing blasphemous content (see **Prosecutions and Detentions for Online Activities**).
- Numerous activists associated with the April 2016 protests reported hacking and hijacking attacks on their social media accounts (see **Technical Attacks**).

Introduction

Internet freedom declined in The Gambia due to frequent disruptions in internet and mobile access during protests, as well as growing arrests, violence, and technical attacks against activists and online journalists for their independent reporting.

Under the authoritarian rule of President Yahya Jammeh, who has been in power since overseeing a military coup in 1994, political rights and civil liberties have been severely restricted in The Gambia, with conditions for press freedom and freedom of expression particularly poor, both online and off.

In the past year, as the country geared up for presidential elections set for December 2016, the government ramped up its repression of critical voices, particularly following unprecedented anti-government protests in April 2016 that were sparked by online activism. In a rare and courageous outburst of dissent, protesters demanded electoral reforms and Jammeh's resignation. The protests were nonetheless met with a brutal crackdown, along with an hours-long internet shutdown impacting users in the Greater Banjul Area where the protesters were based.

Dozens of independent online news and opposition websites remained blocked in the past year, while popular communications platforms such as WhatsApp, Viber, and Skype were reportedly blocked beginning in August 2016. Observers suspected that the blocks may be a part of a larger effort to quash anti-government initiatives and sentiments from proliferating online in the lead up to December elections.

Obstacles to Access

Service slowdowns plagued Gambian ICT users throughout the coverage period, lasting several hours at a time, while an internet shutdown in the Greater Banjul Area was reported during anti-government protests in April 2016.

Availability and Ease of Access

Access to the internet in The Gambia expanded incrementally in the past year. Internet penetration increased from 16 percent in 2014 to 17 percent in 2015, according to the International Telecommunication Union (ITU).[1] By contrast, The Gambia has one of the highest mobile phone penetrations in Africa, with a rate of 131 percent in 2015, up from 120 percent in 2014,[2] and most Gambians access the internet via mobile devices, with less than 1 percent of users subscribing to fi ed-broadband services.[3] Nonetheless, connection speeds are generally very slow, averaging 2.0 Mbps (compared to a global average of 6.3 Mbps as of early 2016[4]), according to Akamai's *State of the Internet* report.[5]

Cost remains one of the primary hindrances to internet access in The Gambia, where 48 percent of

1 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1cblxxY.
2 International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions, 2000-2015," http://bit.ly/1cblxxY.
3 International Telecommunication Union, "Fixed (Wired)-Broadband Subscriptions, 2000-2015," http://bit.ly/1cblxxY.
4 Akamai, "State of the Internet, Q1 2016 Report," https://goo.gl/TQH7L7.
5 Akamai, "Average Connection Speed," map visualization, *The State of the Internet*, Q1 2016, accessed August 1, 2016, http://akamai.me/1LiS6KD.

individuals live in poverty.[6] The introduction of 3G wireless internet connections via mobile devices has made internet access more accessible, albeit only for a small subset of the population who can afford the data packages. According to 2015 research by the Alliance for an Affordable Internet (A4AI), 500MB of mobile data costs over 10 percent of the country's GNI per capita, which is well above the target of 5 percent or less set by the UN Broadband Commission in 2011 as a goal for broadband affordability.[7] Nevertheless, A4AI ranked The Gambia fi th among thirty other developing countries for affordability in 2015.[8]

Limited access to telecommunications services in The Gambia is also compounded by a significant urban-rural divide. In general, rural areas suffer from poor or virtually nonexistent infrastructure, a lack of affordable electricity, and frequent power cuts.[9] In addition, network coverage of rural areas has not been an investment priority for most service providers,[10] making rural provinces in The Gambia some of the most disconnected regions of the world.[11] Radio remains the principal mass medium through which most Gambians stay informed.

Restrictions on Connectivity

The Gambian government's control over the country's telecommunications infrastructure enables it to restrict access to the internet and mobile phone services with little to no oversight or transparency. Network slowdowns ensued throughout 2015 and early 2016, leading to strong suspicions of government throttling.

In April 2016, the internet was reportedly shutdown for several hours during unprecedented anti-government protests, affecting users in the Greater Banjul Area where the protesters were based.[12] Activists suspected that the government may have ordered internet services providers (ISPs) to shutdown internet services in an attempt to disrupt the demonstrations, particularly since they received technical support from Gambian activists based abroad.[13]

The state-owned telecom company, Gambia Telecommunications Company Limited (Gamtel), owns the fibe -optic cable that runs across the country and controls the country's connection to the international internet via the ACE (Africa Coast to Europe) submarine cable system, allowing private telecoms to lease access to the gateway for data services.[14] In a positive step, the government began liberalizing gateway services in May 2013 by granting international data transmission licenses to private telecom operators.[15] Details are vague as to how many new licenses had been issued by the end of 2015, but sources said no more than fi e.[16] The government also launched the country's fi st internet exchange point (IXP) in July 2014 to boost speed, security, and affordability of internet ser-

6 "Gambia," World Bank data, accessed August 1, 2016, http://data.worldbank.org/country/gambia-the

7 The 2015-16 Affordability Report, February 2016, http://linkis.com/a4ai.org/KFLhN

8 The 2015-16 Affordability Report, February 2016, http://linkis.com/a4ai.org/KFLhN

9 "World Bank Boosts Energy Supply to Support Regional Trade and Integration in West African Countries," April 29, 2015, http://bit.ly/2fMpXnP

10 Interviews by Freedom House with several customers of the national GSM operator, GAMCEL, April 2016.

11 Enrico Calandro et al., "Mapping Multistakeholderism in Internet Governance: Implications for Africa," Research ICT Africa, July 2013, http://bit.ly/1L1FFlb

12 Sidi Sanneh, "Gambia's Information Minister orders shut-down of the internet as protests against Jammeh spread," (blog), April 16, 2016, https://sidisanneh.blogspot.nl/2016/04/gambias-information-minister-orders.html

13 Freedom House author interviews, May 2016.

14 "The African Coast to Europe (ACE)," Gambia, December 3, 2012, http://bit.ly/1VGThFe.

15 Michael Malakata, "Gambia opens up international gateway for data," *PC Advisor*, May 23, 2013, http://bit.ly/1R17r2B.

16 Interviews by Freedom House, January 2016

vices across the country.[17] As of mid-2016, no issues of government control over the new IXP have been reported. Fixed-line voice communications, on the other hand, remain purely state-owned and controlled, seen mostly as part of the government's effort to protect Gamtel's monopoly.

ICT Market

The Gambia's ICT market is relatively small, with four ISPs—state-owned Gamtel and privately-owned QuantumNet, Netpage, and Airtip[18]—and four mobile phone providers, Gamtel's subsidiary Gamcel, and privately-owned Qcell, Africell, and Comium.[19] All mobile providers offer 2G/3G data service.

The telecommunications sector is not well regulated, and like many other sectors, businesses must contend with inefficient bu eaucracies coupled with nepotistic and preferential practices conducted by government officials. op regime officials ften have working relationships with business entities and investors "across all sectors of the economy," according to local observers.[20] Registration for internet and mobile phone service providers is an onerous and expensive process with numerous requirements to fulfill. In addition, corruption among the authorities is rife [21]

Internet cafe operators must also contend with regulatory obstacles. For example, under an April 2013 directive, cybercafe owners are required to register with the regulatory agency for an operating license (in addition to a requisite business license) through an application that requires details of the ISP, the number of computers installed, and services provided.[22] Cybercafes must renew their licenses every year and pay annual renewal fees of USD 20 to the regulatory body or face closure.[23] In September 2013, the regulator issued further guidelines that dictated specific equirements on the physical layout of cybercafes and the signs that must be displayed.[24] Since the regulations came into effect, dozens of cafes have closed down, likely as a result of the economic obstacles imposed by the strict regulations as well as increasing mobile broadband access.[25]

Regulatory Bodies

The telecommunications sector is regulated under the Public Utilities Regulatory Authority Act 2001, which established the Public Utilities Regulatory Authority (PURA) in 2004 to regulate the activities

17 African Union, "AU Launches Internet Exchange Point in Gambia: "Contributing to a faster, secure and affordable internet in Africa," press release, July 17, 2014., http://bit.ly/1Mgh49T.

18 Access Gambia, "Information Technology in Gambia," accessed August 8, 2014, http://www.accessgambia.com/information/information-ict.html.

19 Henry Lancaster, *Gambia – Telecoms, Mobile and Broadband*, BuddeComm, May 26, 2015, http://bit.ly/1Mgii4Z.

20 Interviews by Freedom House consultant, April 2015.

21 For example, when Qcell, one of the leading GSM companies in country, was forced to suspend its mobile money service known as QPOWER in 2013, it reportedly gifted two new cars to Gambian President Yahya Jammeh for his birthday, which led to a subsequent resumption of the QPOWER service. Modou S. Joof, "QPOWER service is back," *Front Page International* (blog), June 14, 2013, http://bit.ly/1jQErQD.

22 Public Utilities Regulatory Authority (PURA), "Internet/Cyber Café Registration Form," accessed August 8, 2014, http://bit.ly/1hsvbjZ.

23 Modou S. Joof, "PURA tells internet cafes: register or stop operations," *Front Page International* (blog), May 15, 2013, http://bit.ly/1L1I2o7.

24 Yaya Bajo, "PURA sets guidelines for internet café operators," *FOROYAA Newspaper*, *All* Africa, September 19, 2013, http://bit.ly/1MgiXDv.

25 Interviews by Freedom House consultant, May 2016

of telecom service providers and other public utilities.[26] Consumer activists have described PURA as an ineffective regulator that seems more concerned about its image than the interests of consumers.[27] As it stands in 2016, PURA lacks the expertise, equipment, and enforcement power to carry out its mandate.[28] Furthermore, PURA is not independent, at least in its composition. The president appoints the governing board on the recommendation of the Minister of Finance and Economic Affairs.[29]

Limits on Content

Dozens of independent online news and opposition websites remained blocked in The Gambia, while popular communications platforms such as WhatsApp, Viber, and Skype were reportedly blocked beginning in August 2016. Observers believe the blocks may be a part of a larger effort to quash anti-government initiatives and sentiments from proliferating online in the lead up to December 2016 elections.

Blocking and Filtering

Over 20 webpages remained blocked in The Gambia during this report's coverage period,[30] many of which are news and opposition websites known for their criticism of the government,[31] such as *Gambia Echo*, *Hello Gambia*, *Jollof News*, *Gainako*, and *Freedom Newspaper*.[32] Most of the blocked outlets are based abroad and operated by exiled Gambian activists and journalists.

YouTube, Facebook, Twitter and international blog-hosting platforms were not restricted in late 2015 or early 2016. But communications platforms met with restrictions beginning in August 2016, outside of this report's coverage period. On August 17, WhatsApp was reportedly inaccessible for approximately 12 hours,[33] which local observers attributed to a message disseminated anonymously on the platform that warned of an imminent attack against the president. Activists also speculated that the block was a trial run for further restrictions as the government prepared for the elections period scheduled for December.[34] Later in August, users reported WhatsApp was inaccessible again along with several other communications apps, including Viber, IMO, and Skype.[35] Local users said the platforms were only available via cloud virtual private networks (VPNs) and other proxy servers used by tech-savvy Gambians to access blocked content from within the country.[36]

26 PURA, "Pura Act," accessed August 8, 2014, http://pura.gm/index.php?option=com_content&view=article&id=112&Itemid=137.

27 Interviews by Freedom House consultant, February 2014.

28 Interviews by Freedom House consultant, January 2014.

29 PURA, "Organizational Structure," accessed August 8, 2014, http://www.pura.gm/index.php?option=com_content&view=article&id=86&Itemid=70.

30 Interviews by Freedom House consultant, April 2014.

31 Baboucarr Ceesay, "Gambia: Government's internet phobia and censorship," Africa Review, March 29, 2014, http://bit.ly/1OnY5Pk.

32 Media Foundation for West Africa, "US-based online paper inaccessible from Gambia, deliberate blocking by government suspected."

33 Sanna Camara Twitter post, August 17, 2016, https://twitter.com/maimuhyai/status/766064229321437184

34 Samira Sawlani Twitter post, August 19, 2016, https://twitter.com/samirasawlani/status/766646802804244480

35 Muhammed S. Bah, "Are social networking applications blocked?" Foroyaa Newspaper, August 23, 2016, http://allafrica.com/stories/201608240945.html

36 "Blocking the VoIP services for national security reasons is illogical – Says Sam Phatey," Askani Senegambia, March 19, 2014, accessed September 29, 2014, http://bit.ly/1jQFyzX.

Internet tools and content are blocked without transparency or recourse in The Gambia. The government denies any involvement in the blocking of critical news websites; however, state control over the country's dominant telecommunications provider, Gamtel, gives the authorities the ability to restrict access to internet content. Experts believe that the country blocks specific in ernet protocol (IP) addresses and domain names at the level of the internet gateway.

Content Removal

The government requires websites to take down certain content, though the extent of content affected is not known. Progovernment and state-owned news outlets often receive directives to depict the government in a positive light.

Observers note a disconcerting trend of online content "disappearances," based on accounts from journalists and editors based in the country. A former reporter speaking anonymously said that he often received orders from government officials o take down select content from news websites, particularly "politically sensitive" content.[37] Editors have reported receiving threatening phone calls for their online content, while others have experienced "visits" from officials at their ffices or homes.[38] In general, stories that risk catching the attention of security officials a e likely to be removed, either through self-imposed post-publication censorship, or as a result of unofficial ta e-down orders from government officials. Consequentl , online journalists often express frustration at the level of restrictions on what they can and cannot publish.[39]

Content that is removed from a platform is sometimes accompanied by an apology or rejoinder that appears to be the result of pressure behind the scenes.[40] In April 2016, for example, a Facebook post by Ibrahim Ceesay, then-director of the National Youth Council, called on young people to take part in a peaceful protest. The post was removed, then replaced with another that condemned the initial appeal and admonished "young people to be law abiding and calm."[41] Ceesay was subsequently removed as director of the council. He later reported receiving death threats and fled the count y.

Media, Diversity, and Content Manipulation

Most critical news outlets are operated by exiled dissidents based abroad and blocked within the country. Economic sustainability for independent online media outlets is a challenge, since many businesses avoid advertising with critical outlets out of fear of government reprisals.[42] As a result, the online news and information landscape does not represent a diversity of political and social viewpoints, and newer initiatives to infuse diversity are failing due to a lack of financial sustainabilit .

The highly restrictive environment for bloggers and internet users also undermines the diversity of

37 Interviews by Freedom House consultant, April 2015.

38 Interviews by Freedom House consultant, April 2015.

39 Alieu Khan, "INTERVIEW: Journalist Saikou Ceesay talks work, Gambian media, President Jammeh, and more," November 29, 2015 http://whatson-gambia.com/exclusive/1024-interview-journalist-saikou-ceesay-talks-work-gambian-media-president-jammeh-and-more.html

40 "Since we are not all technically skilled, sometimes when we post critical information online, which in our context is incriminating, we simply delete. Sometimes the removal is accompanied by an apology or a rejoinder. This is how we survive, special circumstances present special approaches," said a local online journalist. Interviews by Freedom House consultant, 2015.

41 National Youth Council The Gambia, Facebook post, April 17, 2016, https://www.facebook.com/nycgambia/posts/1797384103824053

42 Interviews with Industry experts by Freedom House consultant, January 2016.

online content, as the small number of locally-based independent journalists and netizens working to push the boundaries of free expression from within the country is shrinking. The once-popular news blogs, *Front Page International* (FPI) and *Gambia Affairs*, were less active in 2016 compared to previous years.[43]

Furthermore, a climate of fear due to pressure from the authorities in the form of arbitrary arrests, extralegal harassment, and threats has led to a severe degree of self-censorship among journalists, both online and offline [44] Bloggers and online journalists based in the country typically post content anonymously, while many local activists either avoid posting critical content or remove it after posting to evade potential repercussions.

Comments by trolls in many online forums disproportionately distort the news and information landscape, though there is no concrete evidence that the authorities employ progovernment commentators to manipulate online content. In a new trend, the government has increased its efforts to coopt prominent anti-Jammeh activists, incentivizing them to support the regime through handsome gifts from the president himself.[45] Some activists in the diaspora have been offered the opportunity to return home after decades-long exile in exchange for progovernment support. In the past year, at least two former anti-Jammeh activists aligned themselves with the government, ostensibly after being offered high level government positions such as minister of foreign affairs,[46] or deputy representative to the United Nations.[47]

Digital Activism

Digital activism is emerging in The Gambia, though efforts are usually small and unsuccessful, mainly due to heavy-handed government repression against criticism and dissent. Most efforts are led by a growing diaspora community who are increasingly frustrated with Jammeh's repressive regime. In April 2016, unprecedented protests were inspired by the trending #GambiaRising and #JammehFact hashtags, which focused on human rights abuses committed since Jammeh took power in 1994.[48] Although the protests were quickly quashed by security personnel, the hashtags remained active through 2016.

Violations of User Rights

In July 2015, a radio journalist was detained for several months for allegedly sending pictures that incited hatred against the president via Facebook and WhatsApp, before escaping in April 2016; he was separately abducted and subject to torture prior to his arrest. A Facebook user was arrested for alleged-

43 Interviews with Editors by Freedom House, February 2016. Front Page International, website, https://frontpageinternational.wordpress.com/; Gambia Affairs, website, http://gambiaaffairs.com/

44 Buya Jammeh, "Gloomy days for Gambian journalists," Index on Censorship, January 20, 2014, http://bit.ly/1PjT2jN.

45 Mathew K Jallow, "The Gambia: Reconciliation, no; indemnifying, hell no," Gainako, May 6, 2015. http://gainako.com/the-gambia-reconciliation-no-indemnifying-hell-no/

46 State House: Mrs. Neneh MacDouall-Gaye, Minister of Foreign Affairs http://www.statehouse.gm/cv/neneh-macdouall-gaye-foreign-affairs_05012015.htm

47 *The Point*: Changes in diplomatic circles, May 18, 2015. http://thepoint.gm/africa/gambia/article/changes-in-diplomatic-circles

48 Demba Kandeh, "Pressure Mounts on Gambia's President Over Worsening Human Rights Situation," Global Voices (blog), April 23, 2016, https://globalvoices.org/2016/04/23/pressure-mounts-on-gambias-president-over-worsening-human-rights-situation/

ly wounding religious feeling in August 2015, and numerous activists associated with the April 2016 protests reported hacking and hijacking attacks on their social media accounts.

Legal Environment

The 1997 constitution guarantees freedom of speech and press freedom, though fundamental freedoms are severely restricted in practice. President Jammeh is known for his utter disregard for constitutional rights, stating publicly in March 2011 that he would "not compromise or sacrifice the peace, security, stability, dignity, and the well-being of Gambians for the sake of freedom of expression."[49]

A number of draconian laws further undermine freedom of expression, and in recent years, the government has successfully amended existing legislation to increase penalties for certain offenses. The criminal code, which already criminalizes defamation with a minimum prison sentence of one year plus heavy fines, was amended in April 2013 o penalize individuals for "giving false information to public servants" with up to fi e years in prison, up from six months.[50] Observers believe the increased penalty was an effort to intimidate journalists and whistleblowers from seeking legal recourse for the physical abuse they often experience at the hands of the authorities.[51]

Harsh legislation specifically ta geting ICTs was passed in July 2013 in the form of amendments to the 2009 Information and Communication Act (ICA). Under the new amendments, using the internet to criticize, impersonate, or spread false news about public officials is punishable by up o 15 years in prison, fines f up to GMD 3 million (about US$100,000), or both.[52] The government introduced the law in response to online activism and the growing influence f critical news outlets, particularly those overseas, according to the blocked news outlet *Gainako*.[53]

Prosecutions and Detentions for Online Activities

Arrests and prosecutions of online journalists and ICT users for their online activities are common in The Gambia, and users are often prosecuted on "false information" charges under the ICA 2009 as amended in 2013. As Gambians head to the polls in December 2016, observers worry that the government will be more aggressive on its clampdown on citizens who use social media and communications platforms to mobilize and criticize the government.

In July 2015, popular radio journalist Alagie Abdoulie Ceesay was arrested and charged with sedition for sending a picture that allegedly incited hatred against the president through private messages on Facebook and WhatsApp. Immediately prior to his arrest, he had been abducted for eleven days (see Intimidation and Violence). Ceesay, the managing director of independent radio station Taranga

49 Baboucarr Senghore, "President Jammeh meets with the Independent Press," *The Point*, March 17, 2011, http://bit.ly/1R19tQm.

50 Article 19, "The Gambia: ARTICLE 19 condemns new attacks on freedom of expression," statement, April 24, 2013, http://bit.ly/1R19vYn.

51 Article 19, "The Gambia: ARTICLE 19 condemns new attacks on freedom of expression," statement, April 24, 2013.

52 Demba Kandeh, "New Internet Law in The Gambia Puts Gag on Government Criticism," *Global Voices*, July 12 2013, http://bit.ly/1ZgKZIE.

53 "Gambia Government admits growing online media pressure; Pass drastic measures against Internet Activism," *Gainako*, July 4, 2013, http://gainako.com/?p=1176.

FM, spent over six months in state custody.[54] In April 2016, news reports said that Ceesay had escaped custody while receiving medical treatment at the country's main referral hospital in Banjul and was seeking exile in Senegal.[55] The authorities said that his case will proceed without him.[56]

Citizens were also subject to harsh penalties for violating the country's strict laws prohibiting blasphemy. In August 2015, Facebook user Alhagie Mam Seye was arrested for sharing a picture of the Prophet Mohamed on Facebook.[57] He was subsequently charged with "uttering words with intent to wound religious feelings" and released on bail after his lawyer said he was mentally unstable.[58]

Surveillance, Privacy, and Anonymity

Unchecked surveillance of ICTs is a grave concern in The Gambia. Article 138 of the 2009 Information and Communications Act gives sweeping powers to national security agencies and investigative authorities to monitor, intercept, and store communications in unspecified ci cumstances while also giving the regulator, PURA, the authority to "intrude [sic] communication for surveillance purposes," all without judicial oversight.[59] In addition, the law requires service providers to "implement the capability to allow authorized interception of communications." Article 141 also imposes onerous data retention requirements, obliging service providers to retain metadata for three years.

The government also places restrictions on anonymous communication through SIM card and local domain name registration requirements.[60] The latter is managed by the regulatory authority.[61] Africell, one of the largest GSM companies, recently introduced mobile payment services for users with registered SIM cards.[62]

Observers believe the government proactively monitors and intercepts citizens' communications, particularly the communications of activists and independent journalists whom the government perceives as a threat to national security.[63] Intercepted phone and email communications are often used as evidence in trials against government critics. However, the scope of the government's technical surveillance capabilities remains unknown.

In December 2015, the government unveiled plans to set up a new National Cyber Security Strategy that aims to establish a Computer Incidence Reporting Team to monitor cyber threats.[64] Details of the proposed strategy remain unclear, but preliminary documents indicate that it will regulate per-

54 Fatoumatta Camara, In Journalist Alhagie Ceesay's Case: Jammeh Busted; Runaway State Witnesses Say The Journalist Was Setup, Fatu Network, February 22, 2016. http://fatunetwork.com/2398-2/

55 https://jollofnews.com/2016/04/23/escaped-gambian-journalist-arrives-in-senegal/

56 Rohey Jadama, Gambia: 'Taranga FM MD's Case Will Proceed in His Absence', Says Justice Dada, 14 July 2014 All Africa http://allafrica.com/stories/201607140999.html

57 End Blasphemy Laws, "The week in "blasphemy" news #31," http://bit.ly/1OnOSYF; Amadou Jadama, "Judgement shelved in trial of man accused of publishing cartoon of Prophet Muhammad," *The Standard*, August 12, 2015, http://bit.ly/1QaT9ME.

58 Media Foundation for West Africa, "The Gambia: Man arrested, charged for sharing picture of Prophet Mohammed on Facebook," *Free Expression Violations, 2015, http://bit.ly/1P0Fwll*.

59 Information and Communications Act, 2009, art. 138, http://www.wipo.int/edocs/lexdocs/laws/en/gm/gm006en.pdf.

60 PURA, "SIM registration," accessed September 30, 2014, http://www.pura.gm/index.php?option=com_content&view=article&id=127&Itemid=131.

61 Information and Communications Act, art. 9, http://www.wipo.int/edocs/lexdocs/laws/en/gm/gm006en.pdf.

62 Adam Jobe, Africell launches 'free' mobile money service, The Point, February 12, 2016. http://thepoint.gm/africa/gambia/article/africell-launches-free-mobile-money-service

63 Freedom House Interviews, February 2014.

64 Lamin Darboe, "Building Security in ICT is Priority to Government – Says Finance Minister," Daily Observer, December 21, 2015, http://observer.gm/building-security-in-ict-is-priority-to-government-says-finance-minis er/

sonal data protection, electronic transactions, electronic records and signatures, and computer misuse and cybercrime,[65] all of which are currently regulated by Information Communication Act 2009 and provisions in the Criminal Procedure Act. Observers worry that the increased "securitization" of the internet will have negative repercussions on freedom of expression online.

Intimidation and Violence

Gambian journalists face a high degree of violence for independent and critical reporting and increasingly, for their online activities. Before radio journalist Alagie Abdoulie Ceesay was arrested in July 2015, he was abducted for 11 days and reportedly tortured, for unknown reasons at the time. He was arrested four days after his release in relation to content shared privately on WhatsApp and Facebook (see Prosecutions and Detentions for Online Activities).[66] In a separate incident, online journalist Ebrima Janko Ceesay was among those arrested during the April 2016 protests. Ceesay (no relation to Abdoulie Ceesay) was reportedly beaten and lost two teeth while in detention.[67]

As a result of the unsafe environment for media workers, bloggers and online journalists continued to seek exile alongside their traditional media counterparts in the past year.

Technical Attacks

There were no reports of opposition websites or critical online news outlets experiencing debilitating technical attacks during the coverage period, though numerous online journalists, bloggers, activists and users reported that their social media accounts had been hacked. Activists suspect that the government initiated the hackings as part of its effort to counter growing anti-government sentiment online.[68] At least one protest leader, Ibrahim Ceesay, said that his social media accounts and mobile phone numbers were compromised during the April 2016 protest. Ceesay said that hackers accessed his WhatsApp account and sent messages on his behalf.

65 Interview by Freedom House consultant, May 2016

66 Philip Obaji Jr., "Hunting Down Journalists in Gambia," The Daily Beast, March 14, 2016, http://www.thedailybeast.com/articles/2016/03/14/hunting-down-journalists-in-gambia.html

67 Musa Saidykhan, "Brave Gambian Journalist Who Lost 2 Teeth To Torture," Kibaro News, May 20, 2016, http://www.kaironews.com/brave-gambian-journalist-who-lost-2-teeth-to-torture/

68 Interviews with activists & bloggers by Freedom House consultant, February 2016.

Freedom House

Georgia

	2015	2016
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	7	8
Limits on Content (0-35)	6	6
Violations of User Rights (0-40)	11	11
TOTAL* (0-100)	**24**	**25**

* 0=most free, 100=least free

Population:	**3.7 million**
Internet Penetration 2015 (ITU):	**45 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2016 Status:	**Partly Free**

Key Developments: June 2015 – May 2016

- In a triumph for online privacy, the Georgian Constitutional Court reversed the State Security Service's powers to directly access users' telecommunications data in April 2016 (see **Surveillance, Privacy, Anonymity**).
- WordPress and YouTube were briefly bloc ed while the authorities attempted to restrict access to content hosted on the platforms (see **Blocking and filtering**).
- Internet user Sulkhan Tsuladze was detained for a month for a forum post describing a fictional attack on the US Am assador to Georgia which online activists said was intended as a joke (see **Prosecution and Detention for Online Activities**).

Introduction

The Georgian government rarely restricts access to content online, though two isolated blocking incidents involving WordPress and YouTube were documented during the coverage period of this report.

Internet access and usage continues to grow, particularly involving social networks. State bodies and several politicians have also increased their use of the internet and social media to share information with citizens and attract support. The government continues to integrate e-services into a unified governmental portal, though not all agencies are responsive when engaging with citizens online.

There are few indications of censorship or online content manipulation by the Georgian authorities or internet service providers (ISPs). Georgians continue to freely use social media tools to document and respond to significant political and social e ents. The advent of diverse interactive maps and platforms enables users to report matters in the public interest. The number of online campaigns launched by activists and civil society members has significantly inc eased over the past years. However, unreliable and politically biased content, including anti-Western propaganda, also proliferated online.

In recent years, legislative amendments and court decisions have gradually increased checks on the ability of authorities to conduct surveillance of citizens online. In 2016, the Constitutional Court ruled against the government's practice of accessing user metadata without oversight, further shoring up privacy online. However, leaked recordings of private conversations between public officials have raised concerns of unauthorized surveillance.

Obstacles to Access

The number of internet and mobile phone subscriptions in Georgia continues to grow, but high prices for services, inadequate infrastructure, and slow internet speeds remain obstacles, particularly for those in rural areas or with low incomes. The government has said it will address these challenges during the next few years, but has not outlined an exact strategy to overcome the digital divide.

Availability and Ease of Access

Internet access continued to grow during the reporting period. According to the International Telecommunication Union (ITU), 45 percent of the population had access to the internet in 2015, compared to 43 percent in 2013, and just 20 percent in 2009.[1] According to a countrywide survey conducted by the Caucasus Research Resource Centers (CRRC), 46 percent of the population accessed the internet on a daily basis in 2016,[2] and the most active internet users were located in the capital. Only 2 percent of Georgians are unfamiliar with the internet altogether.[3] There is a slight gender gap, as over 51 percent of men use the internet compared to 47 percent of women.[4]

1 International Telecommunication Union, "Percentage of individuals using the Internet,"2000-2015, http://bit.ly/1cblxxY.

2 Caucasus Research Resource Centers, "Survey on Public Policies,June 2016," accessed September 27, 2016, http://caucasusbarometer.org.

3 Caucasus Research Resource Centers, "Survey on Public Policies, June 2016." accessed September 27, 2016, http://caucasusbarometer.org.

4 International Telecommunication Union, "Percentage of individuals using the Internet, 2000-2014." http://bit.ly/1cblxxY.

ISPs offer DSL broadband, fibe -optic, HSPA/EVDO, WiMAX and Wi-Fi connections. Since 2015, 4G LTE internet access has been slowly made available for Georgian consumers.[5] The average cost for an internet connection is US$20 per month, though the lowest price for a faster 8 Mbps DSL connection is about US$25 per month.[6] There were approximately 631,000 fi ed-line broadband internet connections in 2015,[7] up from about 419,000 in 2012.

Mobile phone penetration is greater than that of the internet and has grown from 64 percent in 2009 to 129 percent in 2015.[8] Mobile phones significantly outnumber landlines, and eception is available throughout the country, including rural areas. The vast majority of households access the internet from a home computer or laptop (89 percent) rather than from personal mobile phones (43 percent).[9] The use of mobile devices to connect to the internet may be limited by high costs. However, some providers are offering new and somewhat less expensive services, including CDMA and EVDO technologies.

The government of Georgia lacks a comprehensive strategy outlining a clear and long-term vision for developing internet infrastructure throughout the country. In February 2014, Georgia's Innovation and Technology Agency was established in order to promote the use of innovation technologies in various fields and the comme cialization of innovative technology research and development. [10] Among other programs, it is tasked with ensuring broadband internet access to all citizens (at least 2,000 settlements) by the end of 2017.[11]

In July 2015, the Georgian government established the non-commercial legal entity Open Net to build broadband infrastructure. Reports said the project, costing about US$150 million, will be funded by the Cartu Foundation, set up by Georgian tycoon and former Prime Minister Bidzina Ivanishvili. The move came after a tender to major telecommunications companies to expand infrastructure failed, because it was seen as unprofitable. Civil society o ganizations expressed concern over the lack of transparency and inclusiveness of the project, noting that it was not based on a comprehensive assessment of the market, and could perpetuate lack of competition in the sector.[12]

Many restaurants, cafes, bars, cinemas, and other public places provide Wi-Fi access, allowing customers to use the internet on their personal devices. In 2013, as part of a plan to improve infrastructure for local self-governance, the State Services Development Agency began developing community centers where local citizens can access the internet and online resources including Skype, bank services, telecommunication services, and electronic services developed by the state.[13] As of May 2016, 33 centers were operating in different regions and districts throughout the country.

5 "2015 – the year full of new developments" *ZETI.GE.* [in Georgian] January 12, 2015, http://zeti.ge/menu_id/23/id/755/.

6 Comparative data from two major ISP's prices (SilkNet and Magticom).

7 Georgian National Communication Commission, "Annual Report 2015,"[in Georgian] June 2016, http://gncc.ge/uploads/other/1/1976.pdf.

8 International Telecommunication Union,"Mobile-cellular telephone subscriptions, 2000-2015," http://bit.ly/1cblxxY.

9 Caucasus Research Resource Centers, "Caucasus Barometer 2015 Georgia," accessed September 27, 2016, http://www.crrccenters.org/caucasusbarometer/.

10 Official ebsite of Georgia's Innovation and Technology Agency, accessed February 15, 2016 http://gita.gov.ge/en/agency.

11 Ministry of Economy and Sustainable Development of Georgia, "High Quality Internet to be Accessible to Every Region in Georgia" January 15, 2015, accessed February 15, 2016, http://bit.ly/1EH2msg.

12 Ucha Seturi,"Problems of the Cancelled Governmental Contest Broadband Internet to Every Citizen and Recommendations of IDFI," Institute for Development of Freedom of Information, July 21, 2015, http://bit.ly/1LwMf5D.

13 For more information, see: State Services Development Agency, "Community Center," [in Georgian] http://sda.gov.ge/?page_id=5555.

Restrictions on Connectivity

The Georgian government does not place any restrictions on connectivity, and the backbone internet infrastructure is owned and operated by private companies. Despite expanding internet access, many users complain about the quality of connections and suffer from frequent outages. Users submitted 36 complaints about the poor level of telecommunication service in 2015, according to the Georgian National Communication Commission.[14]

The telecommunications infrastructure in Georgia is still weak, and users may experience disconnections from the international internet up to two or three times per month for a few minutes at a time, during which time they can access only Georgian websites. Connection speeds are generally faster for accessing content hosted in Georgia. Many factors undermine the connection to the international backbone. The major underground fibe -optic cable is often threatened by landslides, heavy rain, or construction work along the roads. In previous years, infrastructural problems led to country-wide internet disruptions, though no such outages were reported in 2015-2016.

ICT Market

According to the Law of Georgia on Electronic Communications, telecommunications companies must be licensed before offering services. There are currently more than 130 entities registered as ISPs in Georgia, 10 of which are large networks of governmental services or corporations that are closed to the public and serve only their own employees or branches.[15] Most ISPs are privately owned. Two ISPs controlled more than two-thirds of the market as of mid-2016: SilkNet with a 41 percent market share, and Caucasus Online, with 27 percent.[16] Consequently, competition is minimal.[17] Three ISPs—Geocell, Magticom and Mobitel—are also mobile operators. The mobile internet market is also dominated by two main providers, Magticom and Geocell.[18]

The Georgian internet market is expected to undergo significant changes, as Magni com is set to purchase the retail segment of Caucasus Online by the end of 2016.[19] Experts do not anticipate any changes to the price of service.

Regulatory Bodies

The Georgian National Communication Commission (GNCC) is the main media and communications regulatory body and is also responsible for regulating online media, although there have yet to be many test cases regarding the latter. The GNCC mostly deals with mobile operators, as well as tele-

14 Georgian National Communication Commission, "Annual Report 2015."

15 List of the internet service providers released by Georgian National Communication Commission, "Internet Provaiderebi," http://bit.ly/1Tw9Ndl.

16 However, the situation changed after the coverage period in August, 2016, when Magticom gained 26 percent of the market, while Silknet controlled 41 percent of the market.
Georgian National Communication Commission: Analytical Portal, accessed February 15, 2016, http://analytics.gncc.ge/.

17 Institute for Development of Freedom of Information, "Internet Freedom in Georgia – Report N5," December 10, 2015, http://bit.ly/1XYIrkp.

18 As of December, 2015, Magticom possessed 39 percent of subscribers, which was followed by Geocell with 38 percent. The share of the third company, Mobitel accounted for 17 percent of this market: Georgian National Communication Commission, Analytical Portal, http://analytics.gncc.ge/.

19 Caucasus Online, "Joint Statement of Caucasus Online LLC. and MagtiCom," May 31, 2016, http://www.co.ge/en/news/240/.

vision and radio broadcasting licenses. There is no significant diffe ence between GNCC procedures for handling traditional media and those pertinent to telecommunications and internet issues.

Criticism surrounds the commission's alleged lack of transparency and independence. In order to increase the legitimacy of GNCC, new rules for the nomination of candidates and the selection of the Head of Commission came into force on October 27, 2013. A new chairman of the agency was elected by the commissioners themselves instead of the president of Georgia in May 2014. Despite this positive development, the revelation that an advisor to the new chairman was also employed by the Ministry of Internal Affairs raised speculation that the central government was attempting to interfere in the work of the regulator and collect data on its activities.[20] However, civil society representatives have confi med that the agency is gradually becoming more open to engagement with and monitoring by various civil society stakeholders.[21]

Limits on Content

Though censorship online remains rare in Georgia, the government briefly blocked access to WordPress and YouTube in two separate incidents within the coverage period. Nevertheless, web content is not subject to systematic manipulation by government agencies. On the contrary, online content is becoming quite diverse and internet users are increasingly using social media tools to organize and disseminate information about matters of public interest. The government of Georgia is increasingly engaging with citizens in policy-making discussions by establishing online communication platforms.

Blocking and Filtering

Georgian users can freely visit any website around the world, upload or download any content, establish their own website, and contact other users via forums, social-networking sites, and instant messaging applications. YouTube, Facebook, and international blog-hosting services are freely available.

An isolated incident of government-initiated blocking occurred in November 2015, when the State Security Service blocked the entire WordPress platform for a short period in an attempt to restrict access to a website hosted by WordPress which was disseminating videos by a pro-Islamic State group.[22] Activists contacted the administrators of WordPress.com through Twitter to resolve the issue and the company corresponded with the government. All websites hosted by WordPress were subsequently unblocked apart from the page disseminating the videos.

In a separate incident, YouTube was blocked twice by authorities following the release of sex videos depicting Georgian politicians. The fi st incident lasted for 20 minutes on March 11, 2016, and affected only Caucasus Online users. Three days later, YouTube was inaccessible again for about an hour for users of Caucasus Online and Silknet.

Aside from these isolated incidents, government blocking and fil ering is not a major hindrance to internet freedom in Georgia. There are no blacklists of websites that should be blocked, and no laws

20 Transpareny International Georgia, "Security Office s ('ODRs') - existing malpractice," October 6, 2014, http://www.transparency.ge/en/node/4693.

21 Interview with Levan Avalishvili, Board Chairman of Institute for Development of Freedom of Information, October 10, 2016.

22 "Georgia Blocks Access to Pro-Islamic State Websites," *Civil.Ge,* November 24, 2015, http://bit.ly/1KBLYPW.

that specifically go ern the internet, require online censorship, or ban content such as pornography or violent material. Though legal regulations, particularly those involving copyright or criminal law, are considered to apply to internet activities, they have not been exploited to impose significant content restrictions. However, in December 2015, some representatives of the government announced their intention to introduce "proper" regulations of online casinos.[23]

Content Removal

During the coverage period of this report, observers reported no cases of content removal directed at individuals or online media representatives were observed. Georgian laws protect users against intermediary liability, with the Law on Freedom of Speech (2004) stating that no entity will be held responsible for defamatory content generated by unknown or anonymous individuals.[24] To date, intermediary liability and forced removal of online content have not been significant impediments o online freedoms in Georgia. Websites hosting pirated material are available, but not widely visited.

Media, Diversity, and Content Manipulation

The online media environment in Georgia is becoming increasingly diverse, and content on a wide range of topics is available. However, a recent Transparency International report indicates that a number of online media outlets, some of which demonstrate bias and are affilia ed with political parties, coordinate informally to disseminate news.[25] These groups effectively dominate the online media landscape, making it difficult for smaller outlets o attract advertising revenue. The Georgian government funds some of these outlets through contracts.[26] Some have links to Russia, and have been known to push an anti-Western agenda.[27]

While there is no systematic or pervasive government manipulation of online content, Georgian internet users self-censor to some extent. Representatives of particular professions sometimes prefer to abstain from expressing themselves freely on social networks. For instance, civil servants in some cases may exhibit self-censorship online due to fear of reprisals from higher officials. In Februa y 2016, a former civil servant was allegedly forced to submit a resignation letter after he used his Facebook account to criticize the government.[28]

Inadequate revenues sources, combined with a lack of technological knowledge, hamper the expansion of traditional media outlets to the internet. At present, most online media outlets face difficulty in attracting advertisers, diversifying content, obtaining multimedia skills, and competing with traditional media. The private sector limits online advertising based on the comparatively small audience.

Even though the Georgian blogosphere has grown impressively, there are few bloggers who create content that has an impact on the political agenda, or who spark widespread discussion online. Minorities and vulnerable groups are represented online through a small number of forums and blogs.

23 "Kvirikashvili: Online Casinos Without Regulations are Very Harmful," *Tabula.Ge,* [in Georgian] December 29, 2015. http://bit.ly/1OorUen.

24 Faig Alizada, "WILMAP: Georgia," The Center for Internet and Society, Stanford University, http://stanford.io/1FIxwCU.

25 Transparency International Georgia, "Who Owns Georgia's Media," November 19. 2015, http://bit.ly/1oZeqkJ.

26 Transparency International Georgia, "Who Owns Georgia's Media," November 19. 2015, http://bit.ly/1oZeqkJ.

27 Nata Dzvelishvili & Tazo Kupreishvili, "Russian Influence on Geo gian NGOs and Media," *Damoukidebloba.Com*, July 22, 2015, http://bit.ly/1L46V61.

28 Reported on Facebook: [Georgian] http://on.fb.me/1Qanygt.

During the last three years, LGBTI (lesbian, gay, bisexual, transgender, and intersex) activists have started to use online tools for coordination, distributing information, and protesting discrimination in the public sphere. Additionally, online media outlets, non-governmental organizations (NGOs), and some public institutions have started using digital tools to disseminate information.

The majority of internet users (75 percent) report that they connect to the internet to check social networks. Other activities frequently carried out by Georgian internet users include searching for news (55 percent), and sending or receiving email (23).[29] Twenty-six percent of people consider the internet as one of their main sources of information.[30] Facebook is the most popular website, with bloggers and journalists increasingly using it to share or promote their content, and engage readers on current events. Civil society activists and others also use it as a tool for discussion about political and social developments.

State bodies have also become increasingly active online. For example, departments in the Ministry of Justice, the Ministry of Finance's unit for Tax Inspection, and others have developed online platforms that allow citizens to register and receive services, apply for identification ca ds, or file tax documentation. Since September 2013, more than 70 e-services have been integrated in a unified governmental portal, My.gov.ge. Citizens can also use it to make requests for public information about the government budget and expenditure. Several central government agencies have introduced discussion platforms where citizens can express their views regarding various policy issues or use social networks to engage their constituencies directly. For example, the Govern From Home project helped local government to livestream official meetings, giving citizens the oppo tunity to participate via the internet.[31]

Most importantly, in June, 2015, the government of Georgia announced an upcoming online petitions platform allowing citizens to submit proposals.[32] In mid-2016 it had yet to be launched.

Digital Activism

Political and civil society groups post calls for action on Facebook and use social media to communicate with their supporters. Though most forms of online activism lack significant ffline im act, the influence f such activities is gradually increasing. The most successful example of the reporting period was the "Beka is not a criminal" campaign in support of Beka Tsikarishvili, who faced up to fourteen years imprisonment for possessing 65 grams of marijuana. The extensive online campaign included a viral video recorded by Tsikarishvili in which he criticized Georgia's drug policy, as well as an online petition protesting against strict punishments for possessing marijuana. Demonstrations in support of Tsikarishvili that were held in several large cities were organized via social networks. On October 24, 2015, the Constitutional Court ruled that imprisonment for possession of up to 70 grams of marijuana is unconstitutional.

29 Caucasus Research Resource Center, "Survey on Public Policies 2015," accessed February 15, 2016, http://caucasusbarometer.org.

30 Caucasus Research Resource Center, "NDI: Public attitudes in Georgia, June 2016," accessed October 17, 2016, http://caucasusbarometer.org.

31 Municipality of Ozurgeti, "Sakrebulo answered citizens' questions," [in Georgian] April 11, 2015. http://ozurgeti.org.ge/?p=7988.

32 Government of Georgia, "An Electronic Petition Portal is to be Launched." June 3, 2015, http://bit.ly/1TumRzD.

Violations of User Rights

Over the past couple of years, the government has progressively passed laws bringing transparency and accountability to its surveillance practices, and the authorities now require oversight to access user telecommunications data. Despite this positive progress, concerns about government surveillance continue to linger following leaks of private conversations between public figures. Users remain free to express themselves online without fear of retaliatory violence or harassment, though the passage of a new law criminalizing public calls for violent actions has sparked concerns about a possible chilling effect on free speech online.

Legal Environment

Civil rights, including the right to access information and freedom of expression, are guaranteed by the Georgian constitution and are generally respected in practice.[33] The Law on Freedom of Speech and Expression makes it clear that other "generally accepted rights" related to freedom of expression are also protected even if they are not specifically mentioned [34] Furthermore, Article 20 of the constitution and Article 8 of the Law of Georgia on Electronic Communications include privacy guarantees for users and their information, though the law allows privacy rights to be restricted by the courts or other legislation.[35] Online activities—mainly cases of alleged defamation, which was decriminalized in 2004[36]— can be prosecuted under the Law on Freedom of Speech and Expression and the law on Electronic Communication. The unlawful use or dissemination of personal data online resulting in "considerable damage" is illegal under the criminal code, with penalties of up to four years in prison.[37]

In June 2015, amendments to the Criminal Code criminalized "public calls to violent actions" aimed at "causing discord between religious, racial, ethnic, social, linguistic or other groups," punishable by fines and community se vice. Repeated offences resulting in injury or death are punishable by up to 5 years in prison.[38] Despite the narrow framing of the law, human rights defenders have claimed that its provisions could be selectively applied to target legitimate expression online.

Lawmakers attempted to introduce a blasphemy law that would have imposed fines on insults o religious feelings. However, the controversial bill was withdrawn in February 2016.[39]

Prosecutions and Detentions for Online Activities

Georgian citizens are generally free to express themselves online without fear of legal sanction. The

33 The Constitution of Georgia, 1995, [in English] http://bit.ly/1L4F5nN.

34 Article 19, "Guide to the Law of Georgia on Freedom of Speech and Expression" (London: Article 19, April 2005) http://bit.ly/1KMt5WJ.
This law offers protections like absolute freedom of opinion, political speech and debates, obtaining, receipt, creation, keeping, processing and disseminating of any kind of information and ideas. The law specifically mentions that it is applicable o the internet as it defines "media as print or elect onic means of mass communication, including the Internet."

35 The law is available in English on the Georgian National Communications Commission website at: "Legal Acts," http://bit.ly/1OH6yhO.

36 Under the Law, the burden of proving that information is incorrect lies with the plaintiff. It also draws a distinction between defamation of a private person and defamation of a public person, setting stricter requirements for proving the defendant's guilt in the latter case.

37 Legislative Herald of Georgia, "The Criminal Code of Georgia," [in Georgian] http://bit.ly/1VADDwp.

38 Legislative Herald of Georgia, "The Criminal Code of Georgia," [in Georgian] http://bit.ly/1VADDwp.

39 "Bill Against 'Insult of Religious Feelings' Dropped," *Civil.Ge,* February 15, 2016, http://civil.ge/eng/article.php?id=28985.

authorities periodically investigate internet users who threaten violence online, and civil society groups say their response can be disproportionate.

In April 2016, the Tbilisi City Court placed internet user Sulkhan Tsuladze in pre-trial detention for a month after he predicted a fictional attack on the US Am assador to Georgia on the Georgian internet forum, Forum.ge. Tsuladze was accused of threatening to commit an assault on a person enjoying international protection. Human rights organizations criticized the detention as unjustified, arguing that Tsuladze is known for provocative speech and that the post was intended as a joke.[40] He was released on bail and court hearings were pending in mid-2016.

An investigation was also launched after Shota Aphkhaidze and Lago Lado Sadghobelashvili, both members of far-right organizations, posted calls for violence targeting the US embassy and followers of opposition party United National Movement (UNM) on Facebook.[41]

Surveillance, Privacy, and Anonymity

In a triumph for privacy online, the Constitutional Court ruled in April 2016 against the Georgian security agency's unrestricted access to telecommunications and internet data. The Public Defender, in addition to a number of NGOs, successfully petitioned the court, arguing that the agency's use of black boxes to access data in real time, as well as requirements that companies retain user metadata for two years, violated Georgian citizens' right to privacy as enshrined in the Constitution.[42] The ruling must be implemented by March 2017. [43]

The decision of the Constitutional Court follows several legislative amendments restricting the government's surveillance powers. In August 2014, the parliament passed a package of legislative amendments that increased oversight mechanisms for government surveillance practices.[44] Law enforcement agencies are now required to present higher standards of justification o obtain a court warrant for surveillance, and limit requests to investigations involving national security, or to prevent disorder and crime. Subsequent amendments in November 2014 introduced a "two-key system" to protect personal data, whereby the Ministry of Foreign Affairs must seek permission from the Office of the Personal Data Protection Inspector, in addition to obtaining a court order, before it can access telecommunications data held by companies. The Supreme Court of Georgia proactively publishes surveillance data annually. The latest data show that the number of motions to request wiretaps made have decreased.[45]

Despite these positive developments, recordings of private, politically sensitive conversations leaked online revived public concerns over illegal eavesdropping in 2015. The exchanges took place on Viber, an instant messaging and VoIP application, between Mikheil Saakashvili, ex-president of Geor-

40 Georgian Young Lawyers' Association, "GYLA Responds to Pre-trial Detention of Sulkhan Tsuladze," April 22, 2016, http://bit.ly/1YP8JBK.

41 Institute for Development of Freedom of Information, "Internet Freedom in Georgia – Report N5," December 10, 2015, http://bit.ly/1XYIrkp.

42 Public Defender of Georgia, "Constitutional Claim regarding Georgian Law 'On Electronic Communications'," February 2, 2014, http://bit.ly/1x7JpZj.

43 "Court Rules Georgia's Surveillance Regulation Unconstitutional," *Civil.ge*, April 14, 2016, http://civil.ge/eng/article.php?id=29102.

44 "Georgia Introduces Stricter Regulation of Secret Surveillance," *Democracy & Freedom Watch,* August 5, 2014, http://bit.ly/1ow5Bws.

45 Institute for Development of Freedom of Information, "Secret Surveillance in Georgia: 2015-2016," April 7, 2016. https://idfi.ge/en/regulating-secret-surveillance-in-georgia.

gia and former governor of Odessa in Ukraine, Nika Gvaramia, director of Rustavi 2 TV broadcaster, and members of the political opposition. The recording was published by a murky website called "Ukrainian WikiLeaks," which is hosted and registered in Russia.[46] An investigation into the unauthorized recording was launched by the State Security Service,[47] and the Office f the Personal Data Protection Inspector.[48]

On November 1, 2014, the mandate of the Personal Data Protection Inspector was extended to cover the private sector. The office is authorized o check the legality of any data processing by private organizations, either on its own initiative or in response to a citizen's application. Inspectors can impose measures provided for by the law for violations, including fines [49] The office s latest report identified major challenges and deep- ooted systematic problems undermining personal data protection including public or private organizations processing large amounts of data by without proper legal grounds; the illegal disclosure of personal information to other states or international organizations; and failure to limit the use of data for direct marketing campaigns.[50] According to the Personal Data Protection Inspector, the Ministry of Internal Affairs and private companies violated data protection rules on six separate occasions in 2015.[51]

There are no restrictions on the use of anonymizing or encryption tools online. However, individuals are required to register when buying a SIM card. ISPs and mobile phone companies are also obliged to deliver statistical data on user activities concerning site visits, traffic, and other opics when asked by the government. Cybercafes are not obliged to comply with government monitoring, as they do not register or otherwise gather data about customers.

Intimidation and Violence

During the coverage period of this report, no cases of extralegal intimidation or physical violence directed at individuals for their online activities were reported in Georgia. Furthermore, there were no reported examples of women, LGBTI individuals, or members of ethnic minority populations being harassed or threatened specifically because f their use of ICTs.

Technical Attacks

Cyberattacks against opposition websites have not been a significant issue in Geo gia, with the latest major attacks occurring in 2008 and 2009 in relation to political tensions with Russia. In 2012, the Data Exchange Agency started monitoring Georgian websites for the presence of malicious code, hacking, or other suspicious activities, publishing the results regularly on their website,[52] and on their Facebook page.[53] The Agency's "Safe Internet - Check My IP" service examines the security of the

46 "Wiretapped Recordings of Saakashvili Discussing Rustavi 2 TV Leaked," *Civil.Ge,* October 30, 2015, http://bit.ly/1RDqIra.

47 "State Security Service Says it Probes into Leaked Saakashvili Wiretapped Recordings," *Civil.Ge,* October 30, 2015, http://bit.ly/1T2wxDm.

48 "Kaldani about the Examination of the Existence of Court Permission," *Netgazeti.Ge,* October 30, 2015. http://www.netgazeti.ge/GE/105/News/51703/.

49 Office f the Personal Data Protection, "The Mandate Of The Personal Data Protection Inspector Extends to The Private Sector," news release, assessed February 20, 2016, http://bit.ly/1DZRPEM.

50 Ibid

51 Office f the Personal Data Protection, Annual Report 2015, [in Georgian] http://personaldata.ge/ge/publications/annual-report.

52 Data Exchange Agency, homepage, http://dea.gov.ge.

53 CERT, Facebook page, https://www.facebook.com/certgovge.

IP address on users' computers, informing them of the nature of any viruses detected. Nevertheless, government websites remain subject to occasional hacking incidents. Within the coverage period, the official ebsites of the Ministry of Agriculture, the State Ministry for Diaspora Issues and the State Ministry for Reconciliation and Civic Equality were hacked.[54]

54 Institute for Development of Freedom of Information, "Internet Freedom in Georgia – Report N5," December 10, 2015, http://bit.ly/1XYIrkp.

Freedom House

Germany

	2015	2016
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	4	3
Limits on Content (0-35)	5	5
Violations of User Rights (0-40)	9	11
TOTAL* (0-100)	**18**	**19**

* 0=most free, 100=least free

Population:	**81.4 million**
Internet Penetration 2015 (ITU):	**88 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2016 Status:	**Free**

Key Developments: June 2015 – May 2016

- The proposal by Germany's telecoms regulator to allow former state-owned monopoly and market leader Deutsche Telekom exclusive use of vectoring technology to develop broadband internet access sparked fears of a slow re-monopolization of the ICT market (see **Regulatory Bodies**).
- In July 2015, the federal prosecutor's office notified the ebsite Netzpolitik.org that two of its journalists were under investigation for treason, for publishing articles containing classified sta e information. While quickly dropped, the case drew widespread public criticism (see **Prosecutions and Detentions for Online Activities**).
- In October 2015, the federal parliament adopted new legislation requiring telecommunications companies to retain certain data for up to ten weeks, despite fie ce protests from data protection officials and the Eu opean Court of Justice's rejection of a similar EU directive (see **Surveillance, Privacy, and Anonymity**).

Introduction

Germany's internet freedom environment declined slightly this year, as a short-lived treason investigation against two online journalists sparked widespread criticism and new legislation concerning data retention raised fresh privacy concerns.

Media and civil society frequently and openly discuss the state of internet freedom in Germany, especially given the prominence of internet regulation issues in widely read online news publications. There is consensus that internet freedoms are essential for an open and democratic society, and politicians, both from the governing parties and the opposition, usually act accordingly.

At the same time, some issues came under renewed pressure during the reporting period. In the course of the European refugee crisis, social media companies were criticized for not doing enough to subdue hate speech on their platforms. In the case of Facebook, this even led to an official criminal investigation against one of its executives. Subsequently, the companies vowed to change their removal practices in Germany, while also citing concerns regarding the freedom of speech.

Another topic of debate was the future of net neutrality in Germany and the European Union, as European legislation prompted concerns about potential loopholes. Germany's liability regime for open access providers also remained a risky obstacle for cafes and other businesses wanting to establish free wireless networks for customers. Although recent amendments have sought to address these liability issues, remaining burdens for providers continued to draw criticism.

In the wake of the European Court of Justice's dismissal of the EU Data Retention Directive in the spring of 2014, law enforcement representatives found support from the governing coalition in their call for new national legislation to enact data retention in Germany. In October 2015, a new law introduced requirements for telecommunications companies to retain data for up to ten weeks, such as the IP addresses of users and the date and time of connections, and for all data to be stored on servers located in Germany. No less than four constitutional complaints were subsequently filed against the cont oversial legislation. Moreover, despite an ongoing parliamentary inquiry, the scandal triggered by Edward Snowden's revelations in 2013 concerning the activity of the NSA and German intelligence services has still not been adequately assessed.

Obstacles to Access

Internet access is high in Germany, and there are few inhibiting obstacles. However, the country still lags behind other European countries in terms of broadband development, despite new and considerably increased funding promised by the federal government. While competition in the ICT market has continued to increase, the regulator's proposal to grant market leader Deutsche Telekom exclusive use of vectoring technologies to expand broadband access sparked fears of a partial re-monopolization of the market.

Availability and Ease of Access

Germany's network infrastructure for information and communication technologies (ICTs) is well

developed, and 88 percent of the population in Germany has private internet access.[1] Together with the number of mobile-only internet users, this has resulted in an overall internet penetration rate of 90 percent, according to Eurostat findings, which is se en percentage points above the European Union (EU) average.[2] Similarly, data compiled by the International Telecommunications Union (ITU) placed the internet penetration rate at 87 percent by the end of 2015.[3] According to a different survey, private internet usage increased from 77 percent to 78 percent, over the past year.[4]

The most widely used mode of access is still DSL, with 23.6 million connections in 2015. However, cable internet connections are becoming more widespread, with 7.2 million connections in 2015, compared to only 6.3 million in 2014.[5] Connections with more than 50 Mbps are available for 68.7 percent of households.[6] According to Akamai, the average connection speed was 12.9 Mbps by the end of 2015.[7] After announcing a roadmap to provide every household in Germany with internet access speeds of at least 50 Mbps by 2018,[8] the federal government presented a policy directive in October 2015 with a projected budget of 2.7 billion Euros.[9] The fi st communes started to request the subsidies in December 2015.[10] However, many businesses in Germany continue to struggle with slow connections.[11]

Mobile phone penetration in Germany is nearly universal, with a penetration rate of 139 percent.[12] In 2015, internet access via mobile devices further increased: people in Germany regularly accessed the internet via UMTS or LTE with 74.3 million devices, compared to only 52.6 million devices the previous year.[13] The total data volume increased from 395 million GB in 2014 to 591 million GB in 2015.[14] According to the Federal Ministry of Economics and Technology, Germany is ranked eighth internationally in terms of mobile internet access.[15] In February 2016, 51 million people in Germany used a smartphone.[16] At the end of 2015, LTE connections were available to 90 percent of all Telekom customers, 84 percent of Vodafone customers, and 75 percent of all Teléfonica Germany customers.[17]

1 Statistisches Bundesamt, 2015, http://bit.ly/1nZmCyY.

2 Eurostat, "Broadband and Connectivity – Households," April 7, 2016, http://bit.ly/1rCjmu7.

3 International Telecommunication Union, "Percentage of Individuals Using the Internet 2000-2015," accessed October 8, 2016, http://bit.ly/1cblxxY.

4 Initiative D21, Digital Index 2015, p. 13, http://bit.ly/1QTRejg.

5 Bundesnetzagentur, Jahresbericht [Annual report 2015], p. 50, May 1, 2016, http://bit.ly/1RWbKe7.

6 Stefan Krempl, "Bundesregierung beschließt Förderprogramm zum Breitbandausbau" [Federal government decides on development plan for broadband internet], heise.de, October 21, 2015, http://bit.ly/2dAnElb.

7 Akamai, State of the Internet, 2015 Q4 Report, http://akamai.me/2b5MgzU.

8 Thomas Heuzeroth, "Industrie investiert Milliarden in Breitbandausbau" [Industry invests billions in broadband development], welt.de, October 7, 2014, http://bit.ly/1P81UbX.

9 Stefan Krempl, "Bundesregierung beschließt Förderprogramm zum Breitbandausbau" [Federal government decides on development plan for broadband internet], heise.de, October 21, 2015, http://bit.ly/2dAnElb.

10 "Bundesregierung vergibt erste Fördergelder für Breitbandausbau" [Federal government awards fi st subsidies for broadband development], Heise.de, December 14, 2015, http://bit.ly/2d3zU9J.

11 Christine Schultze, "Viele Firmen kämpfen auch 2016 mit Breitband-Lücken" [Many businesses continue to struggle with broadband gaps in 2016], heise.de, January 2, 2016, http://bit.ly/2dARdTG.

12 Bundesnetzagentur, Jahresbericht [Annual Report 2015], p. 58, May 1, 2016, http://bit.ly/1RWbKe7.

13 Bundesnetzagentur, Jahresbericht [Annual Report 2015], p. 58, May 1, 2016, http://bit.ly/1RWbKe7.

14 Bundesnetzagentur, Jahresbericht [Annual Report 2015], p. 58, May 1, 2016, http://bit.ly/1RWbKe7.

15 Bundesministerium für Wirtschaft und Technologie [Federal Ministry of Economics and Technology], "Monitoring-Report Wirtschaft DIGITAL 2015", December 2015, p. 61, http://bit.ly/29vsISD.

16 Timm Lutter, "Umsatz mit Smartphones knackt 10-Milliarden-Marke" [Smart phone revenue reaches 10 billion mark], bitkom.org, February 16, 2016, http://bit.ly/1TlHVZj.

17 Bundesnetzagentur, Jahresbericht [Annual Report 2015], p. 60, May 1, 2016, http://bit.ly/1RWbKe7.

There is still a gender gap when it comes to accessing the internet in Germany. While 87 percent of men used the internet every day or almost every day in 2015, only 82 percent of women did.[18] Daily or almost daily internet usage in the 16-24 and 25-44 age groups were 95 and 93 percent, respectively. In the over 65 age group, frequent usage is now at 67 percent.[19]

Differences in internet usage based on formal education have not changed significantly o er the past few years. The gap between people with low and high levels of formal education is still noteworthy.[20] A comparison of net household incomes also confi ms this gap. Households with less than EUR 1,000 (USD $1,100) net income per month have a 51.7 percent penetration rate, whereas those with more than EUR 3,000 (USD $3,300) net income per month have a penetration rate of 94.3 percent.[21] Furthermore, slight differences in internet usage exist between Germany's western region (79 percent) and the eastern region (71 percent), which was formerly part of the communist German Democratic Republic; this gap has remained over the past year.[22] The gap between the urban states Hamburg, Berlin, and Bremen, and the rural states with the smallest internet penetration rate such as Saxony-Anhalt or Mecklenburg-Western Pomerania, is still between 10 to 14 percent.[23]

Telecommunication services have become slightly less expensive, decreasing by about 1.6 percent.[24] Available figu es indicate that prices for flat ra e broadband internet still range from EUR 16 to 30 (US$18 to $33) which is relatively affordable compared to an average income per household of EUR 4,101 (US$4,500).[25] Nevertheless, stark differences in internet usage by levels of income demonstrate how prices continue to be a barrier for people with low incomes and the unemployed. Although the Federal Court of Justice ruled that access to the internet is fundamental for everyday life, costs for internet access are still not adequately reflec ed in basic social benefits [26]

Restrictions on Connectivity

The German government does not impose restrictions on ICT connectivity. Germany's telecommunications infrastructure is largely decentralized. There are more than one hundred backbone providers in the country.[27] Privatized in 1995, the former state-owned Deutsche Telekom remains the only company that acts as both a backbone provider and an ISP. However, the German state owns less than a third of its shares, which crucially limits its control.[28] There are a number of connections in and out of Germany, the most important being the DE-CIX, which is located in Frankfurt. It is privately operated by eco, the association of the German Internet Industry.[29]

18 Statistisches Bundesamt, "IT-Nutzung nach Geschlecht 2015" [IT usage according to gender 2015], http://bit.ly/29vsISD.

19 Statistisches Bundesamt, "IT-Nutzung nach Alter 2015" [IT usage according to age 2015], http://bit.ly/1E0tpKO.

20 Initiative D21, Digital Index 2015, p. 59, http://bit.ly/2dObZQn.

21 Initiative D21, Digital Index 2015, p. 59, http://bit.ly/2dObZQn.

22 Initiative D21, Digital Index 2015, p. 56, http://bit.ly/2dObZQn.

23 Initiative D21, Digital Index 2015, p. 56, http://bit.ly/2dObZQn.

24 Statistisches Bundesamt, "Statistisches Jahrbuch. Deutschland und Internationales" [Statistical Yearbook], 2014, p. 400, http://bit.ly/1jCRrJu.

25 Destatis.de, "Einkommen, Einnahmen & Ausgaben" [Income, revenue & expenses], http://bit.ly/1pCNNhi.

26 Bundesgerichtshof [Federal Court of Justice], "Bundesgerichtshof erkennt Schadensersatz für den Ausfall eines Internetanschlusses zu" [Court awards damages for internet failures], press release 14/13, January 24, 2013, http://bit.ly/1FLvz98. Hartz IV standard rate is € 391, see: http://bit.ly/2d3yFYtl; € 2.28 of that sum are for Internet access, See: Deutscher Bundestag [German Bundestag], Drucksache 17/3404, p. 60, http://bit.ly/1LnUX6U.

27 Björn Brodersen/Alexander Kuch, "Backbones – die starken Hintergrundnetze des Internets" [Backbones – the strong background networks of the internet], teltarif.de, http://www.teltarif.de/internet/backbone.html.

28 "Deutsche Telekom," Wikipedia, accessed October 8, 2016, https://en.wikipedia.org/wiki/Deutsche_Telekom.

29 See https://www.de-cix.net/about/.

ICT Market

The telecommunications sector was privatized in the 1990s with the aim of fostering competition. The incumbent Deutsche Telekom's share of the broadband market was 41.6 percent in 2015, marking a slight decline as competition continued to increase. Other ISPs with significant mar et share included Vodafone with 18.4 percent, 1&1 with 14.1 percent, cable company Unitymedia at 10.1 percent, and O2-Telefónica with 6.9 percent.[30] In early March 2016, the Federal Cartel Office approved the acquisition of 25.11 percent of cable company Tele Columbus by United Internet, the parent company of 1&1.[31]

There are currently three general carriers for mobile internet access: T-Mobile, Vodafone, and Telefónica Deutschland. After a merger between O2 and E-Plus Group in 2014, Telefónica Deutschland remained the market leader with a share of 38.4 percent in 2015. Deutsche Telekom followed with 35.4 percent, while Vodafone had a market share of 26.2 percent.[32] Despite fears that the merger might lead to an increase in pricing of mobile services,[33] the prices continued to decrease in 2015, though probably slower than they might have without the merger.[34]

Regulatory Bodies

Internet access, both broadband and mobile, is regulated by the Federal Network Agency for Electricity, Gas, Telecommunications, Post, and Railway (*Bundesnetzagentur* or BNetzA), which has operated under the supervision of the Federal Ministry of Transport since early 2014.[35] The president and vice president of the agency are appointed for fi e-year terms by the German federal government, following recommendations from an advisory council consisting of 16 members from the German Bundestag and 16 representatives from the Bundesrat. The German Monopolies Commission and the European Commission (EC) have both criticized this highly political setting and the concentration of important regulatory decisions in the presidential chamber of the Federal Network Agency.[36] Similarly, the Court of Justice of the European Union (CJEU) and the EC noted that the regulation of data protection and privacy by agencies under state supervision does not comply with the EU Data Protection Directive 95/46/EC.[37]

In addition to these institutional concerns, regulatory decisions by the BNetzA have been criticized

30 DSLWEB, "Breitband Report Deutschland Q3 2015" [Broadband Report Germany], December 10, 2015, http://bit.ly/2dnx28E.

31 Jörn Krieger, "Bundeskartellamt gibt grünes Licht" [Federal Cartel Office gi es the go-ahead], TV Digital, March 9, 2016, http://bit.ly/2cZQs7D.

32 Statista, "Marktanteile der einzelnen Netzbetreiber an den Mobilfunkanschlüssen in Deutschland von 1998 bis 2015" [Market share of mobile operators in Germany 1998-2015], accessed October 8, 2016, http://bit.ly/2dBWHzR.

33 Bundesministerium für Wirtschaft und Technologie [Federal Ministry of Eceonomics and Technology], "Monitoring-Report Digitale Wirtschaft 2014," December 2014, p. 36, http://bit.ly/1uu9bEL.

34 "Was Handy- und Internetkunden 2016 erwartet" [What mobile and internet costumers may expect in 2016], Welt.de, December 24, 2015, http://bit.ly/2dbMuY4.

35 Markus Beckedahl, "Verkehrsministerium gewinnt Fachaufsicht über Bundesnetzagentur" [Ministry of Transport gains supervision over Federal Network Agency], Netzpolitik.org, February 14, 2014, http://bit.ly/1jDT9KQ.

36 Monopolkommission [Monopolies Commission], "Telekommunikation 2009: Klaren Wettbewerbskurs halten" [Telecommunication 2009: stay on target in competition], Sondergutachten 56, 2009, p. 75, http://bit.ly/2dBXDUY; European Commission, "Progress Report on the Single European Electronic Communications Market (15th Report)", COM(2010) 253, p. 196, http://bit.ly/1Od2qpT.

37 European Commission, "Data Protection: European Commission requests Germany to ensure independence of data supervisory authority," Press Release, Brussels, April 6, 2011, http://bit.ly/2cZPo3n.

for providing a competitive advantage to Deutsche Telekom, the former state-owned monopoly.[38] These reservations most recently reemerged in November 2015 after the BNetzA presented a proposal to allow the Telekom to implement vectoring, a technology that is capable of boosting the bandwidth of DSL connections on pre-existing copper lines.[39] However, in order to function as intended, it requires a single operator to remain in charge of the entire bundle of cables, which in turn means that unbundling and redistributing the connection becomes more difficult, effecti ely privileging the managing operator.[40] Due to this, criticism of the decision has been ongoing and strong. After the federal monopoly commission (*Monopolkommission*) voiced its concerns in an advisory opinion in December 2015,[41] the BNetzA advisory board demanded amendments in January 2016.[42] Telekom competitors even announced that they would consider a constitutional complaint before the Federal Constitutional Court against the decision.[43] As a reaction to persistent criticism, in June 2016 the BNetzA withdrew its original proposal and presented a revised version that is supposed to accommodate the competition and regulators' demands. However, the affected stakeholders maintained that the amendments made only minor changes to the situation.[44] As a result, one competitor has started to prepare a lawsuit against Telekom before the administrative court in Cologne.[45]

Limits on Content

Access to online content in Germany is mostly free. Restrictions concerning content usually involve copyright issues or disputes concerning the remuneration of authors. Some further limitations that potentially affect freedom of expression and freedom of information stem from the ongoing enforcement of the ancillary copyright for press publishers and the EU Court of Justices' decision on the "right to be forgotten" in May 2014.

Blocking and Filtering

Government imposed blocking of websites or internet content rarely occurs in Germany.[46] There

38 European Commission, Progress Report, p. 196. Since the Federal Republic still exercises its rights as a shareholder of Deutsche Telekom (circa 38 percent) through another public law entity, commentators see a potential conflict f interest. See: Christian Schmidt, "Von der RegTP zur Bundesnetzagentur. Der organisationsrechtliche Rahmen der neuen Regulierungsbehörde" [From RegTP to Federal Network Agency. The organizational framework of the new regulator], Die Öffentliche Verwaltung 58 (24), 2005, p. 1028.

39 Tomas Rudl, "Breitbandausbau: Telekom-Vectoring kommt näher" [Broadband development: Telekom vectoring approaches], Netzpolitik.org, November 23, 2015, http://bit.ly/2dOcz0t.

40 Richard Sietmann, "Fiber to the Neverland. Die Telekom forciert VDSL-Vectoring statt Glasfaser" [Fiber to the Neverland. DT pushes VDSL-Vectoring instead of Fiber], c't 10/2013, April 29, 2013, pp. 18-21, http://heise.de/-1847272.

41 Volker Briegleb, "VDSL-Turbo Vectoring: Monopolkommission warnt vor 'Technologiemonopol der Telekom'" [VDSL turbo vectoring: monopoly commission warns against 'technology monopoly of the Telekom'], heise.de, December 7, 2015, http://bit.ly/2eeTyog.

42 Tomas Rudl, "Vectoring: Beirat der Bundesnetzagentur fordert Nachbesserungen" [Vectoring: advisory board of Bundesnetzagentur demands amendments], Netzpolitik.org, January 26, 2016, http://bit.ly/2dD05a2.

43 Volker Briegleb, "VDSL-Vectoring: Telekom-Konkurrenten erwägen Verfassungsklage" [VDSL vectoring: competitors of Telekom consider entertain constitutional complaint], heise.de, January 20, 2016, http://bit.ly/2cZQM6p.

44 Volker Briegleb, "DSL-Turbo Vectoring: Regulierer legt geänderten Entwurf vor" [DSL turbo vectoring: regulator presents amended draft], heise.de, June 21, 2016, http://bit.ly/2dnxKDb.

45 Volker Briegleb, "VDSL-Turbo Vectoring: Schwarzer Supertag für Breitband-Deutschland" [VDSL turbo vectoring: black super day for broadband Germany], heise.de, September 2, 2016, http://bit.ly/2fAiwPv.

46 Due to substantial criticism by activists and NGOs that provoked an intense political debate, the 2010 law on blocking websites containing child pornography, the Access Impediment law (Zugangserschwerungsgesetz), never came into effect and was finally epealed by the German parliament in December 2011.

were no publicly known incidents carried out by state actors during this coverage period. YouTube, Facebook, Twitter and international blog-hosting services are freely available.

Content blocking or fil ering practices enforced by private or corporate actors have been an issue for some time. The ongoing dispute between YouTube and GEMA (German Society for Musical Performance and Mechanical Reproduction)[47] showcases how private entities substantially shape the availability of online content.[48] Since 2009, Google and GEMA have been unable to reach an agreement on the amount Google should pay for a license for copyright-protected music videos disseminated on YouTube. GEMA considers it a copyright infringement if YouTube uses content whose rights ownership is administered by GEMA and the Google-owned video platform refuses to pay adequate compensation to copyright holders.[49] As a result, YouTube blocks videos for users within Germany if the video might contain copyright-protected music, and instead displays an error message stating that the video is not available in Germany because GEMA might not have granted the publishing rights.[50] Google has raised concerns about the undesired effect on freedom of expression.[51] At the end of June 2015, two German courts – one in Hamburg, the other in Munich – decided that on the one hand, YouTube qualifies as a host p ovider, which means that it is in the privileged position of not being bound to pay damages if its users upload copyright-protected material.[52] On the other hand, it is under the obligation to block illegal content once it has gained knowledge of its existence on the platform.[53] The judgment has since been upheld in the second instance in January 2016,[54] which was subsequently appealed. On November 1, YouTube and GEMA finally eached a licensing agreement and the videos in question will no longer be blocked.[55]

In November 2015, the Federal Court of Justice ruled that the blocking of websites may be ordered as a last resort if it is the only possibility for a copyright holder to effectively end the rights infringement on that website.[56] That means that in such cases, after an assessment of all circumstances relevant to the case at hand, the owner of the copyright in question may demand the internet access provider to block the website in question. If the provider disagrees, a court would

47 Collecting societies are private organizations at the national level in Germany authorized by the Copyright Administration Act (*Urheberrechtwahrnehmungsgesetz*). Although they act under the supervision of the German Patent and Trademark Office (DPMA), they belong to the private sector. With the foundation of the collecting society C3S, provided the DPMA grants permission, GEMA's national monopoly could soon come to an end. See: Jens Uthoff, "Neue Wege im Paragraphendschungel" [New paths through the regulation jungle], taz.de, April 9, 2014, http://www.taz.de/!136441/.

48 Compared to 0.9 per cent in the United States and ca. 1 per cent in Austria and Switzerland. See: "Diese Kultur ist in Deutschland leider nicht verfügbar" [This culture is not available in Germany], sueddeutsche.de, January 28, 2013, http://sz.de/1.1584813.

49 GEMA, "GEMA and YouTube," accessed April 23, 2014, http://bit.ly/2eyz5wd.

50 GEMA demands 0.375 cents per retrieval.

51 In particular, Google argues that because the GEMA does not provide a list on the complete repertoire they licensed, most music videos have been blocked in order to avoid financial risks

52 "YouTube erzielt Etappensieg gegen die Gema" [YouTube with stage victory against Gema], *Zeit Online,* June 30, 2015, http://bit.ly/2dK3eEE.

53 Mirjam Hauck, "Kein Ende in Sicht" [No end in sight], Sueddeutsche.de, July 1, 2015, http://bit.ly/2dObaH9.

54 "Gema verliert erneut vor Gericht gegen YouTube" [Gema loses another lawsuit against YouTube], Welt.de, January 29, 2016, http://bit.ly/2dbKLSz.

55 This development occurred outside the period of coverage of this report. See: Tim Ingham, "YouTube strikes deal with GEMA to host music videos in Germany," Music Business Worldwide, November 1, 2016, http://bit.ly/2e8Hv7t.

56 Constanze Kurz, "BGH-Entscheidung zu Netzsperren: Die nichtsnutzige digitale Sichtschutzpappe ist zurück" [Federal Court of Justice decision on blocking of websites: the useless digital screen wall is back], Netzpolitik.org, November 26, 2015, http://bit.ly/2d3wCmY.

decide. The decision has been subject to criticism as such blocking is considered easy to circumvent and thus ineffective.[57]

German ISPs employ deep packet inspection (DPI) for the purposes of traffic management, as ell as to throttle peer-to-peer traffic. Use s are especially affected by peer-to-peer (P2P) related restrictions in the mobile market.[58] Although Vodafone, for example, announced that for the time being the practice shall remain limited to mobile internet access, there is no ultimate confi mation that it will not be extended in the future.[59]

The protection of minors constitutes an important legal framework for the regulation of online content.[60] Youth protection on the internet is principally addressed by states through the Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting (JMStV), which bans content similar to that outlawed by the criminal code, such as the glorification of violence and sedition.[61] A controversial provision of the JMStV reflecting the egulation of broadcasting media mandates that adult-only content on the internet, including adult pornography, must be made available in a way that verifies the age f the user.[62] The JMStV enables the blocking of content if other actions against offenders fail and if such blocking is expected to be effective. The Federal Criminal Police Office *Bundeskriminalamt*) has initiated the deletion of thousands of sites related to child pornography,[63] reporting a considerable increase in discovered sites in 2014.[64]

Content Removal

Most of the content removal issues in Germany relate to the removal of results from search engine functions, rather than deletion of content. The autocomplete function of Google's search engine has repeatedly been subject to scrutiny. In May 2013, the Federal Court of Justice ruled that Google could be held liable, at least under some circumstances, for the infringement of personal rights through its autocomplete function.[65] In its subsequent decision concerning the same case, the Higher Regional Court in Cologne decided that Google's liability amounted to the obligation to

57 Constanze Kurz, "BGH-Entscheidung zu Netzsperren: Die nichtsnutzige digitale Sichtschutzpappe ist zurück" [Federal Court of Justice decision on blocking of websites: the useless digital screen wall is back], Netzpolitik.org, November 26, 2015, http://bit.ly/2d3wCmY.

58 BEREC, "A view of traffic management and other practices esulting in restrictions to the open Internet in Europe. Findings from BEREC's and the European Commission's joint investigation," May 29, 2012, http://bit.ly/1MOMMhj.

59 Andre Meister, "Waschmaschine im Netz: Wie Telekom und Vodafone Deep Packet Inspection als Feature verkaufen" [Laundry machine on the net: How Telekom and Vodafone sell deep packet inspection as a feature], netzpolitik.org, August 1, 2014, http://bit.ly/1Od6TZN.

60 The legal framework regulating media protection of minors in particular consists of the Law for the protection of children and youth ("Jugendschutzgesetz", JuSchG) of the federal government and the Interstate Treaty on the Protection of Minors in the Media (short "Jugendmedienschutzstaatsvertrag", JMStV).

61 Cf. the respective §§ 130, 131 StGB [Crimical Code]. For English translation, see: http://bit.ly/1rT41ps.

62 Cf. the respective § 5, Abs. 3 JMStV.

63 "BKA ließ 2012 tausende Internetseiten löschen," [BKA had thousands of websites deleted in 2012], Handelsblatt.com, February 26, 2014, http://bit.ly/1MON7R2.

64 Stefan Krempl, "Löschen statt Sperren: BKA hat im Inland mehr mit Kinderpornografie zu tun" [Erasing ins ead of blocking: BKA has to deal with more domestic child pornography], heise.de, September 2, 2015, http://bit.ly/2dnwRdG.

65 BGH [Federal Supreme Court], judgment of May 14, 2013, Az. VI ZR 269/12; Jürgen Kuri/Martin Holland, "BGH zu Autocomplete: Google muss in Suchvorschläge eingreifen" [BGH on autocomplete], May 14, 2013 http://heise.de/-1862062.

delete the respective automated search query combination and to refrain from repeating the tort, but not to pay further compensation.[66]

Since the CJEU decision on the "right to be forgotten" in May 2014,[67] Google and other search engines are required to remove certain search queries from their index if they infringe on the privacy rights of a person and that person files a espective application with the search engine. As of March 10, 2016, Google had assessed more than 400,000 applications across the EU, with nearly 67,000 coming from Germany alone.[68] In 48.4 percent of the German requests, Google decided to remove the link. The process follows the guidelines developed by an advisory group of experts set up by the company in 2014, which published its final eport in February 2015.[69] The guidelines aim to strike a balance between the right to be forgotten on the one hand, and freedom of expression and information on the other.[70] In early March 2016, Google announced that it would delist links not only from its European domains such as google.de, google.fr, etc., but in the future resort to geo-blocking so that delisted links could not appear in Google search queries within the European Union even if someone used google.com instead of the national version of the search engine.[71] This had been one of the most pressing demands by European data protection office s since the publication of the CJEU decision.[72]

There is no censorship prior to the publication of internet content. On the other hand, figu es released by ICT companies indicate that post-publication content removal requests are issued with regard to defamation or illegal content. According to Google's latest transparency report regarding requests to remove content covering the period from July to December 2015, the company received 199 requests from the German courts and other public authorities. Defamation remains by far the most common reason for court orders to remove content.[73] Upon request from authorities, between July and December 2015, Facebook restricted access to 366 pieces of content that advocated right wing extremism and Holocaust denial, which are illegal under the German criminal code, up from 188 such removals between January and June 2015.[74]

Amidst the European "refugee crisis," which saw the rise of anti-refugee extremism on social media, the German federal government as well as domestic media started urging Facebook to become more proactive in addressing hateful or offensive content on its platform.[75] In October 2015, a Würzburg-based lawyer even filed a criminal complaint with the public p osecutor in Hamburg against Facebook's managing director for Northern, Central, and Eastern Europe. By doing so, the

66 Beck Aktuell, "OLG Köln: Klage gegen Google auf Unterlassugn bestimmter Suchwortkombinationen erfolgreich" [Higher Regional Court Cologne: Injunction suit against Google concerning certain search query combinations successful], April 8, 2014, http://bit.ly/2dnwPSY; Adrian Schneider, "OLG Köln: Die Autocomplete-Entscheidung im Detail" [Higher Regional Court Cologne: the autocomplete decision in detail], Telemedicus, April 11, 2014, http://bit.ly/1iRT59G.

67 ECJ, Google Spain and Google, 13 May 2014, http://bit.ly/1MKoqFS.

68 Google Transparency Report, European privacy requests for search removals, http://bit.ly/1nhgHFN.

69 Google Advisory Council, http://bit.ly/1j5L0Pd.

70 Eco.de, "Ein Jahr Recht auf Vergessenwerden: Löschen von Suchergebnissen beeinträchtigt die Zivilgesellschaft" [One year right to be forgotten: Removal of search results impairs civil society], May 13, 2015, http://bit.ly/1N9DnDW.

71 Peter Fleischer, "Adapting our approach to the European right to be forgotten, " Google Europe Blog, March 4, 2016, http://bit.ly/2e0CnUG.

72 Friedhelm Greis, "Recht auf Vergessen soll weltweit gelten" [Right to be forgotten shall be applicable globally], Golem.de, November 26, 2014, http://bit.ly/1vQfwkF.

73 Google complied fully or partially with 68 percent of the requests that included a court order, and 66 percent of requests from government agencies or law enforcement. Google, "Google Transparency Report, Germany: July to December 2015," http://bit.ly/2dnbSrg.

74 Facebook, "Government Requests Report: July 2015 – December 2015," http://bit.ly/2dVeZXy.

75 Eike Kühl, "Weniger Toleranz? Ja bitte." [Less tolerance? Yes please.], Zeit Online, November 25, 2015, http://bit.ly/2dK1qvp.

lawyer aimed to hold the executive personally responsible for the social network's alleged failure to curb or subdue hate speech on its platform.[76] Although the prosecutor subsequently opened an official in estigation against the manager, the charges against the Facebook manager were eventually dropped in March 2016 due to a lack of evidence for criminal responsibility.[77]

After initial hesitation, Facebook gradually became more willing to regulate its platform in accordance with German laws governing hate speech. In January 2016, the company set up a new team of employees in Berlin with the sole task of examining, and if necessary, deleting such comments or other content on the platform.[78] Despite some criticism coming from commentators abroad, especially in the United States where hate speech is not prohibited, many Germans seemed to welcome the heightened pressure on Facebook urging the company to change its practice towards hate speech.[79]

Platform operators can be held liable for illegal content under the Telemedia Act. The law distinguishes between full liability for owned content and limited "breach of duty of care" (*Stoererhaftung*) of access providers and host providers for third party content.[80] Although access and host providers[81] are not generally responsible for the content they transmit or temporarily auto store, there is a certain tension between the underlying principles of liability privilege and that of secondary liability.[82] Principally, ISPs are not required to proactively control or review the information of third parties on their servers; they become legally responsible as soon as they gain knowledge of violations or violate reasonable audit requirements.[83]

In 2012, court rulings limited the liability privilege of ISPs by further specifying requirements, responsibilities, and obligations. Additional blocking and fil ering obligations of host providers have been put in more concrete terms by the Federal Court of Justice (*Bundesgerichtshof*, BGH) in the "Alone in the Dark" case.[84] In this specific instance, the game publisher tari sued the file hosting service Rapidshare for copyright violations concerning a video game. Although the judges did not hold Rapidshare liable for direct infringement, they saw a violation of the service's monitoring obligations under the breach of duty of care as a result of Rapidshare's failure to proactively control its service for copyrighted material after it was notified f one infringing copy.[85]

In a subsequent decision concerning Rapidshare in August 2013, the BGH substantiated and further extended host providers' duties. According to the judgment, if the business model of a service aims

76 Ben Crair, "How Germany Is Dealing With Its Facebook Hate-Speech Problem", nymag.com, November 22, 2015, http://slct.al/2dAPVb7.

77 Geoffrey Smith, "Germany Drops Its Hate Speech Probe Into Facebook Managers", fortune.com, March 17, 2016, http://for.tn/2cZPtnL.

78 Fabian Reinbold and Marcel Rosenbach, "Hetze im Netz: Facebook löscht Kommentare jetzt von Berlin aus" [Incitement on the net: Facebook now deletes comments from Berlin], Spiegel Online, January 15, 2016, http://bit.ly/200TbdO.

79 Fabian Reinbold, "Flüchtlingshetze im Netz: Warum Facebook den Hass nicht löscht" [Anti-refugee incitement online: why Facebook does not delete the hate], Spiegel Online, September 7, 2015, http://bit.ly/1JPbxGR.

80 In particular: Part 3, §§ 7-10 TMG: liability for own content (§ 7, Abs. 1 TMG); limited liability for access providers (§§ 8, 9 TMG) and host providers (§ 10 TMG).

81 The BGH in particular has developed the principles of limited liability of host providers: BGH [Federal Court of Justice], judgment of October 25, 2011, Az. VI ZR 93/10.

82 Liability privilege means that information intermediaries on the internet such as ISPs are not responsible for the content their customers transmit. Secondary or indirect liability applies when intermediaries contribute to or facilitate wrongdoings of their customers.

83 BGH [Federal Court of Justice], judgment of March 27, 2012, Az. VI ZR 144/11, http://openjur.de/u/405723.html.

84 BGH [Federal Court of Justice], judgment of July 12, 2012, Az. I ZR 18/11, http://openjur.de/u/555292.html.

85 Timothy B. Lee, "Top German court says RapidShare must monitor link sites for piracy," *Ars Technica,* July 16, 2012, http://bit.ly/2dK2bVb.

to facilitate copyright infringements, the company is considered less worthy of protection with regard to liability privilege.[86] As a consequence, host providers are required to monitor their own servers and search for copyright-protected content as soon as it has been notified f a possible violation.[87] The Federal Ministry of Economy introduced a draft bill in March 2015 to revise the law on the breach of a duty of care. It explicitly provided for a preclusion of liability privilege for providers with such business models.[88]

A special requirement to review the content for any rights violations was also ruled in a case where a blogger integrated a YouTube video onto his website.[89] However, in October 2014, the CJEU ruled that embedding content from other sources by means of framing is not a copyright infringement.[90] In July 2015, the Federal Court of Justice clarified that embedding is legal, as long as the sou ce itself is legal – which at least in theory means that publishers are under the legal obligation to research whether the content they intend to embed was uploaded without a violation of copyright.[91]

An important exception to the liability privilege concerns wireless networks.[92] Because of a highly disputed ruling against the existing liability privilege by the Federal High Court in 2010, legislative initiatives from states and political parties have sought to modify the secondary liability of local Wi-Fi operators. The governing coalition agreed to press ahead with new legislation that aims to encourage the expansion of publicly accessible Wi-Fi networks by creating legal certainty for operators.[93] However, experts and the European Commission criticized the latest bill aiming to revise the current rules on liability, introduced in December 2015, for establishing high obstacles for providers of freely accessible Wi-Fi networks.[94] For example, the proposed requirement for users of such networks to declare that they will not violate the law while being online was considered problematic from both a legal and a technical standpoint.[95]

In addition to these legislative proposals, in September 2014 a Munich court asked the CJEU for a preliminary ruling on the question of the applicability of the liability privilege for a provider of an openly accessible Wi-Fi network.[96] In September 2016, the CJEU decided that although providers are usually not responsible for violations committed by the users of a free network, they are

86 BGH [Federal Court of Justice], judgment of 15 August, 2013, Az. I ZR 80/12, http://bit.ly/1MOQasE .

87 Thomas Stadler, "BGH erweitert Prüfpflich en von Filehostern wie Rapidshare" [Federal Court of Justice extends monitoring duties for host providers such as Rapidshare], Internet-Law, September 4, 2013, http://bit.ly/1N9EWSv.

88 Federal Ministry of the Economy, "Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz)" [Draft bill of a second act to revise the Telemedia Act], March 11, 2015, http://bit.ly/1C9Em24,

89 LG Hamburg [Regional Court Hamburg], judgement of May 18, 2012, Az. 324 O 596/11, http://openjur.de/u/404386.html.

90 CJEU, Case of BestWater International GmbH v Michael Mebes and Stefan Potsch, C-348/13, October 21, 2014, http://bit.ly/2dnq4k9.

91 Andreas Biesterfeld-Kuhn, "Die zweite Realität der Bundesrichter" [The federal judges' second reality], Legal Tribune Online, July 10, 2015, http://bit.ly/1Tzuq75.

92 In 2010, the German Federal High Court sentenced the private owner of a wireless router on the grounds that his or her open network allowed illegal activities. cf. Christopher Burgess, "Three Good Reasons to Lock Down Your Wireless Network," The Huffing on Post (blog), June 8, 2010, http://huff.to/1LYHK3k.

93 Coalition Agreement, p. 35.

94 Volker Tripp, "Anhörung zum Telemediengesetz: Wie geht es weiter mit offenem WLAN und Host-Providerhaftung?" [Hearing on telemedia act: what's next for open wireless networks and host provider liability?], Digitale Gesellschaft, December 16, 2015, http://bit.ly/2dCRT9R.

95 Volker Tripp, "WLAN-Störerhaftung: Die Rechtstreueerklärung muss weg" [Wireless network liability: declaration to abide the law needs to go], Digitale Gesellschaft, January 26, 2016, http://bit.ly/2dbCRZi; See also: Markus Beckedahl, "Trotz Störerhaftungs-Desaster: Dobrindt redet WLAN-Reform schön" [Despite debacle concerning breach of duty of care: Dobrindt sugarcoats Wi-Fi reform], Netzpolitik.org, February 1, 2016, http://bit.ly/1PzhfCZ.

96 "LG München I legt Frage der Haftung bei offenen WLANs dem EuGH vor" [Munich district court submits question on liability concerning open Wi-Fi to ECJ], Offenenetze.de, October 8, 2014, http://bit.ly/1iRW1mK.

obliged to secure free networks with a password.[97] The ruling was largely in line with prior German jurisprudence, and most commentators did not consider it an improvement for providers of openly accessible networks.[98]

Media, Diversity, and Content Manipulation

Germany is home to a vibrant internet community and blogosphere; however, there are some issues regarding the enforcement of ancillary copyright regulations, which may contribute to distorting search results for news outlets attempting to monetize their content.

To date, self-censorship online has not been a significant or ell-documented issue in Germany. Still, there are more or less unspoken rules reflec ed in the publishing principles of the German press.[99] The penal code and the JMStV prohibit content such as child pornography, racial hatred, and the glorification f violence in a well-defined manne . However, the OSCE strongly criticized the criminal investigation into the online media outlet Netzpolitik in July 2015, with regard to their reports on the activities of the German intelligence agencies, for its potential chilling effect on investigative reporting (see Violations of User Rights).[100]

Local and international media outlets and news sources are accessible and represent a diverse range of opinions. However, ancillary copyright for press publishers (*Leistungsschutzrecht für Presseverleger*), in force since 2013, allows publishers to monetize even the small snippets of information that search engine operators display as part of the results of a query.[101] This raised concerns regarding the constitutionally protected rights to freedom of expression and freedom of information.[102] In reaction to the law's enactment, search engines such as Google began excluding search results leading to the websites of publishers that monetized their search links, or displayed links without the corresponding snippets to limit monetization.[103] In response, the publishers' collecting society VG Media lodged complaints and antitrust proceedings against Google. Most recently in September 2015, the Federal Cartel Office decided that Google s practice was not in violation of antitrust laws.[104] Later in November 2015, arbitration proceedings between Google and VG Media failed, as the search engine regarded VG Media's demand to receive 6 percent of Google's aggregate turnover as license fees as inappropriate.[105] In response, VG Media filed a new lawsuit against Google in January 2016.[106]

97 Spiegel Online, "Das bedeutet das Urteil zur Störerhaftung für Deutschland" [This is what the ruling on network liability means for Germany], September 15, 2016, http://bit.ly/2cgKWvo.

98 Johannes Boie, "Das Wlan-Urteil des EuGH ist unsinnig" [The CJEU's wifi ruling does not ma e sense], sueddeutsche.de, September 15, 2016, http://bit.ly/2f15StA.

99 Presserat [Press Council], "Pressekodex" [press code], version dated March 13, 2013, http://bit.ly/1FgsgW8.

100 "OSCE representative warns about impact on free media of criminal investigation of Netzpolitik.org journalists in Germany," Organization for Security and Co-operation in Europe," August 4, 2015, http://bit.ly/2dT3gJK.

101 David Meyer, "Google fighting Ge man plan for linking fee", cnet.com, November 27, 2012, http://cnet.co/1WCkg72.

102 Philipp Otto, "Kommentar: ein unmögliches Gesetz" [Comment: an impossible law], iRights.info, August 30, 2012, http://bit.ly/1jE6XoJ.

103 Henry Steinhau, "Leistungsschutzrecht: T-Online und 1&1 verbannen Verlage der VG Media aus ihren Suchergebnissen" [Ancillary copyright: T-Online and 1&1 ban VG Media publishers from their search results], irights.info, September 16, 2014, http://bit.ly/1JKFxIY.

104 Friedhelm Greis, "Kartellamt hält Googles Vorgehen gegen Verlage für begründet" [Cartel Office conside s Google's approach against publishers justified], golem.de, Sep ember 9, 2015, http://bit.ly/2dJRQc4.

105 Stefan Krempl, "Schiedsverfahren zum Leistungsschutzrecht gescheitert" [Arbitration proceedings regarding ancillary copyright failed], heise.de, October 28, 2015, http://bit.ly/1NPyayF.

106 "Nach gescheitertem Schiedverfahren: VG Media reicht Klage gegen Google ein" [After failed arbitration: VG Media files lawsuit against Google], Urheberrecht.org, January 10, 2016, http://bit.ly/2cZHsiP.

Meanwhile, Germany's Telecoms Act authorizes the federal government to issue an executive order to protect the principle of net neutrality.[107] In November 2015, with the votes from the ruling coalition of Christian and Social Democrats, the German federal parliament rejected a legislative proposal by the Greens party to domestically safeguard net neutrality. Representatives of the majority referred to the EU regulation adopted in October 2015, deeming it a viable compromise.[108] Though formally endorsing the principle of net neutrality, the European regulation on net neutrality prompted concern that certain services may still be privileged within the networks, as experts deemed that the text would make it easy to introduce a fi st-class and second-class internet.[109] However, the final ersion of the "Guidelines on the Implementation by National Regulators of European Net Neutrality Rules," published by the Body of European Regulators for Electronic Communications (BEREC) at the end of August of 2016,[110] provide further safeguards for the principle of net neutrality, closing many of the loopholes for "specialized services."[111] The national legislator ought to follow the now clarified Eu opean standards concerning net neutrality.

Digital Activism

Several civil society initiatives have used the internet to conduct advocacy campaigns on political and social issues in Germany. In the summer of 2015, after the Federal Prosecutor General launched formal preliminary criminal proceedings against the journalists of Netzpolitik.org (see Prosecutions), thousands of Twitter users protested against the decision by using the hashtag #landesverrat ("treason").[112]

When xenophobic and racist comments spread online after the incidents of sexualized violence and robbery on New Year's Eve 2015 in the city of Cologne, several prominent German feminist activists (the same who, three years ago, had initiated the famous #aufschrei campaign against sexism) launched an online campaign to tackle both racism and sexualized violence, using the Twitter hashtag #ausnahmslos.[113] Several German and international politicians and activists endorsed the campaign and helped spread the hashtag, including the Federal Minister of Justice Heiko Maas.[114] Among other issues, the activists made calls to reform the German law governing sexual offenses.[115]

Separately, in January 2016 the non-governmental organization Digitale Gesellschaft started an

107 See section 41a of the Telecommunications Act.

108 Stefan Krempl, "Bundestag will Netzneutralität nicht umfassend absichern" [Federal parliament does not want to safeguard net neutrality comprehensively], heise.de, November 13, 2015, http://bit.ly/2eeGM9h.

109 Chris Baraniuk, "European Parliament votes against net neutrality amendments," Bbc.com, October 27, 2015, http://bbc.in/1jOhTAs; See also: Tomas Rudl, "EU-Parlament beschließt umstrittene Netzneutralitätsregeln" [EU Parliament enacts controversial net neutrality rules], Netzpolitik.org, October 27, 2015, http://bit.ly/1ids9R5.

110 "BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules," August 30, 2016, http://bit.ly/2fdSy3H.

111 Amar Toor, "Europe's net neutrality guidelines seen as a victory for the open web," *The Verge,* August 30, 2016, http://bit.ly/2c88eSd.

112 Judith Horchert, "Netzpolitik.org: Solidarität mit den #Landesverrätern" [Netzpolitik.org: Solidarity with the traitors], Spiegel Online, July 31, 2015, http://bit.ly/2dEWcSw.

113 Campaign website, http://ausnahmslos.org/english.

114 See Twitter post: http://bit.ly/2d3mrii.

115 "Twitter-Kampagne gegen sexualle Gewalt" [Twitter campaign against sexualized violence], Zeit Online, January 11, 2016, http://bit.ly/1PScaEm.

online video campaign against the proposed introduction of the mandatory retention of passenger name records within the European Union.[116]

Violations of User Rights

The scandal triggered by Edward Snowden's 2013 revelations concerning the activity of the NSA and German intelligence services remained inadequately assessed despite an ongoing parliamentary inquiry. Most significantly, a new data retention law was criticized for its extensive intrusion into private telecommunications data. The reintroduction of spy software for law enforcement authorities also raised concerns. The criminal investigation against two journalists for publishing articles containing classified state information drew widespread public criticism.

Legal Environment

German Basic Law guarantees freedom of expression and freedom of the media (Article 5) as well as the privacy of letters, posts, and telecommunications (Article 10). These articles generally safeguard offline as ell as online communication. A groundbreaking 2008 ruling by the Federal Constitutional Court established a new fundamental right warranting the "confidentiality and in egrity of information technology systems" grounded in the general right of personality guaranteed by Article 2 of the Basic Law.[117]

Online journalists are largely granted the same rights and protections as journalists in the print or broadcast media. Although the functional boundary between journalists and bloggers is starting to blur, the German Federation of Journalists maintains professional boundaries by issuing press cards only to full-time journalists.[118] Similarly, the German Code of Criminal Procedure grants the right to refuse testimony solely to individuals who have "professionally" participated in the production or dissemination of journalistic materials.[119]

Legislation to transform the Office f the Federal Commissioner for Data Protection and Freedom of Information from a subdivision of the Federal Ministry of the Interior to an independent supreme federal authority came into force on January 1, 2016. It is expected to significantly st engthen the Commissioner's powers in relation to data protection in Germany.[120] Aside from the change of constitutional status, the authority will in the future also administer a significantly higher budget and a larger staff.[121]

116 Ingo Dachwitz, "Wir fordern: NoPNR! Videoaktion gegen die EU-Vorratsdatenspeicherung von Reisedaten" [We demand: NoPNR! Video campaign against the EU retention of passenger name records], Digitale Gesellschaft, January 27, 2016, http://bit.ly/2e0tE4J.

117 BVerfG [Federal Constitutional Court], Provisions in the North-Rhine Westphalia Constitution Protection Act (Verfassungsschutzgesetz Nordrhein-Westfalen) on online searches and on the reconnaissance of the internet null and void, judgment of February 27, 2008, 1 BvR 370/07 Absatz-Nr. (1 - 267), http://bit.ly/1YVssS3; See also: Press release no. 22/2008, http://bit.ly/2dnoChN. For more background cf. Wiebke Abel/Burkhard Schaferr, "The German Constitutional Court on the Right in Confidentiality and In egrity of Information Technology Systems – a case report on BVerfG," NJW 2008, 822", 2009, 6:1 SCRIPTed 106, http://bit.ly/2dNZSCJ.

118 See: http://bit.ly/1P9Y563.

119 Code of Criminal Procedure (StPO), § 53 (1) 5, http://bit.ly/1O9zcXz.

120 "Endlich! Unabhängige Datenschutzbehörde für Deutschland" [Finally! Independent data protection agency for Germany], Datenschutzbeauftragter-info.de, August 27, 2014, http://bit.ly/1jE9tv3.

121 "Bundesdatenschutz-Behörde wird 2016 unabhängig" [Office ft he Federal Commissioner for Data Protection will become independent in 2016], N-TV.de, December 30, 2015, http://bit.ly/2eeGkYL.

Prosecutions and Detentions for Online Activities

In July 2015, the then-Federal Prosecutor General Harald Range instituted preliminary criminal proceedings against two online journalists, Markus Beckedahl and Andre Meister of Netzpolitik.org, for charges of treason after the site had published classified documents while reporting on activities of the Federal Office for the Protection of the Constitution. Initiated by Hans-Georg Maaßen, president of the Federal Office [122] the probe quickly sparked public outrage, chiefly among journalists but also within the ranks of senior politicians of both the federal parliament and the government. Legally, the case hinged on whether the leaked documents would in fact qualify as state secrets. Following an official instruction from the Federal Ministry of Justice, the investigations were halted on August 4, 2015, followed by a request from Justice Minister Heiko Maas to temporarily suspend Prosecutor General Range in an effort to calm rising criticism of the government. On August 10, it was determined that no state secrets had been leaked, and the criminal investigation came to an ultimate halt, though the incident continued to cause ripples over the following months.[123] Meanwhile, the incriminated journalists declared that they had reason to believe that they had been under surveillance by the Federal Criminal Police Office during the investigations.[124]

In another case that sparked a wider debate over freedom of speech in Germany in April 2016, Chancellor Merkel announced the decision to allow criminal proceedings against German satirist Jan Boehmermann.[125] Turkey's President Recep Tayyip Erdogan had filed a criminal complaint against the comic for a provocative poem mocking him, under an obscure German law that penalizes insults against foreign heads of state.[126] First aired on ZDF Television's Neo Magazin Royale show, ZDF also decided to remove the video clip from its official online channels, arguing that the poem did not meet the standards expected of its satire shows.[127] Prosecutors finally dropped the case against Boehmermann in October 2016 due to insufficient evidence [128]

The German Criminal Code (StGB) includes a provision on "incitement to hatred" (§ 130 StGB), which penalizes calls for violent measures against minority groups and assaults on human dignity.[129] The German people mostly regard this provision as legitimate, particularly because it is generally applied in the context of holocaust denials.[130] In the context of the ongoing refugee crisis, there has been a surge of criminal investigations invoking this provision, most of the time due to hate speech against asylum seekers on social media platforms such as Facebook. As a result, there have been

122 "Netzpolitik.org: Bundesanwaltschaft ermittelt gegen Journalisten wegen Landesverrats" [Federal prosecutor's office investigates against journalists for treason], Spiegel.de, July 30, 2015, http://bit.ly/1H6QXiu.

123 Martin Klingst, "Wer wann was verbockt hat" [Who failed when regarding what], Zeit Online, August 11, 2015, http://bit.ly/2eeFYl3.

124 Markus Beckedahl, "#Landesverrat: Wir müssen davon ausgehen, umfassend vom Bundeskriminalamt überwacht zu werden" [#Treason: We have to assume that we are under thorough surveillance by the Federal Criminal Police Office], Netzpolitik.org, August 7, 2015, http://bit.ly/2e0tla5.

125 Alison Smale, "Angela Merkel Draws Criticism for Allowing Turkey's Case Against Comic," *The New York Times,* April 15, 2016, http://nyti.ms/1V6IlVG.

126 Hasnain Kazim "Erdogan's Demand for Legal Action Puts Merkel in a Bind," *Spiegel,* April 12, 2016, http://bit.ly/2fdOL6z.

127 "German Television Pulls Satire Mocking Turkey's Erdogan," *The Intercept,* April 1, 2016, http://bit.ly/1MJVG3r.

128 "Germany drops Turkey President Erdogan insult case," *BBC,* October 4, 2016, http://bbc.in/2fAgzm6.

129 See Bundeszentrale für politische Bildung [Federal agency for political education], "Volksverhetzung" [incitement to hatred], http://bit.ly/2eoHnab.

130 BVerfG, [Federal Constitutional Court] 1 BvR 2150/08 from November 4, 2009, Absatz-Nr. (1 - 110), http://bit.ly/1KWt940; See also: Press release no. 129/2009 of 17 November 2009, Order of 4 November 2009 – 1 BvR 2150/08 – § 130.4 of the Criminal Code is compatible with Article 5.1 and 5.2 of the Basic Law, http://bit.ly/2e0uK0C.

considerably more convictions for incitement to hatred than usual.[131]

Surveillance, Privacy, and Anonymity

Following the classified documents lea ed by former NSA contractor Edward Snowden in 2013, the activities of the NSA, the British government's intelligence organization GCHQ, and the German intelligence service continued to stir debates during this coverage period. New legislation concerning data retention and reforms of the German intelligence service raised fresh concerns regarding the rights to privacy and freedom of expression.

The parliamentary commission of inquiry continued efforts to investigate and analyze the foreign intelligence agencies' activities on German territory as well as the involvement or complicity of German government or intelligence agencies. In July 2015, the federal government, following the parliamentary commission's proposal, appointed former federal judge Kurt Graulich as a special investigator to examine and assess the NSA's top-secret target lists for surveillance.[132] Graulich's final eport in October 2015 made serious allegations against the American intelligence agency. For instance, the judge found that the NSA had surveilled European government institutions, despite a contractual agreement between the agency and the Federal Intelligence Agency (*Bundesnachrichtendienst*, BND) explicitly restricting the practice. The report also found that European businesses, such as the Airbus armaments subsidiary EADS, were on the target list. At the same time, due to the alleged breach of contract, the BND was largely exonerated by the report.[133]

Opposition parties in the commission criticized Graulich's assessment, accusing the federal government of bias in investigating its own behavior, and demanded that the target list be handed to the commission itself.[134] A few days later, it was revealed that Graulich had copied internal reports by the BND to write his own report, which further undermined his asserted independence. Representatives of the Greens party alleged that the investigator's true role was to whitewash the federal government's conduct in the course of the affair.[135] In the aftermath of the scandal, the federal government vowed to introduce new legislation with the express purpose of controlling the BND's activities more tightly in the future. However, a draft bill approved by the cabinet in June 2016 has raised further criticism for attempting to legalize controversial surveillance practices rather than curtailing them.[136]

131 See for example: Pia Ratzesberger, "Verurteilt wegen Hasskommentaren auf Facebook" [Convicted for hateful comments on Facebook], sueddeutsche.de, February 3, 2016, http://bit.ly/1P8Luzi; Lisa Steger, "Hennigsdorfer soll Geldstrafe wegen Volksverhetzung zahlen" [Person from Hennigsdorf fined for inci ement to hatred], rbb-online.de, April 26, 2016, http://bit.ly/2d3m8Uz; "Bewährungsstrafe wegen Facebook-Hetze gegen Flüchtlinge" [Suspended sentence for incitement against refugees on Facebook], Zeit Online, October 16, 2015, http://bit.ly/1PKYR6U.

132 "Spionageaffäre: Union und SPD einigen sich auf NSA-Sonderermittler Graulich" [Espionage affair: CDU and SPD agree on NSA special investigator Graulich], Spiegel Online, July 1, 2015, http://bit.ly/2eeGe3i.

133 Maik Baumgärtner and Martin Knobbe, "Geheimdienstaffäre: Sonderermittler spricht von klarem Vertragsbruch der NSA" [Espionage affair: special investigator talks about clear breach of agreement], Spiegel Online, October 30, 2016, http://bit.ly/2dEVl4d.

134 "NSA und BND: Opposition kritisiert Bericht zur Geheimdienstaffäre" [NSA and BND: opposition criticizes report on espionage affair], Spiegel Online, October 31, 2015, http://bit.ly/2dO0gkx.

135 Thorsten Denkler, "Zweifel an der Unabhängigkeit" [Independence in doubt], Sueddeutsche.de, November 4, 2015, http://bit.ly/2dCQ6Bz.

136 Andre Meister, "Wir veröffentlichen den Gesetzentwurf zur BND-Reform: Große Koalition will Geheimdienst-Überwachung legalisieren" [We are publishing the draft of the BND reform: grand coalition wants to legalize surveillance], Netzpolitik.org, June 6, 2016, http://bit.ly/212OKAs; See also: "Germany's intelligence service reform stokes controversy," Euractiv.com, October 21, 2016, http://bit.ly/2dQ3iUL.

In early July 2015, revelations showed that the NSA had spied on German journalists in 2011. While the federal government had gained knowledge of the activity, it had apparently failed to investigate the case or attempt to stop the American intelligence agency. Moreover, it had not reported the activity to the federal parliament's control committee for intelligence. As a result, the affected news magazine filed a cha ge to the federal prosecutor's office [137]

In February 2016, reports revealed that Federal Bureau of Criminal Investigation (BKA) had finished developing a new version of its own spyware (the so-called *Bundestrojaner*, "federal Trojan horse") that would be ready before mid-2016 to spy on the communications of suspected criminals. In accordance with a 2008 ruling of the Federal Constitutional Court, the software would not be capable of sifting through whole computer systems or hard drives. However, experts raised serious doubts concerning its purported capacity, as there is no significant echnical difference between the two modes of operation.[138]

Furthermore, the use of so-called silent SMS or stealth pings by the BKA has vastly increased. The technology is used to monitor a target person's movements, without the target's notice. In the second half of 2015, the BKA sent 116,948 of those invisible text messages, compared to only 22,357 in the fi st half of last year. Both the federal police and the Federal Office for the P otection of the Constitution also resorted to the use of silent SMS, in 41,671 and 45,376 instances, respectively. Despite judicial oversight, the practice has drawn criticism, in particular from the party Die Linke.[139]

Telecommunications interception by state authorities for criminal prosecutions is regulated by the code of criminal procedure (StPO) and may only be employed for the prosecution of serious crimes for which specific evidence exists and when othe , less-intrusive investigative methods are likely to fail. According to recent statistics published by the Federal Office f Justice, there were a total of 22,590 orders for telecommunications interceptions in 2015, compared to 23,382 in 2014, of which 7,431 concerned internet communications, compared to only 5,485 in the year before.[140] There were also a total of 27,164 orders requesting internet traffic data in 2015, com ared to 22,701 in 2014.[141]

Surveillance measures conducted by the secret services under the Act for Limiting the Secrecy of Letters, the Post, and Telecommunications exceed these figu es. In 2014, the competent Parliamentary Control Panel reported that a total of 25,209 telecommunications – most of them email – were scanned, of which only 82 were considered relevant.[142] The panel highlighted the steady and significant decline in su veillance measures, the number of which had been above 2.8 million in 2011, and 851,691 in 2012. The email contents were scanned for keywords relating to certain "areas

137 "Überwachung: SPIEGEL im Visier von US-Geheimdiensten" [Surveillance: SPIEGEL in U.S. intelligence services' crosshairs], Spiegel Online, July 3, 2015, http://bit.ly/2e0tU3X.

138 Falk Steiner, "Neuer Bundestrojaner steht kurz vor der Genehmigung" [New federal Trojan horse to be approved soon], Deutschlandfunk.de, February 22, 2016, http://bit.ly/20PKsLM.

139 Tomas Rudl, "'Stille SMS': Bundeskriminalamt verschickte fünf Mal so viele wie im ersten Halbjahr" [Stealth ping: BKA sent fi e times as many as in the fi st half oft he year], Netzpolitik.org, January 20, 2016, http://bit.ly/23gmo8O.

140 Bundesamt für Justiz [Federal Office f Justice], "Übersicht Telekommunikationsüberwachung (Maßnahmen nach §100a StPO) für 2015", July 14, 2016 [Summary of telecommunication surveillance for 2015], http://bit.ly/2e2ktVI.

141 Bundesamt für Justiz, "Übersicht Verkehrsdatenerhebung (Maßnahmen nach § 100g StPO) für 2015" [Summary of traffic data collection for 2015], July 22, 2016, http://bit.ly/2dMGVis.

142 These are aggregated figu es related to the three areas of risk in which scanning took place according to the report of the Parliamentary Control Panel. See: Deutscher Bundestag, Drucksache 18/7423, January 29, 2016, p.7 et seq., http://bit.ly/2e0t8Ui. Note that the numbers presented annually do not refer to the last year but to the year before, i.e. 2014. The Parliamentary Control Panel periodically reports to the parliament and nominates the members of the G10 Commission. The G10 Commission controls surveillance measures, and is also responsible for overseeing telecommunications measures undertaken on the basis of the Counterterrorism Act of 2002 and the Amendment Act of 2007.

of risk," namely international terrorism, proliferation of arms and other military technology, and human smuggling.[143]

Excessive interceptions by secret services formed the basis of a 2008 Federal Constitutional Court ruling, which established a new fundamental right warranting the "confidentiality and in egrity of information technology systems." The court held that preventive covert online searches are only permitted "if factual indications exist of a concrete danger" that threatens "the life, limb, and freedom of the individual" or "the basis or continued existence of the state or the basis of human existence."[144] Based on this ruling, the Federal Parliament passed an act in 2009 authorizing the Federal Bureau of Criminal Investigation (BKA) to conduct covert online searches to prevent terrorist attacks with a warrant.[145] In addition to online searches, the act authorizes the BKA to employ methods of covert data collection, including dragnet investigations, surveillance of private residences, and the installation of a program on a suspect's computer that intercepts communications at their source. The anti-terror legislation fi st passed after the September 11 terrorist attacks, and that *inter alia* obliges banks or telecommunications operators to disclose customer information to the authorities, was once again extended in November 2015 through 2021.[146]

The amended telecommunication act of 2013 reregulates the "stored data inquiry" requirements (*Bestandsdatenauskunft*).[147] Under the new provision, approximately 250 registered public agencies, among them the police and customs authorities, are authorized to request from ISPs both contractual user data and sensitive data. While the 2004 law restricted the disclosure of sensitive user data to criminal offenses, the amended act extends it to cases of misdemeanors or administrative offenses. Additionally, whereas the disclosure of sensitive data and dynamic IP addresses normally requires an order by the competent court, contractual user data (such as the user's name, address, telephone number, and date of birth) can be obtained through automated processes. The requirement of judicial review has been subject to two empirical studies, both of which found that in the majority of cases a review by a judge does not take place.[148] Data protection experts criticize the lower threshold for intrusions of citizens' privacy as disproportionate.

143 See the report of the Parliamentary Control Panel: Deutscher Bundestag, Drucksache 18/7423, January 29, 2016, p. 7-8, http://bit.ly/2e0t8Ui.

144 Bundesverfassungsgericht [Federal Constitutional Court], Provisions in the North-Rhine Westphalia Constitution Protection Act (Verfassungsschutzgesetz Nordrhein-Westfalen) on online searches and on the reconnaissance of the Internet null and void, judgment of February 27, 2008, 1 BvR 370/07; For more background cf. W Abel and B Schafer, "The German Constitutional Court on the Right in Confidentiality and In egrity of Information Technology Systems – a case report on BVerfG", NJW 2008, 822, (2009) 6:1 SCRIPTed 106, http://bit.ly/2dNZSCJ.

145 Dirk Heckmann, "Anmerkungen zur Novellierung des BKA-Gesetzes: Sicherheit braucht (valide) Informationen" [Comments on the amendment of the BKA act: Security needs valid information], Internationales Magazin für Sicherheit nr. 1, 2009, http://bit.ly/1KWuRm6.

146 "Anti-Terror-Gesetze gelten bis 2021" [Anti terror laws in force until 2021], Tagescchau.de, November 27, 2015, http://bit.ly/2cZGl2H.

147 Bundesrat, "Mehr Rechtssicherheit bei Bestandsdatenauskunft" [More legal certainty for stored data inquiry], Press release no. 251/2013, May 3, 2013, http://bit.ly/1j5NgWK.

148 Two independent studies from by the Universität of Bielefeld (2003: Wer kontrolliert die Telefonüberwachung? Eine empirische Untersuchung zum Richtervorbehalt bei der Telefonüberwachung" [Who controls telecommunication surveillance? An empirical investigation on judicial overview of telecommunication surveillance], edited by Otto Backes and Christoph Gusy, 2003) and Max-Planck-Institut Institute for Foreign and International Criminal Law (Hans-Jörg Albrecht, Claudia Dorsch, Christiane Krüpe 2003: Rechtswirklichkeit und Effizienz der Übe wachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen [Legal reality and efficiency f wiretapping, surveillance and other covert investigation measures], http://www.mpg.de/868492/pdf.pdf) evaluated the implementation of judicial oversight of telecommunication surveillance. Both studies found that neither the mandatory judicial oversight nor the duty of notification f affected citizens are carried out. According to the study by the Max Planck Institute, only 0.4 percent of the requests for court orders were denied.

Despite the CJEU 2014 decision to declare the EU Data Retention Directive unconstitutional,[149] the federal parliament enacted a law concerning the reintroduction of data retention with the votes of the governing coalition in October 2015.[150] Both the opposition and data protection officials had fie cely opposed the legislative proposal, maintaining that the law contradicts civil laws and violates the guidelines established by the CJEU. Under the new law, different sets of data have to be stored on servers located within Germany for ten weeks, while providers have to retain the numbers, and the date and time of phone calls and text messages, and internet providers are required to retain IP addresses of all internet users, as well as the date and time of connections. The location data of mobile phone connections must be saved for four weeks. The requirements exclude sites accessed, email traffic metadata, and the con ent of communications. Though solely aimed at assisting law enforcement agencies, in January 2016 leading representatives of the governing Christian Democratic Union demanded an extension of the law so that domestic intelligence agencies could also access the data.[151] In reaction to the controversial legislation, so far no less than four constitutional complaints have been filed against the la . Among other issues, the complainants claim that, contrary to the CJEU guidelines, which only allow for the retention of data of suspects, the law would enable indiscriminate mass retention of data.[152]

User anonymity is compromised by SIM cards registration requirements under the telecommunication act of 2004, which requires the purchaser's full name, address, international mobile subscriber identity (IMSI), and international mobile station equipment identity (IMEI) numbers, if applicable.[153] Nonetheless, the principle anonymity on the internet is largely upheld as a basic right, despite disapprovals from the Federal Minister of the Interior and some other members of the conservative parties.[154] A decision by the Federal Court of Justice further strengthened this right, confi ming that an online review portal is under no obligation to disclose the data of an anonymous user. In the preceding judgment, the Higher Regional Court in Stuttgart had ruled to the contrary.[155] Website owners and bloggers are not required to register with the government. However, most websites and blogs need to have an imprint naming the person in charge and contact address. The anonymous use of email services, online platforms, and wireless internet access points are legal. In January 2016 however, reports noted how the Federal Criminal Police Office continued o lobby against encryption technologies at the European level.[156]

Intimidation and Violence

There have been no known cases of direct intimidation or violence against online journalists or other

149 Court of Justice of the European Union, "The Court of Justice declares the Data Retention Directive to be invalid," press release No 54/14, April 8, 2014, http://bit.ly/1svi4QN.

150 "Bundestag beschließt Vorratsdatenspeicherung" [Bundestag enacts data retention], Faz.net, October 16, 2015, http://bit.ly/2e0seXT.

151 Markus Beckedahl, "CDU verspricht Verfassungsschutz den Zugriff auf Vorratsdatenspeicherung und mehr Staatstrojaner" [CDU promises domestic intelligence agency access to data retention and more state Trojan horses], Netzpolitik.org, January 13, 2016, http://bit.ly/2dW17S5.

152 Jakob May, "Weitere Verfassungsbeschwerde gegen Vorratsdatenspeicherung eingereicht" [Further constitutional complaint against data retention filed], Netzpoliti .org, January 27, 2016, http://bit.ly/1nQGru9.

153 Telecommunications Act (TKG), § 111, http://bit.ly/2dNZTqh.

154 Anna Sauerbrey, "Innenminister Friedrich will Blogger-Anonymität aufheben" [Federal Minister of Interior wants to abolish anonymity of bloggers], Tagesspiel online, August 7, 2011, http://bit.ly/2dCQ2BX.

155 "BGH weist Auskunftsanspruch gegen Internet-Portal zurück" [Federal Court of Justice rejects claim to disclosure against internet portal], Zeit.de, July 1, 2014, http://bit.ly/1iUs1Xa.

156 Matthias Monroy, "BKA auf EU-Ebene weiterhin gegen 'Anonymisierung und Verschlüsselung' aktiv" [BKA continues to be active against 'anonymization and encryption' on the EU level], Netzpolitik.org, January 6, 2016, http://bit.ly/2dJQi1z.

ICT users during the coverage period.

Technical Attacks

Human rights activists and nongovernmental organizations are rarely victims of cyberattacks or other forms of technical violence. However, cyberattacks have become an increasingly significant problem for industry in Germany. According to a survey conducted by the Federal Office for Information Security (BSI), 58.5 percent of German businesses and public institutions were affected either by a successful or unsuccessful cyberattack in the past two years. This represents a slight increase compared to the previous year, when the number was at 56.4 percent.[157] In the summer of 2015, hackers attacked the federal parliament's network and left it entirely crippled.[158] The whole network went offline for four days until the se vers were renewed.[159]

To strengthen its response capabilities to cyberattacks, the federal parliament enacted an IT security law in June 2015 obliging telecommunication fi ms and critical infrastructure operators to report security breaches to the BSI. However, the new law has been subject to criticism for being largely ineffective and overly intrusive concerning the storage of traffic data o determine the source of possible cyberattacks.[160]

157 BSI, "Cyber-Sicherheits-Umfrage 2015" [Cyber security survey 2015], October 5, 2015, http://bit.ly/2dCOZSo.

158 Marie Rövekamp, "Findet den Trojaner!" [Find the Trojan horse!], *Zeit Online*, August 11, 2015, http://bit.ly/2dJOky7.

159 Anna Biselli, "Wir veröffentlichen Dokumente zum Bundestagshack: Wie man die Abgeordneten im Unklaren ließ" [We are publishing documents concerning the Bundestag hack: how the members of parliament were left in the dark], Netzpolitik.org, March 7, 2016, http://bit.ly/2dEUqAN.

160 Anna Biselli, "Heute im Bundestag Verabschiedung des IT-Sicherheitsgesetzes – ein Überblick" [Today in the parliament enactment of the IT security law – an overview], Netzpolitik.org, June 12, 2015, http://bit.ly/1FcCwIH.

Freedom House

Hungary

	2015	2016
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	4	5
Limits on Content (0-35)	9	10
Violations of User Rights (0-40)	11	12
TOTAL* (0-100)	**24**	**27**

* 0=most free, 100=least free

Population:	**9.8 million**
Internet Penetration 2015 (ITU):	**73 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2016 Status:	**Partly Free**

Key Developments: June 2015 – May 2016

- In January 2016, the European Court of Human Rights found that Hungary's internet and telecommunication surveillance practices violate the European Convention on Human Rights (see **Surveillance, Privacy, and Anonymity**).
- Hungarian citizens campaigned online against xenophobic, anti-immigration rhetoric employed by government agencies throughout the refugee crisis (see **Digital Activism**).
- Public officials continue o use defamation and libel charges against citizens commentating on social networks (see **Prosecutions and Detentions**).

Introduction

Internet freedom declined Hungary in 2015-2016, reflecting inc easing defamation cases launched by public officials against o dinary users, while the European Court on Human Rights condemned the government's surveillance practices.

The internet remains relatively free in Hungary, and the government does not engage in any politically motivated blocking or fil ering of online content. However, individuals and websites have been held liable by Hungarian courts for content posted on their pages by third parties, a practice which has been condemned by the European Court of Human Rights as undermining the right to freedom of expression. The diversity of the online media landscape is further threatened by the inequitable and politically biased distribution of advertising revenue, resulting in the closure of some independent online outlets over the past few years.

While social media users and online commentators do not face prison sentences for their activities online, public officials ften initiate defamation proceedings against users posting or even sharing critical content. Though these proceedings are often either dropped or result in small fines, this orrying trend demonstrates the government's low tolerance for criticism and may have a chilling effect on expression.

Following unsuccessful attempts to raise the issue in Hungarian courts, the European Court of Human Rights ruled in January 2016 that Hungary's online surveillance practices constitute a violation of the European Convention on Human Rights.[1] The Anti-Terrorism Task Force, a special police unit, possesses broad powers to gather information from telecommunications systems without judicial oversight, and the extent to which the authorities monitor ICTs is unclear. The legal system permitting these practices remains unchanged.

Obstacles to Access

Internet access is widespread in Hungary, with internet penetration rates steadily increasing over the past several years, despite a slight slump in 2015. The government recently announced plans to reduce taxes paid by internet service providers which may reduce prices for consumers. The internet and mobile markets remain concentrated among a handful of providers.

Availability and Ease of Access

The internet penetration rate has been steadily increasing in Hungary over the past several years, though the ITU registered a slight drop in 2015, with 72.8 percent penetration compared to 76 percent in 2014.[2] Other figu es were similar. According to a 2015 Gemius survey, the internet penetration rate in Hungary was at 70 percent among users aged 18 to 69 years old.[3] The National Media

1 Szabó and Vissy v. Hungary (application no: 37138/14), http://bit.ly/1Rk9i6o.

2 International Telecommunication Union, "Percentage of individuals using the Internet," accessed February 25, 2015, http://bit.ly/1FDwW9w.

3 Gemius, "Internet penetration in 12 European Union countries," May 8, 2015, https://www.gemius.com/e-commerce-news/internet-penetration-in-12-european-union-countries.html.

and Infocommunications Authority of Hungary (NMHH) reported that there were over 2.5 million broadband internet subscriptions in January 2016, in a country of less than 10 million inhabitants.[4]

Dial-up internet service is not widely used. The NMHH recorded a mobile phone penetration rate of about 117 percent and over 4 million mobile internet subscriptions in 2014.[5] In 2014, only 22 percent of the population had never used the internet, a decrease from 52 percent in 2006.

Hungary's internet penetration levels differ based on geographical and socioeconomic conditions, with lower access rates found among low-income families and in rural areas. According to the 2014 data from the TNS Hoffmann research company, internet penetration was over 82 percent among the employed but only 52 percent among those who were unemployed. Internet penetration also differs between those living in the capital and in the countryside.[6] A digital divide based on ethnicity has also been observed. There is no new data on the internet penetration level among the Roma community, the country's largest ethnic minority, though in the past this group has had lower-than-average levels of internet access.[7]

The National Curriculum for 2013 drastically decreased the number of IT classes in primary and secondary schools, despite protests from IT teachers, potentially further increasing the digital divide among social groups, as children coming from low-income families may not have access to digital devices at home.[8] Poor IT infrastructure at public schools further increases the digital divide.[9]

The cost of internet access is comparatively high. In 2016, the median price for a monthly internet subscription was EUR 52 (US$57), making Hungary the fi th most expensive country for internet access in the EU.[10]

In late 2014, a proposed tax on internet usage sparked widespread protests in Hungary, and the Orban administration withdrew the proposal.[11] The tax would have cost internet service providers (ISPs) approximately HUF 150 (US$0.61) per GB of data, a fee which they would likely have passed on to consumers. During his speech withdrawing the proposal, Orban hinted at the possibility of reintroducing taxes and other regulations. In March 2016, however, the Government announced that it will reduce the value-added tax on internet service from 27 percent to 18 percent from 2017.[12]

4 National Media and Infocommunications Authority Hungary, "Flash report on landline service," December 2015, http://nmhh.hu/cikk/169480/Vezetekes_gyorsjelentes_decemberben_az_adatszolgaltatok_vezetekes_szelessavu_internetelofize eseinek_becsult_szama_2568_millio_volt.

5 National Media and Infocommunications Authority Hungary, "Flash report on mobile internet," January 2014, http://bit.ly/1VJbhnK.The International Telecommunication Union similarly estimated the mobile penetration rate at 118 percent for 2014. The latest available data on this topic is from 2014.

6 TNS-Hoffmann Kft. Media Sector TGI 2014/1–4 quarters.

7 Anna Galácz, Ithaka Kht, eds., "A digitalis jövő térképe. A magyar társadalom és az internet. Jelentés a World Internet projekt 2007. évi magyarországi kutatásának eredményeiről," [The map of the digital future. The Hungarian society and the internet. Report on the results of the 2007 World Internet Project's Hungarian research] (Budapest: 2007): 20.

8 Tamás Papós, "Esélytelen diákok és 1 Mbit-es internet a magyar iskolákban," [A chance for students and 1Mbit internet at Hungarian schools] *Hvg.hu*, October 3, 2013, http://bit.ly/1RxESuy.

9 European Schoolnet and University of Liege, "Survey of schools: ICT in education, Country profile: Hunga y," November 2012, http://bit.ly/1IVN56J.

10 Digital Transformation of Small and Medium Enterpises in Hungary, DELab UWCountry Report, February, 2016, http://bit.ly/2dEPDC9.

11 Rick Lyman, "Hungary Drops Internet Tax Plan After Public Outcry," *New York Times*, October 31, 2014, http://nyti.ms/1zmv8Nv.

12 „Internetadó helyett valami egészen mást akarnak Orbánék", [Orban and his crew want something fundamentally different to internet tax now], Hvg.hu, 4 March 2016, http://bit.ly/1M2Jsgu.

Restrictions on Connectivity

The government does not restrict bandwidth, routers, or switches,[13] and backbone connections are owned by telecommunications companies rather than the state.[14] The Budapest Internet Exchange (BIX) is a network system that distributes Hungarian internet traffic among domestic in ernet service providers (ISPs), and is overseen by the Council of Hungarian Internet Service Providers (ISZT)[15] without any governmental interference.[16] Legally, however, the internet and other telecommunications services can be paused or limited in instances of unexpected attacks, for preemptive defense, or in states of emergency or national crisis.[17]

ICT Market

The ICT market in Hungary lacks significant competition, with o er a third of the market belonging to Magyar Telekom. Four ISPs control over 80 percent of the total fi ed broadband market.[18] UPC was the fi st company to enable home routers to serve as Wi-Fi hotspots, at the same time as it entered the mobile phone market as a mobile virtual network operator, which resells service using networks owned by another provider.[19]

There are three mobile phone service providers, all privately owned by foreign companies.[20] Mobile internet network expansion has been relatively stagnant because of the lack of competition. A market with few players is also more easily influenced by the go ernment, which can negotiate individually with service providers.

The government levied two special taxes on the telecommunication industry in 2010, both of which triggered infringement proceedings in the European Union in 2012. The government withdrew the tax and both proceedings were withdrawn.[21] Another tax on mobile phone calls and text messages was introduced in mid-2012 (a maximum of $3 a month per subscriber).[22] All mobile service providers have since raised their prices.[23]

Regulatory Bodies

13 Zoltán Kalmár, Council of Hungarian Internet Service Providers, e-mail communication, January 24, 2012.

14 rentITKft., "Magyarország internetes infrastruktúrája" [Hungary's internet infrastructure] January 29, 2010, http://bit.ly/1N38PRq.

15 Budapest Internet Exchange (BIX), "BIX Charter," April 21, 2009, http://bix.hu/?lang=en&page=charter.

16 Zoltán Kalmár, Council of Hungarian Internet Service Providers, email communication, January 24, 2012.

17 Act CXIII of 2011 on home defense, Military of Hungary, and the implementable measures under special legal order, Art. 68, par. 5.

18 These major internet service providers are: Telekom with a 36.1 percent market share, UPC 21.9 percent, DIGI 14.8 percent, and Invitel 9.4 percent. See National Media and Infocommunications Authority Hungary, *Flash report on landline service*, December 2015,http://bit.ly/1QAmgaz.

19 "UPC Hungary launches voice/data MVNO and national free Wi-Fi service," *Tele Geography*, November 14, 2014, http://bit.ly/1ME8fJ0.

20 The three mobile phone companies are: Telekom with a 46.82 percent market share, Telenor 30.48 percent, and Vodafone 22.7 percent. See National Media and Infocommunications Authority Hungary, *Flash report on mobile internet*, January 2014, http://bit.ly/1VJbhnK.

21 European Commission vs. Hungary, Case C-462/12, November 22, 2013; and "EC drops suit over Hungary telecoms tax," *Politics*, September 27, 2013, http://bit.ly/1QdD20V.

22 Andras Gergely, "Hungary Phone Tax Burden May Affect Magyar Telekom Dividend," *Bloomberg Business*, May 10, 2012, http://bloom.bg/1G2ceQG.

23 "Telefonadó: A Telenor és a Magyar Telekom is emeli a díjait," [Telephone tax: both Telenor and Magyar Telekom raises prices] *Hvg.hu*, September 10, 2013, http://hvg.hu/gazdasag/20130910_Vandorlasba_kezdhet_a_mobilpiac.

The National Media and Infocommunications Authority of Hungary (NMHH) and the Media Council, established under media laws passed in 2010, are responsible for overseeing and regulating the mass communications industry. The Media Council is the NMHH's decision-making body in matters related to media outlets, and its responsibilities include allocating television and radio frequencies and penalizing violators of media regulations. The Head of the Media Council appoints the president of the MTVA, the fund responsible for producing content for the public service media.[24] The members of the Media Council are nominated and elected by parliamentary majority, then appointed by the president of the republic.[25] The head of the NMHH is appointed by the president based on the proposal of the prime minister, for a non-renewable nine-year term.[26]

Some of the decisions of the Media Council have been regarded as politicized. Critics contend that the Media Council operates with unclear provisions and can impose high fines [27] which might give rise to uncertainty and fear, lead to self-censorship, and have a chilling effect on journalism as a whole. OSCE Representative on Freedom of the Media, Dunja Mijatovic, warned that the 2010 media laws "only add to the existing concerns over the curbing of critical or differing views in the country."[28]

With the adoption of the Fundamental Law of Hungary, which entered into force in January 2012, the governing parties prematurely ended the six-year term of the Data Protection Commissioner, replacing the former office with the National Authority for Data P otection and Freedom of Information. The head of the new authority is appointed by the president of the republic based on the proposal of the prime minister for a nine-year term and can be dismissed by the president based on the proposal of the prime minister,[29] calling into question the independence of the agency. In 2014, the Court of Justice of the European Union ruled that Hungary failed to fulfill its obligations under EU law when it ended the Data Protection Commissioner's term.[30]

Limits on Content

The government of Hungary does not engage in any significant blocking of content online and does not place restrictions on access to social media, though a number of websites purportedly containing Holocaust denial content were blocked by the authorities after the coverage period. Online content is somewhat limited as a result of lack of revenue for independent media outlets online, the dominance of the state-run media outlet, and the biased nature of the allocation of state advertisement funds. In the past, Hungarian courts have held hosting service providers and even Facebook page administrators liable for content posted on their pages, though this may change following a decision of the European Court of Human Rights declaring this practice to be in violation of the European Convention on Human Rights.

Blocking and Filtering

The government does not place any restrictions on access to social media or communication appli-

24 Act CLXXXV of 2010, art. 136. par. 11.
25 Act CLXXXV of 2010, art. 124.
26 Act CLXXXV of 2010, art. 111/A.
27 Article 19, *Hungarian media laws Q&A*, August 2011, http://bit.ly/1LlBPVq.
28 OSCE, "Revised Hungarian media legislation continues to severely limit media pluralism, says OSCE media freedom representative," press release, May 25, 2012, http://www.osce.org/fom/90823.
29 Act CXII of 2011 on data protection and freedom of information, Section 40, par. 1, 3; Section 45, par. 4–5.
30 Case C-288/12, Commission v Hungary, April 8, 2014.

cations. YouTube, Facebook, Twitter, Tumblr, international blog-hosting services, instant messaging, and other applications are freely available.

The authorities often block content related to Holocaust denial. In August 2016, a Hungarian court ordered the blocking of 20 websites which contained material denying the Holocaust, in compliance with laws banning public Holocaust denial.[31] In January 2015, the Metropolitan Court of Justice ordered the far-right website Kuruc.info[32] to delete an article denying the Holocaust.[33] The stipulation of the penal code is often called the "Kuruc.info law" by experts, as the law was largely drafted to target the infamous website, which is hosted abroad.[34] Since the website is hosted outside of the Hungarian jurisdiction and therefore cannot be forced to shut down, the prosecutors of district V and XIII of Budapest stated that the article on Kuruc.info would be permanently blocked in May 2015, though the article was still accessible as of October 2016.[35]

The new penal code, which took effect on July 1, 2013, includes provisions based on which websites can now be blocked for hosting unlawful content.[36] The law stipulates that if the illegal content is hosted on a server located outside of the country, the Hungarian court will issue a query to the Minister of Justice to make the content inaccessible; the minister then passes the query onto the "foreign state," and if there is no response from that state for 30 days, the court can order domestic ISPs to make the given content inaccessible.[37] The prosecutor, ISP, and the content provider can appeal the court order to block within eight days of a decision being issued. The NMHH is the authority designated to manage the list of websites to be blocked based on court orders[38] (or the tax authority in case of illegal gambling), while the operation of the system is regulated by a decree of the NMHH, which enables the authority to oblige ISPs to block the unlawful content.[39] The list, referred to as KEHTA (Hungarian acronym for "central electronic database of decrees on inaccessibility"), went into effect on January 1, 2014 with the primary aim of fighting child po nography. However, the blacklist is not public, as only certain institutions have access, such as the courts, parliamentary committees, and the police. The NMHH refused to publish the number of blocked websites following a public data request in February 2016.[40]

Online gambling is considered illegal if the tax authority has not authorized the operation of the

31 "Hungarian court blocks Holocaus denial websites," *Times of Israel*, September 1, 2016, http://www.timesofisrael.com hungarian-court-blocks-holocaust-denial-websites/.

32 For more about Kuruc.info and attempts to close it down see Borbala Toth,"Online hate speech – Hungary," 2014, 6–7, http://bit.ly/1BO6iIT.

33 "Court orders Holocaust denying article on far-right website to be blocked," *Hungary Today*, January 14, 2015, http://bit.ly/153Rs1J.

34 Gábor Polyák, "Végképp eltörölni – Adatszűrés és blokkolás a Magyar jogban," [Erasure – Data fil ering and blocking in the Hungarian jurisdiction] *Hvg.hu*, May 17, 2013, http://bit.ly/1BO61W8.

35 "Elérhetetlenné tenné a kuruc.info holokamu oldalát az ügyészség," [Prosecution would make the holo-lie page of kuruc.info inaccessible] *Hvg.hu*, May 27, 2015, http://bit.ly/1BVUK18.

36 Act C of 2012, art. 77.

37 Act XXXVIII of 1996 on International Assistance in Criminal Matters, art. 60/H.

38 Act C of 2003 on electronic communication, art. 10, par. 28., art. 159/B.

39 19/2013. (X.29.) NMHH az egyszerű adatátvitelt és hozzáférést biztosító elektronikus hírközlési szolgáltatók és a kereső- és gyorsítótár-szolgáltatók központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisához való kapcsolódásának és a Nemzeti Média- és Hírközlési Hatósággal való elektronikus kapcsolattartás szabályairól szóló 19/2013 (X.29.) NMHH decree.

40 Fővárosi Törvényszék 36.P.21.366/2016/3., June 7, 2016.

website.[41] ISPs had blocked 63 gambling websites as of March 2016;[42] however, gambling websites have been known to change their URLs in order to circumvent blocking.[43]

Content Removal

Though the law in Hungary generally protects against intermediary liability for content posted by third parties, in some cases courts in Hungary have held individuals responsible for comments posted by third parties on their pages and websites. In early 2016, László Toroczkai, far-right politician and mayor of Ásotthalom, was held liable by a court for "disseminating" defamatory comments posted by another person on his Facebook page. The court found that, by allowing commenting on his page, Torockai had accepted responsibility for any unlawful content posted by others.[44] The comments said a journalist "should be hanged."

In June 2015, a popular news website, 444.hu, was held liable for publishing a hyperlink to a YouTube video which undermined the reputation of Jobbik, a far right party.[45] The court found that by publishing the hyperlink, 444.hu had assumed liability for the defamatory content contained in the YouTube video. The case will be considered before the European Court of Human Rights in 2017.[46]

In February 2016, the European Court of Human Rights ruled in favor of a Hungarian website administrator (Index.hu ZRT) and a self-regulatory body of content service providers (Magyar Tartalomszolgáltatók Egyesülete), contradicting previous judgements issued by Hungarian courts.[47] The applicants appealed to the ECtHR after both the Hungarian Supreme Court and Constitutional Court found that, by enabling comments on their websites, the applicants were liable for any damage caused by content posted by third parties, including defamation.[48] The ECtHR found that that the Hungarian courts had failed to properly balance the right to reputation and the right to freedom on the press, a decision which could influence futu e defamation proceedings in Hungary.

According to Hungarian legislation, intermediaries are not otherwise legally responsible for transmitted content if they did not initiate or select the receiver of the transmission, or select or modify the transmitted information.[49] Intermediaries are also not obliged to verify the content they transmit, store, or make available, nor do they need to search for unlawful activity.[50] Hosting providers are required to make data inaccessible, either temporarily or permanently, once they receive a court order stating that the hosted content is illegal.[51]

Nevertheless, the 2010 media laws contain several general content regulation provisions concerning online media outlets, particularly if these outlets provide services for a profit. For example, both print

41 Act XXXIV of 1991 on Gambling, art. 36/g.

42 The list of the National Tax and Customs Administration can be accessed at: http://bit.ly/1OxJ35p.

43 Ajándok Gyenis, "A NAV blokkol, de hiába," [The tax authority is blocking in vain] *Hvg.hu*, July 29, 2014, http://bit.ly/1BbkSdu.

44 "Facebook-perek sora kezdődhet a súlyos joghézag miatt" [Many Facebook-related lawsuits may be initiated due to legal loophole], *mno.hu*, February 3, 2016, http://bit.ly/2esv9cD.

45 Pfv.IV.20.011/2015/3, June 10, 2015.

46 Magyar Jeti Zrt. v. Hungary, Application no. 11257/16. Many prominent internet stakeholders intervened in the case, such as Mozilla or Buzzfeed: http://hudoc.echr.coe.int/eng?i=001-164079.

47 Magyar Tartalmoszolgáltatók Egyesülete and Index.hu Zrt. v. Hungary, (application no. 22947/13).

48 Pfv.IV.20.217/2012/5, June 13, 2012.

49 Act CVIII of 2001 on Electronic Commerce, art. 8, par. 1.

50 Act CVIII of 2001, art. 7. par. 3.

51 Act CVIII of 2001, art. 12/A, Act XIX of 1998 on criminal proceedings, art. 158/B-158/D.

and online media outlets bear editorial responsibility if their aim is to distribute content to the public for "information, entertainment or training purposes," but that editorial responsibility "does not necessarily imply legal liability in relation to printed press materials."[52] The law fails to clarify what editorial responsibility entails and whether it would imply legal liability for online publications. A member of the Media Council said that the provision could apply to a blog if the blog were produced for a living.[53] According to László Bodolai, a lawyer for the news outlet Index.hu and a media law expert, based on a 2015 court decision, bloggers cannot legally be forced to amend or correct content with which someone disagrees, though they may be subject to lawsuits and damages.[54]

The 2010 media laws stipulate that media content—both online and offline—may not offend, discriminate or "incite hatred against persons, nations, communities, national, ethnic, linguistic and other minorities or any majority as well as any church or religious groups."[55] Further, the law states that constitutional order and human rights must be respected, and that public morals cannot be violated.[56] However, the law does not define the meaning of "any majority" or "public morals." If a media outlet does not comply with the law, the Media Council may oblige it to "discontinue its unlawful conduct," publish a notice of the resolution on its front page, and/or pay a fine of up to HUF 25 million (approximately $93,000).[57] If a site repeatedly violates the stipulations of the media regulation, ISPs can be obliged to suspend the site's given domain, and as a last resort, the media authority can delete the site from the administrative registry.[58] Any such action can be appealed in court, although a 2011 overhaul of the judiciary called into question the independence of the court system (see Legal Environment).[59]

Media, Diversity, and Content Manipulation

The online media environment in Hungary is relatively diverse, though independent outlets face increasing economic and political pressure. In October 2016, Hungary's leading opposition newspaper and online news portal, *Népszabadság* (People's Freedom), abruptly shut down. Though the owner said it was a business decision, journalists and non-governmental organizations (NGOs) regard the move as a consequence of political pressure, particularly because it followed the publication of several highly critical articles exposing government corruption and misuse of state funds by ministers.

In a 2015 survey, journalists told the Mérték Media Monitor that they experience persistent political and economic pressure to self-censor.[60] Hungarian journalists were cynical about the state of freedom of expression in another recent survey, with 50 percent of respondents reporting they had experienced political pressure in their everyday work.[61] Nine out of ten respondents said they felt that political pressure on the media is very strong.

52 Act CIV of 2010, art. 1, par. 6.

53 "Tanácsnokok és bloggerek," [Members and bloggers] *Mediatanacs-blo*g, January 11, 2011, http://bit.ly/1P33k8F.

54 László Bodolai, personal communication, March 2, 2015.

55 Act CIV of 2010, art. 17.

56 Act CIV of 2010, art. 16, and art. 4, par. 3.

57 Act CLXXXV of 2010, art. 186, par. 1, 187, par. 3. bf.

58 Act CLXXXV of 2010, art. 187, par. 3. e, 189, par. 4.

59 Zsófia Ge gely, "Megszólalnak a bírók: jobbelugrani a kényesügyelől", [The judges speak up: it is better to avoid politically sensitive cases], *Hvg.hu*, 1 March 2016, http://bit.ly/1QR84Ah.

60 Attila Mong, et al, "The Methods Are Old, the Cronies Are New, Soft Censorship in the Hungarian Media in 2015," p. 49-53 http://bit.ly/2e7d8AW.

61 Attila Mong, et al, "The Methods Are Old, the Cronies Are New, Soft Censorship in the Hungarian Media in 2015," p. 49-53 http://bit.ly/2e7d8AW.

Online media outlets that publish critical content are far less likely to attract revenue from state advertising or private companies owned by government-friendly oligarchs. As the Hungarian online advertisement market is not yet fully developed, this loss in revenue poses a significant th eat to the operations of critical online outlets. This pushes online media to stick with politically "safe" content and many outlets veer away from covering controversial topics such as corruption. [62]

In May 2015, the government allocated HUF 25 billion (US$88 million) for the advertisement of governmental activity,[63] which it has channeled to newly-established online media outlets, such as 888.hu, Faktor.hu, and Ripost.hu, among others. Some already existing news portals have also received funding to advertise governmental policies, such as anti-refugee propaganda. These websites generally lack commercial advertisements,[64] but operate with significant staff and p oduce government friendly content.[65] The prevalence and financial ad antage of these outlets has the effect of distorting the online media landscape. An example of the political nature of advertising allocation was seen in July 2013, when the manager of Stop.hu, a website close to the opposition Socialist party which posts content critical of the government, said they would reduce staff partly because businesses would not consider advertising on their site.[66]

The introduction of the advertisement tax, which media outlets pay based on their advertising revenues, is also a burden for some media outlets, particularly smaller online ventures.[67] In May 2015, the tax was converted from a progressive tax into a flat tax [68] as the European Commission started investigating whether the tax harms competition.[69]

Despite reports of self-censorship and challenges of maintaining financial viabilit , some online media outlets have become a tool to scrutinize public officials. For instance, sta ting in January 2012, Hvg.hu published a series of articles on how the then-president of the republic plagiarized his doctoral dissertation. Although he denied any wrongdoing, Pál Schmitt resigned in April 2012.[70] However, journalists have faced consequences in the past for publishing content critical of the government online. In June 2014, Gergo Saling, the editor-in-chief of the online media outlet Origo.hu, was dismissed following the publication of a series of articles critical of the government, including an article that revealed a possible abuse of public funds by the undersecretary of the prime minister, prompting speculation that the government pressured the publication to fi e the editor.[71] Saling sub-

62 Attila Bátorfy, journalist of Kreativ.hu, authored an in-depth analysis of public funds moving to private hands via media advertisements between 2010–2014: "Hogyan működött Orbán és Simicska médiabirodalma?" [How did the media empire of Orbán and Simicska work?] *Kreativ,* February 18, 2014, accessed March 7, 2015, http://bit.ly/1EZM9yM.

63 "Meglepő részletek a 25 milliárdos kormányzati pályázatban," [Surprising details of the 25 billion governmental tenders], *Hvg.hu*, May 2015, http://bit.ly/1QQM5mZ.

64 Attila Mong, et al, "The Methods Are Old, the Cronies Are New, Soft Censorship in the Hungarian Media in 2015," p. 49-53 http://bit.ly/2e7d8AW.

65 Based on a personal interview with journalist Pal Daniel Renyi on March 3, 2016.

66 "Leépítés a Stop.hu-nál," [Redundancies at Stop.hu] *Index*, July 4, 2013, http://bit.ly/1VIPlDY.

67 Act XXII of 2014 on the advertisement tax.

68 Pricewaterhouse Cooper, "Changing advertising tax rates," May 27, 2015, http://pwc.to/1MEwHKp.

69 European Commission, "State aid: Commission opens in-depth investigation into Hungarian advertisement tax," March 12, 2015, http://bit.ly/1b5b88P.

70 Palko Karasz, "Hungarian President Resigns Amid Plagiarism Scandal," *New York Times*, April 2, 2012, http://nyti.ms/1QdGyZ3.

71 Péter Erdélyi, Péter Magyari, Gergő Plankó,"Deutsche Telekom, Hungarian government collude to silence independent media," *444*, June 5, 2014, http://bit.ly/1hClHm6.

sequently founded an investigative journalism site called Direkt36 that publishes articles based on extensive investigations concerning corruption.[72]

Since 2011, the state-owned Hungarian News Agency (MTI) has had a virtual monopoly in the news market. MTI offers its news free of charge, making it difficult for other ac ors to compete. Many online media outlets that have been impacted by the economic crisis lack staff to produce original stories and tend to republish MTI news items. MTI is part of the system of public service broadcasting under the media authority. During the refugee crisis of 2015, public service media content was in line with the government's anti-refugee stance.[73]

Although MTI has a major effect on traditional and online content, the online media landscape is otherwise relatively diverse. Most civil society organizations have websites, and an increasing number of them have a presence on Facebook. Some media outlets, including online portals, represent the minority Roma community,[74] the LGBTI (lesbian, gay, bisexual, transgender, and intersex) community, and religious groups. Nevertheless, many news sources, although independent, often reflect the politically-divided nature of Hungarian society, and partisan journalism is widespread.

Blogs are generally considered an opinion genre and do not typically express independent or balanced news. There are also blogs analyzing governmental policies, the activities of public fi ures, and corruption. The comments sections of online articles are moderated, typically to prevent negative discussions. A survey conducted in 2011 among netizens indicated that 87 percent of the respondents encountered trolling on websites, but an overwhelming majority of the respondents considered commenting as a form of freedom of expression.[75]

Digital Activism

Social media platforms such as Facebook, which had almost 4.6 million users in Hungary as of March 2015, have grown increasingly popular as a tool for advocacy. In November 2015, the Hungarian Civil Liberties Union launched an online campaign after Tata resident Mária Somogyi was charged with libel for posting critical comments on Facebook questioning spending by the Tata council (see Prosecutions and Detentions for Online Activities).[76] The group started a crowdfunding campaign to assist Somogyi pay for the fines imposed and litigation costs, as ell as launching a broader online campaign, "Politikuss", which allows users to generate satirical memes depicting Hungarian politicians, in protest of the country's defamation and libel laws.[77]

Throughout the European immigration crisis, Hungarians increasingly used the internet to mobilize against the government's strict immigration policies and anti-refugee rhetoric. In June 2015, the Hungarian Two-Tailed Dog party launched an online crowdfunding campaign to counter the gov-

72 Anita Vorák, "Így kaptak Tiborczék szabad utat a milliárdokhoz", [This is how Tiborcz and his crew gained access to the billions], 444.hu, 11 March, 2015,http://bit.ly/1T67rmA.

73 Márton Kasnyik, "Neten terjedő kamufotóval kelt félelmet az állami tévé és az udvari napilap" [State television and government friendly newspaper mongers fear with a fake picture from the net], *444.hu*, September 8, 2015, http://bit.ly/21Tyc2P.

74 Borbala Toth, "Minorities in the Hungarian media. Campaigns, projects and programmes for integration" (Center for Independent Journalism: Budapest, 2011): 19.

75 Magyarországi Tartalomszolgáltatók Egyesülete (MTE), "Kommentek megítélése. Elemzés," [Judgement of comments Analysis] 2012, 3 and 81, http://bit.ly/1GAkrXi.

76 Hungarian Civil Liberties Union, "Help Maria Somogyi!" http://tasz.hu/somogyimaria.

77 Marietta Le, "Hungarian woman fined for acebook post about state spending," *Global* Voices, November 6, 2015, https://globalvoices.org/2015/11/06/hungarian-woman-fined-fo -facebook-post-about-state-spending/.

ernment's anti-immigration billboards displayed around the country.[78] The campaign gained popular support, raising over $100,000. In July 2015, the campaigners put up spoof billboards containing messages such as, "Sorry about our Prime Minister!"[79]

In May 2015, the Hungarian Helsinki Committee NGO launched a campaign in response to xenophobic language in surveys relating to migration which the government distributed to millions of residents. The group started a Tumblr blog to highlight the bias behind the survey and provide a platform for Hungarian citizens to share their own migration stories.[80]

Since the 2010 parliamentary elections, several large demonstrations have been organized through Facebook, mobilizing tens of thousands of people.[81] In 2014, online campaigns drew thousands of people to protest against the introduction of a tax on internet use.[82] Due to the overwhelming demonstrations, the government decided to withdraw the planned tax.[83]

Violations of User Rights

The right to freedom of expression is protected in the Fundamental Law of Hungary, and the government does not generally prosecute individuals for posting controversial political or social content online. However, the law includes criminal penalties for defamation, and public officials occasionally initiate defamation proceedings against individuals posting critical content on social media. Judicial oversight of surveillance by intelligence agencies continues to be a concern, and the government recently passed a law granting authorities access to encrypted communications.

Legal Environment

The Fundamental Law of Hungary acknowledges the right to freedom of expression and defends "freedom and diversity of the press,"[84] although there are no laws that specifically p otect online expression. In 2013, the Fundamental Law was amended to specify instances in which freedom of speech could be limited. Article 9.2 states that freedom of speech may not be exercised with the aim of violating the dignity of the Hungarian nation or of any national, ethnic, racial, or religious community. The amendment has been criticized for its overbroad scope and lack of clarity.[85]

The independence of the judiciary has come under question in the past, such as when the government essentially forced hundreds of judges into early retirement by lowering the retirement age.[86]

78 Marietta Le, "Hungarian Activists raise a boatload of cash to counter a government campaign," June 14, 2015, https://globalvoices.org/2015/06/14/hungarian-activists-raise-a-boatload-of-cash-to-counter-a-government-campaign/.

79 Paula Kennedy, "Posters mock Hungary anti-immigration drive," July 1, 2015, http://www.bbc.co.uk/monitoring/posters-mock-hungary-antiimmigration-drive.

80 "Hungary lays the xenophobic on thick in national questionnaire about immigration," *Global Voices,* May 29, 2015, https://globalvoices.org/2015/05/29/hungary-lays-the-xenophobia-on-thick-in-national-questionnaire-about-immigration/.

81 Walter Mayr, "Facebook generation fights Hungarian media la ," *Spiegel Online*, January 4, 2011, http://bit.ly/1LsDRi1.

82 Associated Press, "Hungarians march again in protest against internet tax plan," *The Guardian*, October 29, 2014, http://bit.ly/1tDiNAS

83 "Hungary internet tax cancelled after mass protests", *BBC*, October 31, 2014, http://bbc.in/1wPNKEs.

84 The Fundamental Law of Hungary (25 April 2011) art. VIII., 1–2.

85 Venice Commission, "Opinion on the Fourth Amendment to the Fundamental Law of Hungary," 17 June, 2013, http://bit.ly/1U8x0CD.

86 "European Commission launches accelerated infringement proceedings against Hungary over the independence of its central bank and data protection authorities as well as over measures affecting the judiciary" European Commission.

However, after a ruling by the CJEU, in 2013 the parliament changed the law to gradually reduce the retirement age over 10 years.[87]

The criminal code bans defamation, slander, the humiliation of national symbols (the anthem, flag, and coat of arms), the dissemination of totalitarian symbols (the swastika and red pentagram), the denial of the sins of National Socialism or communism, and public scare-mongering through the media.[88] Defamation cases have decreased since a 1994 Constitutional Court decision, which asserted that a public figu e's tolerance of criticism should be higher than an ordinary citizen's.[89] In February 2013, the Constitutional Court ruled the ban on using totalitarian symbols unconstitutional,[90] though the parliamentary majority decided to include it again in revisions to the penal code in April 2013.

Hungarian law does not distinguish between traditional and online media outlets in libel or defamation cases, and the criminal code stipulates that if slander is committed "before the public at large," it can be punished by imprisonment of up to one year.[91] On November 5, 2013, the criminal code was modified o include prison sentences for defamatory video or audio content. Anyone creating such a video can be punished by up to one year in prison, while anyone publishing such a recording can be punished by up to two years. If the video is published on a platform with a wide audience or causes significant ha m, the sentence can increase to up to three years in prison.[92] The amendment was condemned both by domestic and international actors for threatening freedom of expression and for targeting the media.[93] While libel and defamation are generally prosecuted by the victim, in cases where a public official brings the cha ge, the state will provide a public prosecutor. In these cases, the defendant must go through an invasive registration process: his or her photograph and finge - prints are taken before the court procedure even begins.[94]

A new civil code, which took effect in March 2014, also protects citizens from defamation and insults to their honor,[95] and includes an indemnification fee for non-pecunia y damages caused by violating civil rights.[96] The code includes a provision that may limit the free discussion of public affairs in cases where the human dignity of a public figu e is violated.[97]

A series of amendments to the Freedom of Information (FOI) Act has imposed restrictions on the accessibility of public data. The latest amendment came into force in October 2015, imposing higher and potentially arbitrary fees for FOI requests, allowing denials for repeated FOI requests (even

87 "Megszavazták a bírák lassú nyugdíjba küldését," [The law on the slow retirement of judges was accepted] *Hvg.hu,* March 11, 2013, http://bit.ly/1PkOSbn.

88 Act C of 2012, art. 226, 227, 332–335.

89 Péter Bajomi-Lázár and Krisztina Kertész, "Media Self-Regulation Practices and Decriminalization of Defamation in Hungary," in *Freedom of Speech in South East Europe: Media Independence and Self-Regulation*, ed. Kashumov, Alexander (Sofia: Media Development Center, 2007): 177-183.

90 4/2013. (II. 21.) Constutional Court decision, "Constitutional Court voids ban on "symbols of tyranny"; red star, swastika to become legal on April 30," *Politics*, February 21, 2013, http://bit.ly/18eRl0o.

91 Act C of 2012, art. 227.

92 Act C of 2012, art. 226/A and 226/B.

93 Hungarian Civil Liberties Union, "Tightening of the Criminal Code is Unconstitutional," November 14, 2013, http://bit.ly/1P37c9M; OSCE, "Higher prison sentences for defamation may restrict media freedom in Hungary, warns OSCE representative," press release, November 6, 2013, http://www.osce.org/fom/107908; and Dalma Dojcsák, "New law further restricts freedom of speech and freedom of the press in Hungary," IFEX, November 18, 2013, http://bit.ly/1N3dSRT.

94 Threat of prosecution for defamation has chilling effect says HCLU, *The Budapest Beacon*, November 3, 2015, http://bit.ly/1niXX9D.

95 Act V of 2013 on the Civil Code, art. 2:45.

96 Act V of 2013 on the Civil Code, art. 2:52–53.

97 Bill Nr. T/7971, art. 2:44.

where previous requests received no response), and allowing public bodies to refuse to make certain information public where that information is deemed to have been used in decision-making processes. Critics say these amendments are part of a wider trend of restricting public access to information.[98]

Prosecutions and Detentions for Online Activities

During the coverage period, there were no instances of detentions for online activities. However, public officials ha e been known to initiate civil and criminal procedures against ordinary citizens for their activity online, including commenting, authoring blog pieces, or even sharing content on social media. Authorities are effectively punishing citizens for their political engagement online, a trend which is likely to cause a chilling effect on critical discussions and mobilization on social media.[99]

- In June 2016, the Supreme Court of Hungary upheld the decision of a lower court which found that a Facebook user, Mária Somogyi, had violated the personality rights of Tata town council. Somogyi had shared and commented a post that claimed the council was misusing public funds.[100]

- In November, 2015, the then-mayor of the Hungarian town of Siófok initiated criminal proceedings against 17 Facebook users after they shared a post about suspicious real estate deals in their town involving the mayor.[101] In June 2016, the first instance court found that no crime was committed and terminated the criminal procedure. The former mayor has appealed the decision.[102]

- In November 2014, András Vágvölgyi said on his Facebook page he had once been detained at the same time as President János Áderduring during his compulsory military service. Index.hu shared the story but said it was probably untrue.[103] Both Vágvölgyi and Index.hu were found liable for violating the personality rights of Áder and were ordered to pay an indemnification fee f 600,000 HUF (US$2,100).[104] In September 2016, the Supreme Court reduced the indemnification fee o 50 000 HUF (US$180).

Surveillance, Privacy, and Anonymity

The lack of judicial oversight for surveillance of ICTs, combined with evidence revealing that the Hungarian government has purchased invasive surveillance technologies from Hacking Team and other companies, raises concerns about the degree to which the right to privacy online is fully protected.

98 Transparency International Hungary, "Transparency international turns to higher authorities," July 3, 2013, http://bit.ly/1Opd8tD.

99 "Criticism of Public Officials Is a Right and a Duty!" Libe ties.eu, 10 November, 2015, http://bit.ly/1L6n5vN.

100 She can pay 85 thousand for a Facebook share, 3 November, Index.hu, 2015, http://bit.ly/1poPBPy

101 László Szily, "Sima Facebook-megosztásért hallgattak ki és rabosítottak 17 embert Diófokon" [17 people interrogated and fingerprin ed for a Facebook share], *444.hu*, November 27, 2015, http://bit.ly/2cYf4Mx.

102 Imre Fónai, "Facebook-per:a siófoki expolgármester nem hagyja annyiban" [Facebook trial: Siófok ex-Mayor will not give up], *sonline.hu*, June 23, 2016, http://bit.ly/2dz6t3C.

103 Szabolcs Panyi, "We have a jail acquaintance with János Áder," [Mi egy börtönkapcsolat vagyunk Áder Jánossal], 1 December, 2014, *Index.hu*, http://bit.ly/1QVmBLf.

104 Szabolcs Dull, "János Áder won against Index", [Áder János pert nyert az Index ellen], 8 December, 2015, *Index.hu*, http://bit.ly/24DpjJF.

In July 2016, new antiterrorism legislation sought to expand the authorities' access to encrypted content online. The legislation amends the Online Trade Services and Services Connected to the Information Society Act, obligating providers of encrypted services, including messaging platforms, to grant authorized intelligence agencies access to the communications of their clients upon request, unless the communication is encrypted end-to-end, making compliance impossible. Providers of encrypted services must store their clients' messages and metadata for up to one year.[105] The legislation reveals the authorities' intent to undermine encryption, though it's not clear how it will be enforced.

ISPs and mobile phone companies in Hungary must also retain user data for up to one year to provide to investigative authorities and security services on request, including personal data, location information, phone numbers, the duration of phone conversations, IP addresses, and user IDs.[106] There is no data on the extent of these activities, even though there is a legal obligation to provide the European Commission with statistics on the data queries made by investigating authorities.[107] Electronic communications service providers are also obligated to "cooperate with organizations authorized to perform intelligence information gathering and covert acquisition of data."[108] Additionally, the Electronic Communications Act states that "the service provider shall, upon the written request from the National Security Special Service, agree with the National Security Special Service about the conditions of the use of tools and methods for the covert acquisition of information and covert acquisition of data."[109]

In October 2014, the Hungarian Civil Liberties Union launched litigation against two of the major mobile phone providers in an attempt to force the Hungarian Constitutional Court to annul data retention requirements.[110] The Constitutional Court declined to hear the case on procedural grounds, and the HCLU has initiated an appeal.

National security services can gather metadata "from telecommunications systems and other data storage devices" without a warrant.[111] Security agents can access and record the content of communications transmitted via ICTs, though a warrant is required.[112] Privacy experts say the authorities have installed black boxes allowing them direct access to ISP networks.[113] There is no data on the extent to which, or how regularly, the authorities monitor ICTs.

In June 2012, staff members of the Budapest-based watchdog Eötvös Károly Institute (EKINT) asked the Constitutional Court to annul a legal provision that allows the justice minister to oversee the

105 Hungarian Civil Liberties Union, "Hungarian parliament about to enact new anti-terror laws," May 3, 2016, http://tasz.hu/en/news/hungarian-parliament-about-enact-new-anti-terror-laws.

106 Act C of 2003, art. 159/A; "Hungary – Privacy Profile" Privacy International, January 22, 2011.

107 Act C of 2003, art. 159/A, par. 7.

108 Act C of 2003, art. 92, par. 1. Electronic service providers provide electronic communications service, which means a "service normally provided against remuneration, which consists wholly or mainly in the conveyance, and if applicable routing of signals on electronic communications networks, but exclude services providing or exercising editorial control over the content transmitted using electronic communications network; it does not include information society services, defined under se arate legislation, which do not consist primarily in the conveyance of signals on electronic communications networks," Act C of 2003, art. 188, par. 13.

109 Act C of 2003, art. 92, par. 2.

110 Hungarian Civil Liberties Union, "HCLU litigates Hungarian service providers to terminate data retention," news release, October 13, 2014, accessed March 7, 2015, http://bit.ly/1A3Upr6

111 Act CXXV of 1995 on the National Security Services, Art. 54, http://bit.ly/1bhE9cm.

112 Act CXXV of 1995, art. 56.

113 "Hungary – Privacy Profile" Privacy International, January 22, 2011.

work of the Counter Terrorism Center to approve the secret surveillance of individuals,[114] saying that surveillance should be approved by a judge rather than a minister.[115] The Constitutional Court rejected the complaint, and EKINT addressed the same complaint to the European Court of Human Rights in May 2014. The application was joined by the U.K.-based Privacy International and the U.S.-based Center for Democracy and Technology.[116] In January 2016, the Court decided in the favor of the applicants and found that the Hungarian law on surveillance is in violation of the European Convention on Human Rights.[117]

Reports indicate that the government may be abusing these surveillance powers to spy on local NGOs. In September 2015, Tivadar Hüttl, an attorney at the Hungarian Civil Liberties Union, was speaking by telephone with Benedek Jávor, a member of the European Parliament, when the line disconnected, after which Jávor reported hearing their conversation played back. Ministers overseeing the secret services said no illegal surveillance took place.[118] In June 2016, Eötvös Károly Intézet reported finding a su veillance device on computer equipment in their office. The Go ernment denied any link to the device. In July, the public prosecutor ordered an investigation.[119]

Several privacy and digital rights organizations say the Hungarian authorities have purchased potentially invasive surveillance technologies over the past few years. In July 2015, files lea ed from the Milan-based commercial spyware company Hacking Team revealed that the Hungarian government was a client.[120] In 2013, Privacy International reported that Hungarian law enforcement agencies are connected with at least one surveillance technology company,[121] and that several government agencies attended the ISS World surveillance trade shows over the years.[122] The University of Toronto-based Citizen Lab also reported finding a FinFisher Command and Cont ol server, which facilitates surveillance, in Hungary.[123] Though it is not clear whether the server is operated by the government or other actors, the software is marketed to governments.[124]

Generally, users who wish to comment on a web article need to register with the website by providing an email address and username, or they need to use a Facebook login. The operator of a website may be asked to provide the authorities with a commenter's IP address, email address, or other data in case of an investigation.[125] Additionally, users must provide personal data upon purchase of a SIM card to sign a contract with a mobile phone company.[126] Encryption software is freely available

114 Act CXXV of 1995, art. 58, par. 2. states that in some instances – including the tasks of the Counter Terrorism Center – the minister for justice can grant the warrant.

115 The complaint can be downloaded at: http://ekint.org/ekint_files/File/constitutionalcomplaint_ek.pdf.

116 Eötvös Károly Policy Institute, "Szabo and Vissy v. Hungary: No secret surveillance without judicial warrant," http://bit.ly/1Bh3uhu;

117 Szabó and Vissy v. Hungary, Application no, 37138/14., 14 January 2016.

118 József Spirk, "Egy ügyvédet lehallgattak, a többiek csak a jeleit észlelték" [Attorney tapped, others suspect the same], *index.hu* April 21, 2016, http://bit.ly/2drjUk8.

119 Viktória Serdült, "Prosecutor orders investigation into surveillance bug found in NGO office" *The Budapest Beacon*, July 14, 2016, http://bit.ly/2cOhJoE.

120 Alex Hern, "Hacking Team hack casts spotlight on murky world of state surveillance", *The Guardian*, July 11, 2015, http://bit.ly/2efzrIq.

121 Privacy International "Surveillance Industry Index," November 18, 2013, https://www.privacyinternational.org/node/403.

122 "Surveillance Who's who," Privacy International.

123 Tamás Bodoky, "Nem cask az USA szeme látmindent: kormányzati kémprogram Magyarországon," [Not only USA can see everything: governmental surveillance software in Hungary] *atlatszo.hu*, September 16, 2013, http://bit.ly/1FWperq.

124 Morgan Marquis-Boireet. al. "For their eyes only: The Commercialization of Digital Spying," Citizen Lab, September 16, 2013, http://bit.ly/1pCA0Y4.

125 Act XIX of 1998 on criminal proceedings, art. 178/A, par. 1.

126 Act C of 2003 on Electronic Communications, art. 129, http://bit.ly/1R2nc9u.

without government interference; Pretty Good Privacy (PGP), a data encryption program, is used by investigative journalists.[127]

Intimidation and Violence

Bloggers, ordinary ICT users, websites, or users' property are not generally subject to extralegal intimidation or physical violence by state authorities or any other actors.

Technical Attacks

There were no significant cyberattacks against NGO ebsites or news outlets during the coverage period. In the past, technical attacks in Hungary have been primarily perpetrated by non-state actors against government websites, particularly by the international group Anonymous. For instance, in 2012 the group rewrote the text of the fundamental law on the website of the Constitutional Court, and several sites suffered from distributed denial-of-service (DDoS) attacks during that time.[128]

127 Borbala Toth, *Mapping Digital Media: Hungary,* Open Society Foundations, February 2012, 50, http://osf.to/1LDDurj.

128 Máté Nyusztay, "'A rendszert támadjuk' – Magyarország is az Anonymous célkeresztjében," ['We attack the system' – Hungary is among the targets of Anonymous] *Nol*, February 15, 2012, http://bit.ly/1MnHW9k.

Freedom House

Iceland

	2015	2016
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	1	1
Limits on Content (0-35)	1	1
Violations of User Rights (0-40)	4	4
TOTAL* (0-100)	**6**	**6**

* 0=most free, 100=least free

Population:	**330,800**
Internet Penetration 2015 (ITU):	**98 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2016 Status:	**Free**

Key Developments: June 2015 – May 2016

- Iceland continues to have one of the highest rates of internet access in the world, with an internet penetration rate of 98 percent in 2015 (see **Availability and Ease of Access**).
- In 2015 and 2016, the activist hacker group Anonymous attacked Icelandic government websites to protest against commercial whaling (see **Technical Attacks**).

Introduction

Iceland has one of the highest rates of internet and social media usage in the world, according to the World Economic Forum.[1] There was no change in the internet freedom environment in 2016.

Internet and digital media play a vital role in Icelandic society, and Iceland is an international leader when it comes to promoting free speech. In 2010, the Icelandic parliament launched a new media initiative protecting free speech, aiming to make Iceland a safe haven for journalists and whistleblowers.[2] Following in the wake of the country's financia collapse in 2008, social media platforms such as Facebook were integrated into the process of creating a new constitution.[3] The "crowdsourced constitution" process continued in 2015 and 2016.[4]

On April 5, 2016, Prime Minister Sigmundur Davíd Gunnlaugsson stepped down from his post under growing public and political pressure after leaked documents known as the Panama Papers revealed his links to undisclosed offshore assets. The papers, leaked from the Panamanian law fi m Mossack Fonseca and published by the International Consortium of Investigative Journalists, identifie shareholders of thousands of offshore companies, which have been linked to tax evasion. Two days later, he was replaced by Sigurdur Ingi Johannssón from the same Progressive Party.[5]

In early 2016, polls showed that the Pirate Party, which supports online freedom, could become the largest in parliament in the parliamentary elections scheduled for October.[6] In early 2015, a series of bills primarily submitted by the Pirate Party failed to pass in parliament.[7] The bills sought to address data retention and whistleblower protection, among other issues.

Obstacles to Access

Iceland is one of the most connected countries in the world, with the highest percentage of households with access to the internet in Europe. There are very few obstacles to accessing the internet; however, the ICT regulatory agency's ability to address concerns about concentration in the market has been limited. In 2013, the government passed legislation to address this issue, allowing the Competition Authority some oversight powers with regard to regulating media concentration.

Availability and Ease of Access

According to the International Telecommunication Union (ITU), Iceland had an internet penetration rate of 98 percent in 2015, compared to 97 percent in 2013 and 93 percent in 2009,[8] with only a minimal difference in usage between the capital region and other regions of the country, or between

1 World Economic Forum, *The Global Information Technology Report 2015*, bit.ly/1yutYRc.

2 International Modern Media Institute (IMMI), https://immi.is/.

3 Robert Robertson, "Voters in Iceland back new constitution, more resource control," *Reuters*, October 21, 2012, http://reut.rs/Myiq8g

4 Email interview with employee at the Legislative Department at the Offic of the Prime Minister, March 3, 2016.

5 Charles Duxbury et al., Iceland's Prime Minister Sigmundur David Gunnlaugsson steps aside after release of 'Panama Papers', *The Wall Street Journal*, April 6, 2016, http://on.wsj.com/1RWC4bo.

6 Anna Margrét Björnsson, "Almost Half of Icelandic Nation now wants the Pirate Party", *Iceland Monitor*, May 3 2016, http://bit.ly/1PTk2T9. Despite gains, the Pirate Party won 14.5 percent of the vote on October 29, 2016. http://bit.ly/2enSzPa

7 Email interview with member of the Icelandic Media Commission, January 14, 2016.

8 International Telecommunication Union, "Percentage of individuals using the internet," 2015, 2013 & 2008, http://bit.ly/1cblxxY.

women and men.[9] This is the highest percentage of internet users of all European countries; the average household internet penetration rate within the European Union was 81 percent in 2014.[10]

Broadband connections were put into operation in 1998, and by 2006, slightly less than 90 percent of Icelandic households had internet access. The percentage of households with high speed internet connections, such as ADSL or SDSL, has increased greatly in recent years.[11] In 2007, the Icelandic city of Seltjarnes became the fi st municipality in the world where every citizen has access to fibe -optic internet service.[12] In 2015, the vast majority of the population was connected via broadband (73 percent), while a growing number connected via fibe -optic cable (26 percent).[13]

In addition, 82 percent of Icelanders had access to the internet via a mobile connection in 2014.[14] Mobile penetration was 114 percent in 2015, according to the ITU.[15] More than half of internet subscriptions (54 percent) have speeds of 50 to 100 Megabits per second (Mbps), and almost a quarter are 100 Mbps or faster (23 percent).[16]

Accessing the internet via computers and mobile phones is very affordable: a basic internet subscription with 5 GB of data costs around ISK 3,750 per month (US$29), and a basic mobile phone connection with 500 Mb of data costs around ISK 690 per month (US$36).[17] The average monthly salary is approximately ISK 555,000 (US$4,310).[18]

With near ubiquitous access, Icelanders are frequent internet users, with 95 percent connecting to the internet daily or almost daily, and 99 percent connecting every week in 2014.[19] Furthermore, 84 percent of individuals used social networks, 95 percent read news online, 95 percent sent or received emails, 36 percent stored electronic content online, and 66 percent used internet commerce.[20]

Restrictions on Connectivity

There are no government-imposed restrictions on connectivity in Iceland. The country has been connected to the internet via the NORDUnet network in Denmark since 1989. The following year, a leased line to NORDUnet in Sweden was established, and the link was gradually upgraded. The Nordic connection was supplemented in 1997, when ISnet established a direct connection to Teleglobe in Canada, which was upgraded when the line was moved to New York in 1999.[21]

Iceland has multiple channels connecting the country to the international internet, including connections to the international backbone through three submarine cables: FARICE-1, DANICE, and Green-

9 Statistics Iceland, " Statistical Yearbook of Iceland 2015", http://bit.ly/1QUsztW

10 Statistics Iceland, http://www.statice.is; Eurostat, "Digital economy and society statistics - households and individuals," June 2015, http://bit.ly/2fLwU7D

11 Birgir Gudmondsson, "Media Landscapes – Iceland," European Journalism Centre, 2010, http://bit.ly/1zkzQg5.

12 Idega, "Seltjarnes," http://bit.ly/1JGg0zu.

13 Post and Telecom Administration, "Statistics on the Icelandic Electronic Communications Market for the First Half of 2015," http://bit.ly/1nKMrUO.

14 Statistics Iceland, " Statistical Yearbook of Iceland 2015," http://bit.ly/1QUsztW.

15 International Telecommunication Union, "Mobile-cellular subscriptions," http://bit.ly/1cblxxY.

16 Post and Telecom Administration, "Statistics on the Icelandic Electronic Communications Market for the First Half of 2015."

17 Síminn Iceland, http://bit.ly/1c3gke0 and http://bit.ly/1rjhFSU.

18 Statistics Iceland, " Statistical Yearbook of Iceland 2015," http://bit.ly/1QUsztW.

19 Statistics Iceland, " Statistical Yearbook of Iceland 2015," http://bit.ly/1QUsztW .

20 Statistics Iceland, " Statistical Yearbook of Iceland 2015," http://bit.ly/1QUsztW.

21 Cathy Newman, "Iceland Internet Diffusion," http://bit.ly/1QxYiP9.

land Connect. The Reykjavik Internet Exchange Point (IXP), which exchanges internet traffi among internet service providers (ISPs) located in Iceland, is operated independently of the government by the top-level domain registry ISNIC.

ICT Market

Iceland's ICT market is competitive and relatively diverse. Síminn is the main internet and telecommunications operator in Iceland and runs fi ed-line and mobile voice call services, as well as internet services and broadband television. Síminn is based on a merger between Landssími Íslands, which was privatized in 2005, and the company Skipti ehf. The companies Tal and 365 merged under the banner of 365 in July 2014.[22] Of all the ISPs, Síminn holds the largest market share (49 percent), followed by Vodafone (28.4 percent), 365 (13.6 percent), and Hringdu (4.9 percent), with the remaining companies comprising 4.2 percent. Regarding market share in mobile broadband, Síminn leads slightly with the largest market share (35.3 percent), followed by Nova (33.4 percent), Vodafone (26.8 percent), and 365 (3.7 percent).[23]

Regulatory Bodies

The main regulatory body governing information and communication technologies (ICTs) in Iceland is the Post and Telecom Administration (PTA), an independent center under the direction of the Ministry of the Interior. The Ministry is responsible for the legal matters relating to online content.

The PTA supervises development, logistics, and fair competition in the fiel of telecommunications networks. Decisions of the PTA may be referred to the Rulings Committee for Electronic Communications and Postal Affairs. The Rulings Committee consists of three persons appointed by the Minister of Transport and Communication. The chairman and vice chairman must comply with the competence qualification applying to Supreme Court judges. Committee members are appointed for a period of four years.[24]

A new media law established on September 1, 2011 stirred debate in subsequent years.[25] While the intention of the law was to create greater press freedom through a comprehensive framework governing broadcast, press, and online media, it also established an oversight body, the Media Commission, which prompted discussion of possible government influenc over the press. According to the law, the Minister of Education, Science and Culture appoints fi e people to the Media Commission for terms of four years at a time. Two representatives are appointed in accordance with a nomination by the Supreme Court, one in accordance with a nomination by the standing Committee of Rectors of Icelandic Higher Education Institutions, and one in accordance with a nomination by the National Union of Icelandic Journalists. The fi th member is appointed by the minister without an outside nomination.[26]

The Media Commission has no authority to deal with media concentration issues (a major topic of public debate in Iceland), but legislation passed as an amendment to the media law in March 2013

22 Fanney Birna Jónsdóttir, "365 og Tal ræda sameiningu," *Visir*, July 22, 2014, http://bit.ly/22hYNTR.

23 The Post and Telecom Administration, "Statistics on the Icelandic Electronic Communications Market for the First Half of 2015," http://bit.ly/1nKMrUO.

24 The Post and Telecom Administration, "Rulings Committee," [in Icelandic] http://www.pfs.is/Default.aspx?cat_id=146.

25 Email interview with former employee at the Icelandic Media Commission, Jan 29, 2014.

26 Fjolmidlanefnd, "The Media Commission," http://fjolmidlanefnd.is/english/.

gave another government agency, the Icelandic Competition Authority, oversight of competition cases when media companies are concerned, in consultation with the Media Commission. Thus, the Competition Authority can look at issues such as plurality and whether there will be a decrease in newsrooms resulting from mergers and acquisitions, for example. According to the bill, the Media Commission shall in such cases give its opinion from a media authority's perspective.[27]

In July 2014, the Prime Minister appointed a working group to review the laws, regulations and administrations of regulatory authorities and evaluate how principles of good regulations and practices are met. In 2014, the Minister for Education, Science and Culture appointed a consulting group to research the feasibility of the merger of four regulatory authorities: the Media Commission, the Post and Telecom Administration, the Icelandic Competition Authority, and the monitoring part of the National Energy Authority. The research concluded with a positive assessment from the consulting group that was presented in government, however, the possible merger has been stalled since the presentation of the report.[28]

Limits on Content

Access to information and online communication is generally free from government interference. Iceland is not a member of the European Union, although the country is part of the European Economic Area and has agreed to follow legislation regarding consumer protection and business law similar to other member states.[29] In February 2016, the committee for the crowdsourced constitution publicly issued three draft bills for public comment

Blocking and Filtering

Political, social, and religious websites are not blocked in Iceland. Social media platforms such as YouTube, Facebook, Twitter, and international blog hosting services are freely available and are used by a large part of the population.

Similar to other Nordic countries, ISPs in Iceland fil er websites containing child pornography. The ISPs collaborate with the Icelandic Save the Children (called Barnaheill) and participate in the International Association of Internet Hotlines (INHOPE) project which solicits reports of illegal content[30] In addition, pornography in general is illegal in Iceland, although the ban is not strongly enforced, and online pornography is not blocked.

In October 2014, the Reykjavík District Court ordered two ISPs (Hringdu and Vodafone) to block the file-sharin website The Pirate Bay and the largest private Icelandic torrent website, Deildu.[31] The court order came after the music rights group STEF and the motion picture association SMAIS reported the torrent websites to police in 2013 due to copyright infringement, since much on the content on these sites is pirated material. In May 2014, the Supreme Court declared that only STEF could seek the injunction. In September 2015, a local news outlet reported that all major ISPs in Iceland had agreed to block access to the sites following the court order, but that proxy servers to circum-

27 Fjolmidlanefnd, "The Media Commission."
28 Email interview member of the Media Commission, January 14, 2016.
29 OpenNet Initiative, "Nordic Countries," https://opennet.net/research/regions/nordic-countries.
30 INHOPE, http://www.inhope.org.
31 Reuters, "Iceland court orders Vodafone to block Pirate Bay," *RT*, October 17, 2014, http://bit.ly/1El2WIc.

vent the block were widely available. Ásta Gudrún Helgadóttir, a member of parliament for the Pirate Party, criticized the ban as internet censorship.[32]

Prior to the blocking, in April 2013, The Pirate Bay website had relocated from Sweden to Iceland and acquired an ".is" domain name, after the Swedish authorities attempted to seize its domains. Within a week of the move, however, the site chose to relocate again outside of Iceland, even though ISNIC stated it had no intention of trying to seize the domain.[33] According to Icelandic law, the registrant is responsible for ensuring that the use of the domain is within the limits of the law.[34]

In 2013, then-Minister of the Interior Ögmundur Jónasson proposed two new bills in an effort to uphold and reinvigorate an existing law banning pornography and gambling online that is vaguely worded and rarely enforced. The ban focused on making it illegal to pay for pornographic material with Icelandic credit cards, in addition to creating a national internet fil er and a blacklist of websites that contain pornographic content.[35] Opponents led by Icelandic member of parliament and free speech activist, Birgitta Jónsdóttir, deemed that the ban would limit free speech online, a position that was supported by academics and free speech advocates from outside Iceland.[36] The plan for banning pornographic content online has been stalled since the change in government after the parliamentary election on April 27, 2013. Since then, there have been no changes to the relevant legislation, and no changes have been formally proposed.[37]

Content Removal

There were no problematic incidents of content removal during the coverage period of this report.

Icelandic law number 30/2002 establishes a system of takedown notices for IP addresses or other online content that violates the law, in accordance with the Directive 2000/31/EC of the European Parliament. The Ministry of the Interior is responsible for handling matters related to online content, and the appeals process for disputing the removal of content goes through the independent courts in Iceland.

ISPs and content hosts are not held legally liable for the content that they host or transmit. Claims regarding intellectual property rights are handled by the Icelandic Patent Office which is dependent on international cooperation, and Iceland is party to a number of international agreements in this field Moreover, as a member of the World Trade Organization (WTO), Iceland has adapted legislation to the provisions of TRIPS (Trade-Related Aspects of Intellectual Property Rights). Furthermore, the Agreement on the European Economic Area has led to several legislative amendments in Iceland that align with the directives and regulations of the European Union.

In October 2014, the domain hosting company ISNIC, which operates the Icelandic .is domain, was forced to shut down a website for the fi st time when it discovered that the domain was being used by the self-described Islamic State terrorist group.[38] The ISNIC board made the decision based on regulations holding the registrar responsible for ensuring that the use of the .is domain does not vi-

32 Paul Fontaine, "Icelandic ISPs will block Access to Pirate Bay and Deildu", *Reykjavik Grapevine,* September 16, 2015, bit.ly/1pIqYgE.
33 Stan Schroeder, "The Pirate Bay Moves to the Caribbean," *Mashable*, May 1, 2013, http://on.mash.to/1VULcwP.
34 ISNIC, "Domain Rules," https://www.isnic.is/en/domain/rules.
35 "Banning the Sex Industry - Naked Ambition," *The Economist,* April 20, 2013, http://econ.st/12q1wwM.
36 "Iceland's Porn Ban Effort Draw Fire from Abroad," *IceNews*, March 17, 2013, http://bit.ly/1lFHkD2.
37 Email interview with member of the Icelandic Media Commission, January 14, 2016.
38 Eyglo Svala Arnarsdottir, "IS Terrorist Organization Picks Icelandic Domain," Iceland Review, October 13, 2014, http://bit.ly/1zzxjz3.

olate Icelandic laws. No similar incidents were reported during the coverage period of this report.

Media, Diversity, and Content Manipulation

Iceland has a vibrant digital sphere, and almost all traditional media, including print, radio, and television, offer versions of their content online. Self-censorship is not a widespread problem in Icelandic online media, and there are very few instances of government or partisan manipulation of online content.

The websites of some newspapers, like the daily *Morgunbladid*, are among the most popular Icelandic-language sites.[39] Internet banking is widely used, and a large majority of Icelanders (93 percent) are online bank users.[40] E-governance initiatives have been successful in Iceland, and in recent years, public institutions have started a migration process from proprietary to free and open software.[41] On January 1, 2015, the public administration in Iceland switched to eInvoicing, which includes digital management of payments and storage of receipts. The Ministry of Finance also encourages private companies to use the electronic invoice system.[42] In addition, the government promotes the use of digital signatures and electronic filing and since 2008, the use of digital signatures is supported through legislation such as the Public Administration Act.[43] In 2013, the electronic Mobile ID, which expands digital identificatio to phones, was launched. Several public administration services are accessible via Mobile ID reached via the officia e-service portal online. Mobile ID can be used to log into public systems, as well as to sign documents.[44]

Digital Activism

Digital tools are widely used for social, political, and civic activism in Iceland. In summer 2015, a digital campaign to raise awareness on sexual abuse grew from a women's group on Twitter, followed by a campaign on Facebook. Women who had experienced sexual violence, or who knew someone else who had been a victim, changed their profil picture to a specifi emoji in yellow or orange, in order to speak out about the problem.[45]

The popularity of social media sites like Facebook has been used to engage the population in the process of redrafting the Icelandic constitution over the past few years. The existing constitution is an almost exact copy of the Danish constitutional text, which was adopted when Iceland gained independence from Denmark in 1944. In the wake of the Icelandic financia crisis in 2008, the population demanded an extensive review of the country's constitution.[46] A 25-member council consisting of ordinary residents helped draft a new constitution and worked through sixteen versions in four months based on 16,000 comments from Icelandic citizens using social media platforms such as

39 Gudmondsson, "Media Landscapes – Iceland."

40 Statistics Iceland, http://www.statice.is.

41 Gijs Hillenius, "IS: Public administration in Iceland is moving to open source," ePractice Community, European Commission, April 4, 2012, http://bit.ly/1EBAntk.

42 Gijs Hillenius, "Iceland Government has Switched to eInvoicing," ePractice Community, European Commission, February 25, 2015, bit.ly/1Xsf2KK.

43 IDABC – European eGovernment Services, "Study on Mutual Recognition of eSignatures," July 2009, http://bit.ly/1zzwczv.

44 Review Gemalto, "How mobile ID conquered Iceland," January 9, 2015, http://bit.ly/22gTzLH and Azazo.com, "The Icelandic Minister of the Interior signs this press release, using Mobile ID in CoreData," February 25, 2014, http://bit.ly/1QUhLLf.

45 Loulla-Mae Eleftheriou-Smith, "Women in Iceland are changing their Facebook profil pictures to yellow and orange sad face to highlight the prevalence of sexual violence," *The Independent*, June 10, 2015, ind.pn/1M4izy1.

46 Robertson, "Voters in Iceland Back New Constitution, More Resource Control."

Facebook, Twitter, and YouTube.[47] A majority of the population voted for the draft constitution in a national referendum on October 20, 2012,[48] though a law has yet to be passed in parliament. In 2013, the prime minister appointed a committee on constitutional affairs to continue the work on the constitution, in accordance with an agreement reached by parliamentary parties. Emphasis continues to be on transparency, informed debate, and public participation. In February 2016, the committee on constitutional affairs publicly issued three draft bills for public comment, concerning natural resources, environmental issues, and a referendum on the initiative of a share of voters, and comments and feedback were made public.[49]

According to a poll from January 2016, the Pirate Party led by Birgitta Jónsdóttir, which supports online freedom, would become the largest in parliament with almost 42 percent of the votes if elections were held at the time of the poll, followed by the Independence Party, with 23 percent.[50] Parliamentary elections were scheduled for October 2016. The Icelandic Pirate Party is aligned with a network of other similarly named political parties throughout the world that also promote a platform of free expression, and was the first Pirate Party to win seats in a national election in 2013.[51]

Violations of User Rights

Iceland has a strong tradition of protecting freedom of expression that extends to the use of the internet. The Icelandic Modern Media Initiative seeks to develop legal frameworks for protecting the press, bloggers, and whistleblowers from illegitimate prosecutions or harassment. Individuals are rarely prosecuted for social or political content posted online, though libel laws remain a concern. In late 2015, Icelandic government websites were the target of several cyber attacks from the activist group Anonymous as a protest against Iceland's commercial whaling activity.

Legal Environment

Freedom of expression is protected under Article 73 of the Icelandic constitution.[52] The Icelandic Media Law, which came into effect in September 2011, established several legal protections for journalists that extend to the online sphere, including editorial independence from media service providers' owners and the protection of anonymous sources.[53]

Despite strong protections for free speech, libel and insult are criminal offenses subject to fine or a prison sentence of up to one year. According to Article 51, journalists cannot be held responsible for potentially libelous quotes from sources, but they can be held responsible for libel in their own content.[54] Journalists consider the court's practice with regard to libel laws to be too rigid, leading to lawsuits that aim to silence critical press.

47 "A Proposal for a New Constitution for the Republic of Iceland", drafted by *Stjórnlagaráð*, a Constitutional Council, appointed by an *Althingi* resolution, March 24, 2011, http://bit.ly/1gFFBEX.

48 Julia Mahncke, "Iceland's grassroots constitution on thin ice," *Deutsche Welle*, March 13, 2013, http://bit.ly/XmC9Hj.

49 Email interview with employee at the Legislative Department at the Office of the Prime Minister, March 3, 2016; and the website on the work with the draft constitution and constitutional matters in general: http://www.forsaetisraduneyti.is/stjornarskra/ and bit.ly/1nKNzrz.

50 Vala Hafstad, "Pirate Party Support Exceeds 40 Percent", *Iceland Review,* January 28, 2016, bit.ly/1PHx3pg.

51 Interview with employee at the Icelandic Media Commission, May 17, 2013.

52 Constitution of the Republic of Iceland, http://www.government.is/constitution/.

53 Media Law No. 38, art. 24 and 25, April 20, 2011, http://bit.ly/15C05KS.

54 Media Law No. 38, April 20, 2011, http://bit.ly/15C05KS.

In the past few years, the government has pursued several legislative and policy initiatives to enhance internet freedom. In June 2010, following the 2008 financia crisis and inspired by the whistleblower website WikiLeaks, the Icelandic parliament approved a resolution on the Icelandic Modern Media Initiative, which aims to create a global safe haven with legal protection for the press, bloggers, and whistleblowers.[55] In 2012, the Minister of Education, Science and Culture appointed a committee of experts to report on online and offlin challenges freedom of expression and information and propose recommendations for their promotion.[56] In 2013, the new Minister of Education, Science and Culture assigned funding for the Icelandic Modern Media Initiative and appointed a new committee to undertake the task of decriminalizing defamation, among other duties. A member of the committee expects that at least two bills will come out of this work.[57]

In early 2015, a series of bills to further the objective of establishing Iceland as a safe haven for free speech were submitted to Parliament, primarily by the Pirate Party, but were not passed.[58] The bills included whistleblower protections, the removal of a clause on data retention, and a resolution establishing an offic of independent oversight for police wiretapping procedures and other comparable investigative measures.[59]

In June 2015, blasphemy was repealed as a criminal offence under Article 125 of the Penal Code. It had carried penalties of fine or imprisonment for up to three months.[60] The Pirate Party had proposed repealing it in Parliament in the aftermath of the terrorist attack on the office of the *Charlie Hebdo* magazine in France in January 2015.[61]

Other legislative efforts are ongoing. A parliamentary resolution on equal access to the internet concerning the benefit of a free and unrestricted internet and the protection of user rights, was adopted in late 2014 and awaited implementation in mid-2016.[62]

Prosecutions and Detentions for Online Activities

Icelandic internet users are periodically prosecuted for their online activities, particularly for libel. In May 2015, an Icelandic woman was charged with libel and fine ISK 50,000 (US$385) as well as her own legal fees of ISK 1.2 million (US$9,230) for comments posted on Facebook. The comments suggested that the Chairman of Eyjar and Miklaholt District Council had been bribed with a tractor by her neighbor Ólafur Ólafsson, but the court found no evidence of such a gift, or that the woman was repeating gossip. The woman apologized and removed her remarks.[63]

Surveillance, Privacy, and Anonymity

Following revelations in 2013 that U.S. and UK intelligence agencies have been collecting and storing

55 IFEX, "Authorities create a safe haven for press freedom," June 23, 2010, http://www.ifex.org/iceland/2010/06/23/safe_haven/

56 Email interview with former employee at the Icelandic Media Commission, Jan 29, 2014.

57 Email interview with member of the Icelandic Media Commission, January 14, 2016.

58 Email interview with member of the Icelandic Media Commission, January 14, 2016.

59 Disclosure of Information and Protection of Whistleblower Bill, case no. 453, http://bit.ly/1VV5xY8; and IMMI, "A bill on Whistleblowers, removal of Data Retention and more," March 25, 2015, http://bit.ly/1PvI2zQ.

60 International Press Institute, Media Laws Database, http://bit.ly/1RjVMui

61 Kevin Rawlinson, "Iceland Repeals Blasphemy Ban after Pirate Party Campaign," *The Guardian*, July 3, 2015, http://bit.ly/1D1If4K

62 Email interview with member of the Media Committee, April 29, 2015; IMMI, "Data Protection," http://bit.ly/1X7lvLU; and the Icelandic Parliament, "Resolution on the internet," http://bit.ly/1I3o8tx.

63 Iceland Monitor, "Iceland Facebook libel fine" May 28, 2015, http://bit.ly/1HOCpaP

massive amounts of user data from online communications around the world, free speech activists in Iceland such as Birgitta Jónsdóttir expressed concern that Iceland's efforts to protect journalists and whistleblowers from surveillance may ultimately prove ineffective.[64] Iceland is part of a greater international surveillance network that cooperates with the activities of the "Five Eyes Alliance"—the intelligence operations agreement between the United States, the United Kingdom, Australia, Canada, and New Zealand.[65]

Currently, the Electronic Communications Act of 2003 implements data retention requirements mandated by Iceland's inclusion in the European Economic Area.[66] The law applies to telecommunication providers and mandates the retention of records for six months. It also states that companies may only deliver information on telecommunications in criminal cases or on matters of public safety, and that such information may not be given to anyone other than the police or the public prosecution.[67] The government does not place any restrictions on anonymous communication. No registration is required when purchasing a SIM card in Iceland.

Intimidation and Violence

There have been no physical attacks against bloggers or online journalists in Iceland.

Technical Attacks

In November and December 2015, the internet activist group Anonymous attacked several Icelandic government websites, including those operated by the Ministry of Home Affairs, the Ministry of Foreign Affairs, as well as the Prime Minister's Office The attacks were a protest against Iceland's commercial whaling activity and were flagge on social media under the hashtag #OpWhales.[68] A similar attack was carried out in January 2016, disabling government websites for a short while.[69] In December 2015, a distributed denial-of-service (DDoS) attack hit the telecom company Vodafone, temporarily forcing its website to crash by overloading it with requests, without anyone claiming responsibility.[70]

Since June 2013, the Icelandic National CERT, operating within the Post and Telecom Administration in Iceland, has been the national center point for cyber security incidents and participates in international efforts and cooperation.[71] In July 2015, the Ministry of the Interior published a new ICT security policy that aims to increase resilience, raise awareness about security issues, and extend collaboration to organizations including the United Nation and the European Union, in addition to NATO.[72]

64 Alex Hern, "NSA surveillance hinders Iceland's attempts to be a haven for free speech," *The Guardian*, November 19, 2013, http://bit.ly/1vR6s9M.

65 Carly Nyst, "The Five Eyes Fact Sheet," Privacy International, November 26, 2013, http://bit.ly/1LwbVOI.

66 Electronic Communications Act No. 81, March 26, 2003, http://bit.ly/1MF6rSA.

67 Icelandic Media Initiative, https://immi.is/index.php/projects/immi.

68 Iceland Monitor, "Anonymous pursue Iceland Cyber Attacks", December 10, 2015, http://bit.ly/1OjGcxC.

69 Iceland Monitor, "Government Office suffer Cyber Attack", January 12, 2016, http://bit.ly/1mTOVAM.

70 Paul Fontaine, Vodafone Falls Prey to Cyber Attack", *the Reykjavik Grapevine*, December 9, 2015, http://bit.ly/1RjFyRX.

71 Post and Telecom Administration in Iceland, http://bit.ly/LXusIn.

72 Gijs Hillenius, "Iceland boosts ICT Security Measures, Shares Policy," ePractice Community, European Commission, August 28, 2015, http://bit.ly/1SPsSYw and Icelandic National Cyber Security Strategy 2015-2026, http://bit.ly/1QUMgBU

Freedom House

India

	2015	2016
Internet Freedom Status	Partly Free	Partly Free
Obstacles to Access (0-25)	12	12
Limits on Content (0-35)	10	9
Violations of User Rights (0-40)	18	20
TOTAL* (0-100)	**40**	**41**

* 0=most free, 100=least free

Population:	**1.311 billion**
Internet Penetration 2015 (ITU):	**26 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Partly Free**

Key Developments: June 2015 – May 2016

- Authorities ordered service providers to temporarily shut down local mobile internet service in at least 23 separate reported cases, purportedly to prevent unrest or even cheating in an exam (see **Restrictions on Connectivity**).
- Regulators passed strong net neutrality regulations following sustained digital advocacy, prohibiting service providers from charging more for some data services (see **Digital Activism**).
- The Supreme Court upheld the constitutional validity of laws criminalizing defamation (see **Legal Environment**).
- At least 17 people were arrested for information circulated on WhatsApp, including group administrators based on content shared by other group members (see **Prosecutions and Detentions for Online Activities**).
- In May 2016, the Central Monitoring System was reported to be operational in New Delhi and Mumbai, allowing direct government surveillance of online traffic (see **Surveillance, Privacy and Anonymity**).
- In June 2015, journalist Joginder Singh died in Uttar Pradesh when assailants set him on fi e after he posted allegations about a local official s wrongdoing on Facebook (see **Intimidation and Violence**).

Introduction

Internet freedom declined slightly in 2016, offsetting gains made in 2014 and 2015. The number of network shutdowns ordered by local authorities increased dramatically.

Internet penetration increased during the reporting period, as India overtook the United States to become the world's second largest internet consumer base behind China. Both government and nongovernmental entities made efforts to bridge the digital divide. After effective digital campaigning, the Telecom Regulatory Authority of India (TRAI) introduced strong net neutrality protections in 2016, prohibiting differential pricing by service providers for different content or applications.

However, other developments undermined internet freedom. Local authorities ordered service providers to temporarily shut down internet access in at least 23 reported incidents in various states. In 2016, the Supreme Court dismissed a petition challenging the use of broad powers provided to state governments under the criminal procedure code to shut down internet services.

The Supreme Court also upheld laws criminalizing defamation which apply to both online and offline speech. Arrests for online activities declined in mid-2015. Many were based on Section 66A of the IT Act, which the Supreme Court declared was unconstitutional in March. But arrests increased again during the coverage period of this report under other sections of the IT Act and provisions of the penal code. At least seventeen people were detained for content circulated on WhatsApp, including group administrators who were not responsible for the content.

India continues to lack a codified law o effectively protect privacy. A Constitution Bench of the Supreme Court is considering whether privacy is a fundamental right at all. Although there were no reported instances of unlawful surveillance during the reporting period of coverage, this may be due to the extreme opacity of the regulatory framework governing surveillance. In May 2016, officials said the government's Central Monitoring System—an ambitious nationwide mass surveillance program—became operational through regional monitoring centers in New Delhi and Mumbai.

Obstacles to Access

Internet penetration in India continued to increase in 2016 with mobile penetration playing a significant role. Inadequate infrastructure remains a significant obstacle to access, especially in rural areas; however, various governmental and nongovernmental efforts to improve access nationwide are underway. There was a sharp increase in both the frequency and duration of ICT shutdowns ordered by local authorities. The top ten internet service providers (ISPs) still hold almost the entire market share, but strong competition among them continues.

Availability and Ease of Access

India had the second largest number of internet subscribers in the world after China in 2016, having

recently overtaken the United States.[1] Official statistics ecorded 331 million subscribers in December 2015,[2] though only 20 million had fi ed-line connections.[3]

However, internet penetration remains low, reaching 26 percent in December 2015,[4] up from 21 percent in December 2014.[5] Mobile penetration was much higher, reaching 82 percent by December 2015.[6] India was ranked 155 out of 189 countries in terms of mobile broadband penetration by the Broadband Commission.[7]

India's average connection speed was 3.5 Mbps, one of the lowest in Asia,[8] and far below the global average, which Akamai documented at 6.3 Mbps in the fi st quarter of 2016.[9] Fifty-nine percent of all internet users had narrowband subscriptions in 2015,[10] down from sixty-eight percent in 2014.[11] Despite overall growth, India still has one of the world's lowest adoption rates for high speed broadband (faster than 10 Mbps), at just 4.8 percent,[12] though that rate grew by 180 percent during the course of 2015.[13] The minimum speed required to qualify as broadband in India has been 512 Kbps since 2012,[14] though the Telecom Regulatory Authority of India (TRAI) has recommended raising the threshold to 2 Mbps.[15]

1 Harriet Taylor, "Mary Meeker: India now has more internet users than US", CNBC, June 1, 2016,http://www.cnbc.com/2016/06/01/mary-meeker-india-now-has-more-internet-users-that-us.html; Vlad Savov, "India rises past the US to become the internet's second biggest user", The Verge, June 2, 2016, http://www.theverge.com/2016/6/2/11837898/india-internet-user-population-stats-mary-meeker-2016; "India Pips US in Number of Internet Users", Huffing on Post India, June 2, 2016, http://www.huffing onpost.in/2016/06/02/india-internet-usage_n_10259450.html.

2 Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators October – December 2015, May 18, 2016, p. ii, http://www.trai.gov.in/WriteReadData/PIRReport/Documents/QPIR_Oct_to_Dec-15.pdf; the International Telecommunication Union separately estimated penetration at 26 percent in 2015. International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1cblxxY.

3 Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators October – December 2015, May 18, 2016, p. ii, http://www.trai.gov.in/WriteReadData/PIRReport/Documents/QPIR_Oct_to_Dec-15.pdf.

4 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1cblxxY; Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators October – December 2015, May 18, 2016, p. ii, http://www.trai.gov.in/WriteReadData/PIRReport/Documents/QPIR_Oct_to_Dec-15.pdf.

5 Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators October – December 2014, May 8, 2015, p. ii, http://www.trai.gov.in/WriteReadData/PIRReport/Documents/Indicator_Reports%20-%20Dec-14=08052015.pdf. .

6 Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators October – December 2015, May 18, 2016, p. i, http://www.trai.gov.in/WriteReadData/PIRReport/Documents/QPIR_Oct_to_Dec-15.pdf; Telecom Regulatory Authority of India, Highlights of Telecom Subscription Data as on April 30th 2016, Press Release No. 49/2016, http://www.trai.gov.in/WriteReadData/PressRealease/Document/Press_Release_No.49_20_june_2016_Eng.pdf. The ITU reported mobile penetration at 79 percent in 2015: International Telecommunication Union, "Mobile-cellular subscriptions," http://bit.ly/1cblxxY.

7 Broadband Commission (ITU & UNESCO), The State of Broadband 2015: Broadband as a Foundation for Sustainable Development, September 2015, p. 89, http://www.broadbandcommission.org/Documents/reports/bb-annualreport2015.pdf (2014 figu e).

8 Akamai, The State of the Internet, Q1, 2016 Report, Vol. 9 No. 1, June 29, 2016, p. 28, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-state-of-the-internet-report-q1-2016.pdf.

9 Akamai, The State of the Internet, Q1, 2016 Report, Vol. 9 No. 1, June 29, 2016, p. 12, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-state-of-the-internet-report-q1-2016.pdf.

10 Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators October – December 2015, May 18, 2016, p. 28, http://www.trai.gov.in/WriteReadData/PIRReport/Documents/QPIR_Oct_to_Dec-15.pdf.

11 Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators October – Dec 2014, May 8, 2015, p. 29, http://www.trai.gov.in/WriteReadData/PIRReport/Documents/Indicator_Reports%20-%20Dec-14=08052015.pdf.

12 Akamai, The State of the Internet, Q1, 2016 Report, Vol. 9 No. 1, June 29, 2016, p. 29, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-state-of-the-internet-report-q1-2016.pdf.

13 Akamai, The State of the Internet, Q1, 2016 Report, Vol. 9 No. 1, June 29, 2016, p. 29, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-state-of-the-internet-report-q1-2016.pdf.

14 Telecom Regulatory Authority of India, "TRAI's Recommendations on the National Broadband Plan", May 4, 2011, http://www.trai.gov.in/WriteReadData/Recommendation/Documents/Reply_DOT_Broadband_modified[1].pd .

15 Report on Need for Reviewing Definition f Broadband, May 24th 2016, TRAI, http://www.trai.gov.in/WriteReadData/Recommendation/Documents/Letter_to_Secretary_DOT_24_may_2016.pdf.

The Global Information Technology Report by the World Economic Forum and INSEAD ranked India in eighth place out of 139 countries for affordable internet access in 2016.[16] It was previously in fi st place,[17] and per minute cellular and fi ed broadband tariffs are still among the lowest in the world.[18] Fixed broadband internet service cost an average INR 1676 (US$ 25) per month.[19]

India ranked 81 out of 140 countries for infrastructure in 2016, according to the World Economic Forum's Global Competitiveness Index.[20] Though up from 87 the previous year, the results suggest poor infrastructure is still an obstacle to access. India ranked a low 98 for electricity supply;[21] and 120 for technological readiness, the capacity of a country to fully leverage ICTs in daily activities.[22] Only 26 percent of all Indian schools had a computer in 2015.[23] That figu e was higher in secondary schools and above (66 percent),[24] though of those, only 37 percent were connected to the internet.[25]

Public and private sector initiatives to improve access are underway. News reports announced government plans to provide free public Wi-Fi zones in mid-2015,[26] targeting 25 top cities by population.[27] Some public Wi-Fi zones have already been established in places like Delhi, Ahmedabad, Bangalore and Patna.[28] During the coverage period of this report, Google partnered with public sector company RailTel to provide free Wi-Fi at over 400 railway stations,[29] starting with 100 by the end of 2016.[30] At least 15 stations were already connected in May.[31]

The Digital India Programme launched in 2014[32] by the Department of Telecom (DoT) and the

16 Silja Baller, Soumitra Dutta, and Bruno Lanvin (Eds.), Global Information Technology Report 2016, World Economic Forum and INSEAD, p. 111, http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf.

17 Thierry Geiger, Soumitra Dutta, and Bruno Lanvin (Eds.), Global Information Technology Report 2015, World Economic Forum and INSEAD, p. 172, http://www3.weforum.org/docs/WEF_Global_IT_Report_2015.pdf.

18 Silja Baller, Soumitra Dutta, and Bruno Lanvin (Eds.), Global Information Technology Report 2016, World Economic Forum and INSEAD, p. 111, http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf.

19 Silja Baller, Soumitra Dutta, and Bruno Lanvin (Eds.), Global Information Technology Report 2016, World Economic Forum and INSEAD, p. 111, http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf. .

20 Klaus Schwab, The Global Competitiveness Report 2015–2016, World Economic Forum, p. 200, http://www3.weforum.org/docs/gcr/2015-2016/Global_Competitiveness_Report_2015-2016.pdf.

21 Klaus Schwab, The Global Competitiveness Report 2015–2016, World Economic Forum, p. 201, http://www3.weforum.org/docs/gcr/2015-2016/Global_Competitiveness_Report_2015-2016.pdf.

22 Klaus Schwab, The Global Competitiveness Report 2015–2016, World Economic Forum, p. 200, http://www3.weforum.org/docs/gcr/2015-2016/Global_Competitiveness_Report_2015-2016.pdf.

23 Flash Statistics: School Education in India 2014-15, National University of Educational Planning and Administration, p. 26, http://dise.in/Downloads/Publications/Documents/U-DISE-SchoolEducationInIndia-2014-15.pdf.

24 Flash Statistics: Secondary Education in India, National University of Educational Planning and Administration, p. 12, http://dise.in/Downloads/Publications/Documents/SecondaryFlash%20Statistics-2014-15.pdf.

25 Flash Statistics: Secondary Education in India, National University of Educational Planning and Administration, p. 13, http://dise.in/Downloads/Publications/Documents/SecondaryFlash%20Statistics-2014-15.pdf.

26 Digital India, DeitY, http://deity.gov.in/sites/upload_files/dit/files/Digital%20India.p .

27 Anirudh Vohra, "Free Wi-Fi: Digital Dilemma", The Financial Express, February 21, 2015, http://www.financialexp ess.com/article/economy/free-wi-fi-digital-dilemma/45804 .

28 "25 Indian cities to get free public Wi-Fi by June 2015", India Today, December 17, 2014, http://indiatoday.intoday.in/technology/story/25-indian-cities-to-get-free-public-wi-fi-by-june-2015/1/407214.htm .

29 Shruti Dhapola, "Explained: What is Google's Wi-Fi at 100 railway station project and how will it work", Indian Express, December 17, 2015, http://indianexpress.com/article/technology/tech-news-technology/explained-what-is-googles-wifi-a -railway-station-project-and-how-will-it-work/.

30 Shruti Dhapola, "Explained: What is Google's Wi-Fi at 100 railway station project and how will it work", Indian Express, December 17, 2015, http://indianexpress.com/article/technology/tech-news-technology/explained-what-is-googles-wifi-a -railway-station-project-and-how-will-it-work/.

31 "Google, RailTel's Free Wi-Fi Service Comes to 5 More Railway Stations", Gadgets 360 NDTV, May 10, 2016, http://gadgets.ndtv.com/internet/news/google-railtels-free-wi-fi-se vice-comes-to-5-more-railway-stations-835810.

32 "Digital India – A programme to transform India into digital empowered society and knowledge economy", August 20, 2014, http://pib.nic.in/newsite/erelease.aspx?relid=108926.

Department of Electronics and Information Technology (DeitY) is expected to be implemented by 2018.[33] It aims to connect India's Gram Panchayats, institutions of self-government for rural areas,[34] via fibe -optic cables,[35] ensuring universal broadband access with accompanying e-literacy programs. Internet-connected Common Service Centers (CSCs) aim to cover all 250,000 Gram Panchayats;[36] as of March 2016, 157,000 had been established, with 20,000 operated by women.[37] The program proposes to use satellites, balloons, or drones to push faster digital connections to remote parts of the country,[38] as well as Multiple System Operators (MSOs) such as cable TV services, which already have last-mile connectivity.[39] As a result of the Digital India Programme, electronic transactions related to e-governance projects almost doubled in 2015;[40] citizen and public records are being digitized through crowd-sourcing efforts;[41] and Digi Locker, a service which provides secure online storage of essential documents such as birth certifica es, has more than 2 million registered users.[42] Digital India also provides capital to develop new technologies.[43]

Language remains a barrier to access. With 22 official languages, only about 12 pe cent of the population of India speaks English,[44] yet more than half the content available online is in English,[45] and over 100 languages were unrepresented online in 2013.[46] Projects to encourage local language usage are underway, and there were nearly 127 million local language users on the internet by 2014.[47] Hindi-language web content grew by 94 percent in 2015, compared to 19 percent growth in English

33 Digital India, DeitY, http://deity.gov.in/sites/upload_files/dit/files/Digital%20India.p .

34 Constitution of India, Article 243(d).

35 National Optic Fibre Network (NOFN), Bharat Broadband Network Limited, http://www.bbnl.nic.in/content/page/national-optical-fib e-networknofn.php.

36 CSC 2.0 Scheme, Common Service Centres Scheme, DeitY, Govt. of India, http://csc.gov.in/index.php?option=com_content&view=article&id=174&Itemid=331.

37 Pranav Mukul, "Govt to set up 1 lakh common service centres in rural areas: Ravi Shankar Prasad", Indian Express, March 23, 2016, http://indianexpress.com/article/india/india-news-india/govt-to-set-up-1-lakh-common-service-centres-in-rural-areas-ravi-shankar-prasad/.

38 "Centre ready to use satellites, drones to connect to rural India: Ravi Shankar Prasad", Economic Times, February 4, 2015, http://articles.economictimes.indiatimes.com/2015-02-04/news/58795885_1_digital-india-ravi-shankar-prasad-pilot-project.

39 "DoT to provide internet via MSOs, cable operators", Times of India, February 16, 2015, http://timesofindia.indiatimes.com_tech/tech-news/DoT-to-provide-internet-via-MSOs-cable-operators/articleshow/46261597.cms.

40 See http://etaal.gov.in/etaal/YearlyChartIndex.aspx; "Digital India: E-governance transactions double in 2015", Times of India, January 11, 2016, http://timesofindia.indiatimes.com/ ech/tech-news/Digital-India-E-governance-transactions-double-in-2015/articleshow/50532400.cms?.

41 Neha Alawadhi, "Digital India: Government digitizes 2 million public records' characters", Times of India, December 15, 2015, http://timesofindia.indiatimes.com/ ech/tech%20news/Digital-India-Government-digitizes-2-million-public-records-characters/articleshow/50185112.cms.

42 See https://digilocker.gov.in/; Muntazir Abbas, "Digital India: Government wants municipalities to replicate Rahuri's DigiLocker Model", Economic Times, April 28, 2016, http://economictimes.indiatimes.com/telecomnews/Digital-India-Government-wants-municipalities-to-replicate-Rahuris-DigiLocker-model/articleshow/52026878.cms.

43 Ashish K Tiwari, "Government launches Rs. 2200 crore Electronics Development Fund", DNA, February 16, 2016, http://www.dnaindia.com/money/report-government-launches-rs-2200-crore-electronics-development-fund-2178223.

44 IMRB-INT, IAMAI Internet in India 2014, October 2014, p. 14; "Local language content to boost India's internet penetration: IAMAI", August 4, 2015,http://timesofindia.indiatimes.com/ ech/tech-news/Local-language-content-to-boost-Indias-internet-penetration-IAMAI/articleshow/48346892.cms.

45 Usage of Content Languages for Websites, W3Techs, http://w3techs.com/technologies; http://w3techs.com/technologies/overview/content_language/all.

46 "Speakers' strength of languages and mother tongues", 2001 Census of India, http://www.censusindia.gov.in/Census_Data_2001/Census_Data_Online/Language/Statement1.aspx; IMRB-INT, IAMAI Internet in India 2013, June 2013, pp. 15-16, http://www.imrbint.com/downloads/Report-BB55685%20IAMAI%20ICUBE_2013-Urban+Rural-C1.pdf.

47 IMRB-INT, IAMAI Internet in Local Language 2014, October 2014, p. 14; "Local language content to boost India's internet penetration: IAMAI", August 4, 2015,http://timesofindia.indiatimes.com/ ech/tech-news/Local-language-content-to-boost-Indias-internet-penetration-IAMAI/articleshow/48346892.cms.

content.[48] Google's Indian Language Internet Alliance (ILIA) seeks to link all local language content available to a single platform,[49] making the content more visible and easier for consumers to navigate.[50] Critics fear this could divert traffic f om the original pages, resulting in loss of revenue and readership,[51] but so far ILIA has partnered with 30 organizations.[52] In 2014, the National Internet Exchange of India (NIXI), which operates and manages Indian domain names, launched the Dot Bharat domain for local language URLs.[53] Indian start-ups, such as online marketplace Snapdeal, Quikr, which offers online classified ad ertising, and Hike messenger, have also introduced services in local languages.[54]

Studies have shown that economic and social conditions result in barriers to internet access for women. In 2015, only 29 percent of Indian internet users were women,[55] falling to 12 percent in rural areas.[56] Growth in the number of female internet users is higher than for men in urban areas, though not overall.[57] Google has partnered with Tata Trusts to launch the Internet Saathi scheme for promoting digital literacy among rural women.[58] The initiative initially aimed to reach 45,000 villages.[59] In December 2015, Google CEO, Sundar Pichai said the project would expand to 300,000.[60]

Restrictions on Connectivity

The Indian government does not routinely block the protocols or tools that allow for instant, person-to-person communication, although local authorities can restrict ICT connectivity and usage

48 "Local language content will boost internet usage: IAMAI", Times of India, February 17, 2016, http://timesofindia.indiatimes.com/tech/tech-news/Local-language-content-will-boost-internet-usage-IAMAI/articleshow/51025569.cms.

49 "Google will Destroy Local Newspapers with Indian language Internet Alliance", Firstpost, November 3, 2014, http://www.fi stpost.com/business/corporate-business/google-will-destroy-local-newspapers-with-indian-language-internet-alliance-1995349.html; Nandagopal Rajan, "Big Boost for Hindi as Google Ropes in partners for Indian Language Internet Alliance", Indian Express, November 4, 2014, http://indianexpress.com/article/technology/technology-others/google-kickstarts-indian-language-internet-alliance-focus-fi st-on-hindi/.

50 "Google will Destroy Local Newspapers with Indian language Internet Alliance", Firstpost, November 3, 2014, http://www.fi stpost.com/business/corporate-business/google-will-destroy-local-newspapers-with-indian-language-internet-alliance-1995349.html; Nandagopal Rajan, "Big Boost for Hindi as Google Ropes in partners for Indian Language Internet Alliance", Indian Express, November 4, 2014, http://indianexpress.com/article/technology/technology-others/google-kickstarts-indian-language-internet-alliance-focus-fi st-on-hindi/.

51 "Google will Destroy Local Newspapers with Indian language Internet Alliance", Firstpost, November 3, 2014, http://www.fi stpost.com/business/corporate-business/google-will-destroy-local-newspapers-with-indian-language-internet-alliance-1995349.html; Nandagopal Rajan, "Big Boost for Hindi as Google Ropes in partners for Indian Language Internet Alliance", Indian Express, November 4, 2014, http://indianexpress.com/article/technology/technology-others/google-kickstarts-indian-language-internet-alliance-focus-fi st-on-hindi/.

52 "Google to concentrate on local language content", Hindustan Times, July 6, 2015, http://indiatoday.intoday.in/technology/story/google-to-concentrate-on-local-language-content/1/449440.html.

53 Anoop Verma, "Internet domain names in Indian languages", Financial Express, February 2, 2015, http://computer.financialexp ess.com/magazine/internet-domain-names-in-indian-languages/8613/.

54 Kunal Doley, "Looking local: Snapdeal, Quikr, Hike, others launch vernacular language support, Financial Express, January 24, 2016, http://www.financialexp ess.com/article/industry/companies/looking-local-snapdeal-quikr-hike-others-launch-vernacular-language-support/201082/.

55 Press Release on Internet in India 2015, IAMAI, November 17, 2015, http://www.iamai.in/media/details/4486.

56 Press Release on Internet in India 2015, IAMAI, November 17, 2015, http://www.iamai.in/media/details/4486.

57 Press Release on Internet in India 2015, IAMAI, November 17, 2015, http://www.iamai.in/media/details/4486.

58 Meghna Rao, "Google launches 'Internet Saathi' for women in rural India", Business Standard, August 25, 2015, http://www.business-standard.com/article/companies/google-launches-internet-saathi-for-women-in-rural-india-115082500329_1.html.

59 Meghna Rao, "Google launches 'Internet Saathi' for women in rural India", Business Standard, August 25, 2015, http://www.business-standard.com/article/companies/google-launches-internet-saathi-for-women-in-rural-india-115082500329_1.html.

60 "Google to partner with India's 'Internet Saathi' program: Ravi Shankar Prasad", DNA, December 16, 2015, http://www.dnaindia.com/money/report-google-to-partner-with-india-s-internet-saathi-program-ravi-shankar-prasad-2156455.

during times of perceived unrest. The number of these shutdowns has increased significantly in the past two years.[61]

During the coverage period of this report, local authorities issued orders to providers to shut off specific se vices in 23 reported cases, including local mobile phone service, SMS, wireless, and occasionally fi ed-line internet access, for periods ranging from a few hours to several days.[62] In one instance, the state government in northeastern Manipur blocked wireless internet and SMS services for seven days following violent protests.[63] Although the majority of shutdown orders cited security or public order threats as reasons, mobile internet was blocked for four hours across Gujarat in February 2016 to prevent cheating in a state entrance exam.[64]

Local authorities increasingly used Section 144 of the Code of Criminal Procedure (1973) to justify these orders, which permits broad state action to curb any violation of law and order;[65] it does not specify telecommunications.[66] The use of this general law to order shutdowns was upheld by the Gujarat High Court in September 2015,[67] and the Supreme Court rejected a petition challenging it in early 2016.[68]

Other laws used to justify shutdowns also lack specificit . Section 69A of the Information Technology (IT) Act, which permits the central government to order website blocks (see Limits on Content) has been considered to apply to blocking of service. Section 5 of the Indian Telegraph Act, which allows state and central authorities to order that any message not be transmitted in public emergencies, has also been cited in support of service disruptions.[69]

As in past years, Jammu and Kashmir had the highest number of documented incidents, including a

61 Sarvjeet Singh, "Incidents of Internet Shutdowns in India (2012 onwards)", Centre for Communication Governance at National Law University, Delhi, https://drive.google.com/open?id=0BycAZd9M5_7NOExCRnQ3Q1pqcm8.

62 Sarvjeet Singh, "Incidents of Internet Shutdowns in India (2012 onwards)", Centre for Communication Governance at National Law University, Delhi, https://drive.google.com/open?id=0BycAZd9M5_7NOExCRnQ3Q1pqcm8.

63 "Internet blocked in Manipur to quell violence", Live Mint, September 3, 2015, http://www.livemint.com/Politics/ZFX1zHdhZ827jnqirpzZqO/Internet-blocked-in-Manipur-to-quell-violence.html; Iboyaima Laithangbam, "Curfew continues in Manipur; internet blocked", The Hindu, September 2, 2015, http://www.thehindu.com/news/national/other-states/internet-blocked-in-manipur-to-check-communal-fla e/article7607186.ece; Binalakshmi Nepram, "Manipur violence: Why the protest and what are the demands", Indian Express, September 6, 2015, http://indianexpress.com/article/blogs/summer-of-revolt-why-manipur-is-one-of-the-worst-conflic -affected-states-in-south-asia/; "Manipur government lifts block on internet", Economic Times, September 9, 2015, http://articles.economictimes.indiatimes.com/2015-09-09/news/66363391_1_internet-services-gaikhangam-manipur-government.

64 "To beat exam cheats, Gujarat to block mobile internet today", Times of India, February 28, 2016, http://timesofindia indiatimes.com/india/To-beat-exam-cheats-Gujarat-to-block-mobile-internet-today/articleshow/51173461.cms.

65 Nakul Nayak, "The Anatomy of Internet Shutdowns – II (Gujarat & Constitutional Questions)". CCG-NLU Blog, September 1, 2015, https://ccgnludelhi.wordpress.com/2015/09/01/the-anatomy-of-internet-shutdowns-ii-gujarat-constitutional-questions/; Nakul Nayak, "The Anatomy of Internet Shutdowns – III (Post Script: Gujarat High Court Verdict)", CCG-NLU Blog, Sept 19, 2015, https://ccgnludelhi.wordpress.com/2015/09/19/the-anatomy-of-internet-shutdowns-iii-post-script-gujarat-high-court-verdict/.

66 Samanwaya Rautrey, "Supreme Court upholds Internet ban by States", Economic Times Tech, February 12, 2016, http://tech.economictimes.indiatimes.com/news/internet/supreme-court-upholds-internet-ban-by-states/50955292; Chinmayi Arun, "Demarcating a safe threshold", Indian Express, February 24, 2016, http://indianexpress.com/article/opinion/columns/demarcating-a-safe-threshold/.

67 Nakul Nayak, "The Anatomy of Internet Shutdowns – III (Post Script: Gujarat High Court Verdict)", CCG-NLU Blog, September 19, 2015, https://ccgnludelhi.wordpress.com/2015/09/19/the-anatomy-of-internet-shutdowns-iii-post-script-gujarat-high-court-verdict/

68 Samanwaya Rautrey, "Supreme Court upholds Internet ban by States", Economic Times Tech, February 12, 2016, http://tech.economictimes.indiatimes.com/news/internet/supreme-court-upholds-internet-ban-by-states/50955292.

69 Nakul Nayak, "The Anatomy of Internet Shutdowns – I (Of Kill Switches and Legal Vacuums)". CCG-NLU Blog, August 29, 2015, https://ccgnludelhi.wordpress.com/2015/08/29/the-anatomy-of-internet-shutdowns-i-of-kill-switches-and-legal-vacuums/; Apar Gupta, "Section 144 and the power to impose an internet curfew", Economic Times, September 19, 2015, http://articles.economictimes.indiatimes.com/2015-09-19/news/66706176_1_mobile-internet-section-144-central-government.

shutdown that affected both mobile and fi ed-line connections, in some cases for weeks at a time, in summer 2016 (outside the coverage period of this report).[70] During the coverage period:

- On June 5, 2015, mobile and fi ed-line internet services were suspended in the Jammu region in the wake of protests by Sikhs over the removal of posters of Sikh separatist leader Jarnail Bhindrawale before the anniversary of his death.[71]
- In August 2015, mobile phone and internet services were suspended for a few hours during a state government function to celebrate independence day.[72]
- In September 2015, police ordered the suspension of mobile internet services for 82 hours during the Muslim festival of Eid.[73]The Jammu and Kashmir High Court had banned beef based on a petition from hardline Hindus, a decision some Muslim groups said they would protest.[74] One news report said the decision to suspend the internet was made after ISPs clarified that it was not possible o slow down internet speeds.[75]
- In October 2015, mobile internet services were suspended for two days in Jammu and Udhampur amid tensions surrounding the recovery of cow carcasses in Udhampur district.[76]
- In April 2016, mobile internet was blocked for almost six days in fi e districts in Kashmir, following violent protests against the alleged molestation of a girl in Handwara on April 12.[77]

After Jammu and Kashmir, the highest numbers of shutdowns were recorded in the state of Gujarat[78]:

- In September 2015, district commissioners banned mobile internet for almost seven days in the cities of Ahmedabad, Vadodara, Surat and Rajkot after protests by the Patel commu-

70 http://www.hindustantimes.com/india-news/mobile-services-partially-restored-in-kashmir-shutdown-continues-for-43rd-day/story-4bGgEKZbmXSiAJmLdlrvkJ.html

71 "Authorities Reach Agreement With Sikhs in Jammu, But Nervous Calm Prevails in City", NDTV, June 6, 2015, http://www.ndtv.com/india-news/authorities-reach-agreement-with-sikh-community-in-jammu-769205

72 "Mobile phone, internet services snapped in Valley on Independence Day", Economic Times, February 9, 2013, http://articles.economictimes.indiatimes.com/2015-08-15/news/65525213_1_mobile-internet-services-independence-day-bakshi-stadium

73 Mir Ehsan and Arun Sharma, "J&K suspends internet services in the state for 2 days", Indian Express, September 25, 2015, http://indianexpress.com/article/india/india-others/to-avoid-tension-during-eid-ul-zuha-govt-ban-internet-in-jk-for-two-days-from-tomorrow/; Two-day Internet ban in Kashmir Valley on Eid, The Hindu (Sept. 25, 2015), http://www.thehindu.com/news/national/other-states/twoday-internet-ban-in-kashmir-valley-on-eid/article7687069.ece; Peerzada Ashiq, "82-hour internet ban on Eid fuels anger in Kashmir", The Hindu, September 28, 2015, http://www.thehindu.com/news/national/internet-ban-on-eid-fuels-anger-in-kashmir/article7699176.ece.

74 "J-K high court asks state govt to strictly enforce beef ban", Hindustan Times, Sept 13, 2015, http://www.hindustantimes.com/india/j-k-high-court-asks-state-govt-to-strictly-enforce-beef-ban/story-QDhQyZv4VqUaQEm531pPTO.html.

75 Basharat Masood, "J&K govt plans three-day mobile internet ban in Valley", Indian Express, September 24, 2015, http://indianexpress.com/article/india/india-news-india/jk-govt-plans-three-day-mobile-internet-ban-in-valley/.

76 "Mobile internet services cut to calm tension in Udhampur", Indian Express, October 9, 2015, http://indianexpress.com/article/india/india-news-india/mobile-internet-services-cut-in-jammu-after-recovery-of-cows-carcasses/

77 "Mobile Internet Restored in Kashmir, Restrictions Lifted for a Few Hours", The Wire, April 18, 2016, http://thewire.in/2016/04/18/mobilet-internet-restored-in-kashmir-restrictions-lifted-for-few-hours-30024/.

78 Sarvjeet Singh, "Incidents of Internet Shutdowns in India (2012 onwards)", Centre for Communication Governance at National Law University, Delhi, https://drive.google.com/open?id=0BycAZd9M5_7NOExCRnQ3Q1pqcm8.

nity;[79] the ban was repeated for 24 hours in April 2016 when the protests resumed.[80] Some news reports said the shutdowns targeted specific applications li e WhatsApp,[81] but the only orders documented related to the internet as a whole.

- In September 2015, mobile internet was suspended for 24 hours in Godhra, Gujarat to prevent circulation of a derogatory message about Islam on social media.[82]
- In February 2016, mobile internet was blocked for four hours across Gujarat to prevent cheating in a state entrance exam.[83]

While shutdowns remained local to states, they were implemented in more of them than ever before. In December 2015, police blocked mobile internet to quell unrest after caste and communal clashes in at least four districts in Rajasthan;[84] in October, internet had been separately suspended for 24 hours in one of those districts, Bhilwara, following communal clashes.[85] Shutdowns were also documented in Haryana in response to violent protests by the Jat community in February and March 2016;[86] and for one day in Bokaro, Jharkhand during the Hindu festival of Ram Navami.[87] In Azamgarh, Uttar Pradesh, both mobile and fi ed-line internet services were shut down on May 17 and 18, 2016, due to communal tensions.[88]

Submarine cables connect India to the global internet. Ten are consortium owned; the rest are private.[89] These undersea cables are mainstays of mobile and internet communications and any damage to them leads to service disruptions.

In January 2016, Agartala in Tripura became operational as a gateway to the international internet via an optical fiber cable linking o Cox's Bazar in southern Bangladesh, facilitating connectivity in

79 "Hardik Patel detained in Surat, mobile internet services suspended across the state", Indian Express, September 19, 2015, http://indianexpress.com/article/india/gujarat/hardik-patel-other-paas-leaders-detained-in-surat-ahead-of-planned-agitation/.

80 "Curfew in Mehsana, Patel agitation turns violent", Business Standard, April 17, 2016, http://www.business-standard.com/article/pti-stories/curfew-in-mehsana-patel-agitation-turns-violent-116041700486_1.html; Vadodara tense, mobile data services suspended, Hindustan Times, Sept. 28, 2014, http://www.hindustantimes.com/india/vadodara-tense-mobile-data-services-suspended/story-wVinjaYdxN8Eq2RONs0wsJ.html.

81 http://www.bbc.com/news/blogs-trending-34074466

82 "Gujarat: Internet services in Godhra suspended for 24 hours", Indian Express, September 28, 2015, http://indianexpress.com/article/india/gujarat/gujarat-internet-services-in-godhra-suspended-for-24-hours/

83 "To beat exam cheats, Gujarat to block mobile internet today", Times of India, February 28, 2016, http://timesofindia indiatimes.com/india/To-beat-exam-cheats-Gujarat-to-block-mobile-internet-today/articleshow/51173461.cms.

84 Amit Anand Choudhary, "Government can block net for law and order: Supreme Court," Times of India, February 12, 2016, http://timesofindia.indiatimes.com/india/Go ernment-can-block-net-for-law-and-order-Supreme-Court/articleshow/50950023.cms; Ashish Mehta, "Rajasthan police to ban internet usage as per needs to maintain communal harmony", Times of India, December 20, 2015, http://timesofindia.indiatimes.com/india/Rajasthan-police- o-ban-internet-usage-as-per-needs-to-maintain-communal-harmony/articleshow/50258271.cms.

85 "Communal tension in Rajasthan cities", The Hindu, October 24, 2015,http://www.thehindu.com/news/national/other-states/communal-tension-in-rajasthan-cities/article7800532.ece

86 "Jat quota stir: Mobile internet services blocked in Rohtak after clashes over reservation", The Indian Express, February 19, 2016, http://indianexpress.com/article/india/india-news-india/rohtak-jat-reservation-mobile-internet-blocked-haryana/; "Jat reservation: Mobile internet services suspended in several Haryana districts", The Hindu, March 18, 2016, http://indianexpress.com/article/india/india-news-india/jat-reservation-agitation-mobile-internet-haryana/.

87 Alok KN Mishra, "Internet services blocked in Bokaro after communal tension", Times of India, April 16, 2016, http://timesofindia.indiatimes.com/city/ranchi/In ernet-services-blocked-in-Bokaro-after-communal-tension/articleshow/51856786.cms.

88 Sarvjeet Singh, "Incidents of Internet Shutdowns in India (2012 onwards)", Centre for Communication Governance at National Law University, Delhi, https://drive.google.com/open?id=0BycAZd9M5_7NOExCRnQ3Q1pqcm8.

89 The ten are: SeameWe-3; SeaMeWe-4; SeaMeWe-5; Asia-Africa Europe-1; Bay of Bengal Gateway; SAFE; Bharat Lanka Cable System; SEACOM/Tata TGN-Eurasia; IMEWE; and Europe India Gateway. See Submarine Cable Map, TeleGeography, http://www.submarinecablemap.com/#/country/india.

north-eastern states.[90] Mumbai and Chennai already serve as international internet gateways.[91] There are four cable landing stations in Mumbai, and three in Chennai; Digha, Kochi and Tuticorin also have one cable landing station each.[92] BSNL, the state-owned telecom operator, owns two cable landing stations; the rest are privately owned. Tata Communications, the world's largest owner and operator of fiber net ork,[93] and Bharti Airtel, both of which are also major telecom operators, own three stations each.[94] These cable landing stations, where submarine cables meet the mainland, have imposed hefty fees on ISPs; however, lower charges came into effect in 2013.[95]

Over 80 percent of telecommunications towers are privately owned.[96] Market share is split between Indus Towers, a joint venture between Bharti Infratel, Vodafone, and Idea Cellular (31 percent); BSNL (18 percent); and Reliance Infratel (12 percent), according to May 2015 figu es.[97] Bharti Infratel, a subsidiary of Bharti Airtel, is one of the largest tower infrastructure providers, having a 42 percent equity interest in Indus Towers and owning 10 percent of towers independently.[98]

ICT Market

There are 133 operational ISPs in India.[99] While there is no monopoly, the top 10 ISPs control over 98 percent of the market.[100] Bharti Airtel holds the highest market share, worth 25 percent, followed by Vodafone with 20 percent. BSNL, Idea and Reliance have slightly over 10 percent market share each.[101] There are 14 mobile operators,[102] with Bharti Airtel controlling almost 24 percent of the market,[103] followed by Vodafone (19 percent), Idea (17 percent) and Reliance (10 percent).[104]

90 India's new internet gateway via Cox's Bazar to open late January, says minister, http://bdnews24.com/neighbours/2016/01/13/india-s-new-internet-gateway-via-coxs-bazar-to-open-late-january-says-minister; "Agartala Becomes India's Third Internet Gateway", NDTV Gadgets, March 23, 2016, http://gadgets.ndtv.com/internet/news/agartala-becomes-indias-third-internet-gateway-817331.

91 Tripura to become 3rd international internet gateway of India, July 4 2015, http://news.webindia123.com/news/articles/India/20150704/2634628.html.

92 India, Submarine Cable Networks, http://www.submarinenetworks.com/stations/asia/india.

93 "Tata Communications Invests in Seaborn Networks' Undersea Cable", NDTV Gadgets, January 19, 2015, http://gadgets.ndtv.com/internet/news/tata-communications-invests-in-seaborn-networks-undersea-cable-650955.

94 India, Submarine Cable Networks, http://www.submarinenetworks.com/stations/asia/india.

95 "TRAI Specifies Access acilitation Charges for Submarine Cable Landing Stations", Ministry of Communication and Information Technology, December 21, 2012, http://pib.nic.in/newsite/erelease.aspx?relid=91106.

96 Indian Tower Industry: The Future is Data, Deloitte, June 2015, p. 7, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-media-telecommunications/in-tmt-indian-tower-industry-noexp.pdf.

97 Indian Tower Industry: The Future is Data, Deloitte, June 2015, p. 7, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-media-telecommunications/in-tmt-indian-tower-industry-noexp.pdf.

98 Indian Tower Industry: The Future is Data, Deloitte, June 2015, p. 7, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-media-telecommunications/in-tmt-indian-tower-industry-noexp.pdf.

99 Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators October – December 2015, May 18, 2016, p. 103, http://www.trai.gov.in/WriteReadData/PIRReport/Documents/QPIR_Oct_to_Dec-15.pdf.

100 Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators October – December 2015, May 18, 2016, p. 30, http://www.trai.gov.in/WriteReadData/PIRReport/Documents/QPIR_Oct_to_Dec-15.pdf.

101 Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators October – December 2015, May 18, 2016, p. 30, http://www.trai.gov.in/WriteReadData/PIRReport/Documents/QPIR_Oct_to_Dec-15.pdf.

102 Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators October – December 2015, May 18, 2016, p. 89, http://www.trai.gov.in/WriteReadData/PIRReport/Documents/QPIR_Oct_to_Dec-15.pdf.

103 Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators October – December 2015, May 18, 2016, p. 8, http://www.trai.gov.in/WriteReadData/PIRReport/Documents/QPIR_Oct_to_Dec-15.pdf.

104 Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators October – December 2015, May 18, 2016, p. 9, http://www.trai.gov.in/WriteReadData/PIRReport/Documents/QPIR_Oct_to_Dec-15.pdf.

The universal license framework, for which guidelines were published in November 2014,[105] reduced the legal and regulatory obstacles for companies by combining mobile phone and ISP licenses, instead of requiring separate licenses for each sector. Licensees must now pay a high one-time entry fee, a performance bank guarantee,[106] and annual license fees adjusted for revenue.[107]

In 2011, the Indian government introduced rules under Section 79 of the IT Act requiring cybercafes to obtain a government-issued ID number in addition to a license, as well as to register and monitor customers.[108] Critics said the rules were "poorly framed,"[109] but penalties for noncompliance are unclear, and enforcement has reportedly been patchy (Common Service Centers are exempt, and operate under separate guidelines).[110]

Regulatory Bodies

India's principal ICT institution is the Ministry of Communications and Information Technology.[111] It consists of two departments – the Department of Electronics and Information Technology (DeitY) and the Department of Telecommunications (DoT). DoT manages the overall development of the telecommunications sector, licenses internet and mobile service providers, and manages spectrum allocation;[112] DeitY formulates policy relating to information technology, electronics, and the internet.[113] In July 2016, the Ministry was divided in two. DeitY became the Ministry of Electronics and Information Technology (MeitY), while the DoT and Department of Posts were placed under the Ministry of Communications.[114]

Internet protocol (IP) addresses are regulated by the Indian Registry for Internet Names and Num-

105 Guidelines for Grant of Unified License, De artment of Telecommunications, November 13, 2014, http://www.dot.gov.in/sites/default/files/Amended%20UL%20Guidelines%2013112014.PD . Guidelines and General Information for grant of licence for operating internet services, 24 August 2007, available at: http://www.dot.gov.in/data-services/internet-services.

106 Draft License Agreement for Unified License, De artment of Telecommunications, Ministry of Communications and IT, page 22, available at: http://dot.gov.in/sites/default/files/Unified%20Licence_0.p .

107 Draft License Agreement for Unified License, De artment of Telecommunications, Ministry of Communications and IT, page 22, available at: http://dot.gov.in/sites/default/files/Unified%20Licence_0.p .Guidelines and General Information for grant of licence for operating internet services, 24 August 2007, available at: http://www.dot.gov.in/data-services/internet-services; Guidelines and General Information for grant of licence for operating internet services, 24 August 2007, available at: http://www.dot.gov.in/data-services/internet-services; The TRAI has recommended steps so as to incentivise telecom operators to expand operations by suggesting that revenue generated by these companies from their non-telecom activities be excluded while calculating their AGR. This would help to reduce the revenue share that these companies would have to pay to the government as well as reduce their license fees and spectrum charges. Shauvik Ghosh, Trai recommends non-telecom activity be excluded from AGR, Live Mint, 7 January 2015, available at: http://www.livemint.com/Industry/7ivGrxiayiOsumswo1KMlN/Trai-recommends-nontelecom-activity-be-excluded-from-AGR.html.

108 Department of Information Technology, Information Technology (Guidelines for Cyber Cafe) Rules, 2011, http://deity.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).p ; Notification, Minist y of Communications and Information Technology, March 16, 2012, http://deity.gov.in/sites/upload_files/dit/files/GSR153E_242012.p .

109 Bhairav Acharya, "Comments on the Information Technology (Guidelines for Cyber Cafe) Rules, 2011", Center for Information and Society, March 31, 2013, http://bit.ly/13KCBY5.

110 Department of Information Technology, Guidelines for the Implementation of the Common Service Centre Scheme in States, October 9, 2006, http://deity.gov.in/sites/upload_files/dit/files/down ads/policiesandguidelines/csc/cscguidelines.pdf.

111 Organizational Structure, Department of Telecommunications, Ministry of Communications & IT, Government of India, http://www.dot.gov.in/about-us/organizational-structure; Organization Chart, DeitY, Ministry of Communications & IT, Government of India, http://deity.gov.in/content/organization-chart.

112 Profile, De artment of Telecommunications, Ministry of Communications & IT, Government of India, http://www.dot.gov.in/about-us/profil .

113 Functions of Department of Electronics and Information Technology, Ministry of Communications & IT, Government of India, http://deity.gov.in/content/functions-deit.

114 http://economictimes.indiatimes.com/news/economy/policy/deity-becomes-a-new-ministry-leg-up-for-ravi-shankar-prasad/articleshow/53285683.cms

bers (IRINN).[115] Since 2005, the registry has functioned as an autonomous body within the nonprofit National Internet Exchange of India.[116]

The Telecom Regulatory Authority of India (TRAI), an independent regulator, was created in 1997 to regulate the telecom, broadcasting, and cable TV sectors.[117] The Telecom Regulatory Authority of India Act mandates transparency in the exercise of its operations, which include monitoring licensing terms, compliance, and service quality.[118] Its reports are published online, usually preceded by a multi-stakeholder consultation.[119] An amendment to the Act in 2000 established a three-member Telecommunications Dispute Settlement and Appellate Tribunal chaired by a former senior judge.[120] Yet appointment and salary decisions for members remain in the hands of the central government. Further, while the TRAI Act initially barred members who had previously held central or state government office, amendments in 2014 dilu ed that prohibition, allowing them to join the regulator two years after resigning that position, or earlier with permission from the central government. Members may undertake commercial employment, except with telecom service providers.[121]

TRAI opinions, however, are generally perceived as independent and largely free of official influence.[122] During the coverage period, it framed regulations prohibiting discriminatory tariffs for data services (see Digital Activism).[123]

Limits on Content

Content blocking of pornographic and terrorism related material and copyright restrictions continued to take place during the coverage period. There was a significant rise in digital mobilization, especially over net neutrality, resulting in strong regulations against differential pricing for data.

Blocking and Filtering

Blocking of websites takes place under Section 69A of the IT Act and a 2009 subordinate legislation called the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules ("Blocking Rules"). The Blocking Rules empower the central government to direct any agency or intermediary to block access to information when satisfied that it is "necessa y or expedient" in the interest of the "sovereignty and integrity of India, defense of India, security of the

115 IRINN, IRINN Policy Version 1.1, http://www.irinn.in/pages/static/IRINN_V1.pdf.

116 About Us, Indian Registry for Internet Names and Numbers, http://www.irinn.in/pages/static/about_us.html.

117 History, Telecom Regulatory Authority of India, http://www.trai.gov.in/Content/History.aspx.

118 Section 11(4), The Telecom Regulatory Authority of India Act, 1997.

119 "DTH operators should provide inter-operability of STBs, says TRAI Chairman", The Economic Times, December 10, 2013, http://articles.economictimes.indiatimes.com/2013-12-10/news/45035128_1_dth-operators-dth-licence-dth-service-providers; TRAI released the draft of: 'The Telecom Commercial Communications Customer Preference (Fifteenth Amendment) Regulations, 2014' for comments from the Stakeholders, January 29, 2014, http://www.trai.gov.in/WriteReaddata/ConsultationPaper/Document/draftTCCCP%2015%20AMEND%202014final.pd .

120 Section 14, The Telecom Regulatory Authority of India Act, 1997; The tribunal was empowered to adjudicate between the licensor (DoT) and the licensee; between two or more service providers; between a service provider and a group of consumers; and to hear appeals against TRAI decisions.

121 Amendment to the TRAI Act, 1997, http://www.prsindia.org/uploads/media/Recent%20Acts/Telecom%20Regulatory%20Act,%202014.pdf.

122 "Trai wants Auction of 3G Spectrum After Formation of New Govt", The Indian Express, February 12, 2014, http://archive.indianexpress.com/news/trai-wants-auction-of-3g-spectrum-after-formation-of-new-govt/1225198/.

123 TRAI Lays Down Historic Order Protecting Net Neutrality, The Wire, February 8, 2016, http://thewire.in/2016/02/08/trai-lays-down-historic-order-protecting-net-neutrality-21090/.

state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above."[124] Intermediaries failing to comply are punishable with fines and prison terms of up to seven years.[125]

The Blocking Rules apply to orders issued by government agencies, who must appoint a "nodal officer" to send in requests and demonstrate that they are necessary or expedient under Section 69A.[126] These requests are reviewed by a committee which includes senior representatives of the law, home affairs, and information ministries, and the nodal agency for cybersecurity, the Indian Computer Emergency Response Team (CERT-IN).[127] The "designated officer," who chairs the committee, issues approved orders to service providers; the committee must also notify the source or intermediary hosting the content, who may respond to defend it within 48 hours.[128]

In emergencies and upon written recommendations from the designated officer, the secretary of DEITY may issue blocking orders directly, but the content must be unblocked if the designated officer does not obtain the review committee's approval within 48 hours.[129]

Indian courts can order content blocks without government approval. The designated officer is required to implement the court order after submitting it to the secretary of DEITY. Court orders can be challenged in a higher court, but internet users are not consistently notified of their implementation.[130] ISPs are not legally required to inform the public of blocks and the Blocking Rules mandate that executive blocking orders be kept confidential [131] A 2014 transparency report issued by Verizon stated that the Indian government required the company to block access to websites, but that it was precluded by law from identifying how many blocking requests were received.[132]

The 2011 cybercafe rules stated that cybercafes "may" install commercial filtering software "to avoid access to the websites relating to pornography, obscenity, terrorism and other objectionable materials."[133] It is not clear how many complied.

In the landmark Shreya Singhal case decided by the Supreme Court in 2015, the petitioners challenged the constitutionality of Section 69A citing opaque procedures among other issues.[134] In March 2015, the Supreme Court upheld Section 69A and the Blocking Rules,[135] saying safeguards within the section were adequate, narrowly constructed, and not in contravention of the provisions of the Constitution of India.[136] At the same time, the court read the Blocking Rules to include both

124 Section 69A(1), The Information Technology Act, 2008.

125 Section 69A(3), The Information Technology Act, 2008.

126 Rule 6, Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

127 Members must be of the rank of joint secretary or above, see Rule 7, Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

128 Rule 8, Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

129 Rule 9, Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

130 Melody Patry, "Index on censorship digital freedom India: Digital freedom under threat?", *Xindex*, November 2013, p. 9, http://www.indexoncensorship.org/2013/11/india-online-report-freedom-expression-digital-freedom-1/; See also Jyoti Panday, The Internet Has a New Standard for Censorship, The Wire, 29 January 2016, http://thewire.in/20386/the-internet-has-a-new-standard-for-censorship/.

131 Rule 16, Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

132 "Verizon Releases Transparency Report", January 22, 2014, http://newscenter.verizon.com/corporate/news-articles/2014/01-22-verizon-releases-transparency-report/.

133 Rule 6(5), Information Technology (Guidelines for Cyber Cafe) Rules, 2011.

134 Common Cause v. Union of India [W.P.(C) No. 21 of 2013]; PUCL v. Union of India [W.P.(Crl) No. 199 of 2013].

135 Shreya Singhal v Union of India, (2015) 5 SCC 1.

136 Shreya Singhal v Union of India, (2015) 5 SCC 1.

the right to be heard and the right to appeal, changing the way Section 69A has been interpreted. It is now clear that blocking orders must provide a written explanation, allowing them to be challenged by writ petition, and that reasonable efforts must be made to contact the originator of the content for a pre-decisional hearing before the blocking order is issued.[137] However, given the requirement in the Blocking Rules that the orders and actions based on them be kept confidential [138] it remains to be seen how and whether the judgment will be effectively implemented.[139]

According to a statement made in Parliament by the Minister of Communication and Information Technology, the government blocked 844 social media pages between January and November 2015. Among these, 492 URLs were blocked under Section 69A, and 352 were blocked in compliance with court orders.[140]

In most cases, there is no information about the content targeted through these orders. However, there were some reports of overbroad content blocking affecting legitimate online activity. In February 2016, the DOT ordered ISPs to block jihadology.net, an online academic repository curating primary source material on the Arab Spring,[141] even though news reports said ISIS recruitment videos remained easily accessible through Google search after a campaign by the anti-terrorism squad resulted in 94 websites being reportedly blocked.[142] In another case in May 2016, the domain names marketplace BuyDomains.com was blocked by some ISPs and mobile internet providers. Visitors were informed that the URL was "blocked under instructions of the Competent Government Authority or in compliance to the orders of Hon'ble Court," with no further details given.[143]

Since 2011, courts have blocked content relating to copyright violations through broad John Doe orders, which can be issued preemptively and do not name a defendant.[144] ISPs have occasionally implemented such orders by blocking entire websites instead of individual URLs, irrespective of whether the websites were hosting pirated material.[145] In 2012, the Madras High Court ruled that John Doe orders should not be used to block entire websites.[146]

These potentially overbroad orders continue to be issued.[147] In July 2015, Phantom Films were granted a John Doe order by the Bombay High Court for blocking websites that may be used to pirate its

137 Chinmayi Arun, "The Case of the Online Intermediary," The Hindu, April 7, 2015, http://www.thehindu.com/opinion/op-ed/shreya-singhal-case-of-the-online-intermediary/article7074431.ece.

138 Rule 16, Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

139 Chinmayi Arun, "The Case of the Online Intermediary," The Hindu, April 7, 2015, http://www.thehindu.com/opinion/op-ed/shreya-singhal-case-of-the-online-intermediary/article7074431.ece.

140 PTI, "Government Blocked 844 Social Media Pages Till November: Prasad, NDTV, December 18,2015, http://gadgets.ndtv.com/social-networking/news/government-blocked-844-social-media-pages-till-november-prasad-779619

141 Shashidhar KJ, "Government blocks Jihadology, an academic site on source material from Jihadis", Medianama, February 3, 2016, http://www.medianama.com/2016/02/223-jihadology-internet-blocks/

142 Zeeshan Sheikh, "Sites blocked but ISIS literature, videos freely available on Internet", Indian Express, January 30, 2016, http://indianexpress.com/article/cities/mumbai/sites-blocked-but-isis-literature-videos-freely-available-on-internet/

143 Riddhi Mukherjee, "BuyDomains blocked once again in India", Medianama, May 27, 2016, http://www.medianama.com/2016/05/223-buydomains-blocked-once-again-in-india/.

144 Kian Ganz, "Update: Bombay HC Passes First Anti-piracy John Doe Order, as Law Firms Commoditise the New Vertical", *Legally India,* June 15, 2012,http://bit.ly/KIibkI. These orders are passed by virtue of the inherent powers of the court under Section 151 of the Civil Procedure Code read with Rule 1 and Rule 2 of Order 39 of the Civil Procedure Code which deal with temporary injunctions.

145 Ananth Padmanabhan, "Can Judges Order ISPs to block websites for Copyright Infringement", January 30, 2014, *Center for internet and Society*, http://cis-india.org/a2k/blog/john-doe-orders-isp-blocking-websites-copyright-1.

146 M/s. R.K. Productions Pvt. Ltd. v. Bharat Sanchar Nigam Limited & 19 Others, C.S.(OS) 208/ 2012 (June 22, 2012), The High Court of Judicature at Madras (India).

147 Nikhil Pahwa, Four John Doe orders for blocking websites in the last month alone, Medianama, June 13, 2016, http://www.medianama.com/2016/06/223-john-doe-orders-india/.

movie 'Masaan'. In October 2015, the Delhi High Court granted a John Doe order to Fox Star Studios for the movie 'Prem Ratan Dhan Payo.' Similar orders were issued throughout the year by various High Courts.[148] Separately, in October 2015, the IT minister for the State of Telangana met with police officials, ISPs and epresentatives of the Telugu film indust y to address movie piracy, citing loss in industry revenue. Following this, ISPs were directed to block around 200 unspecified ebsites to prevent piracy.[149]

The IT Act and the Indian Penal Code prohibit the production and transmission of "obscene material,"[150] but there is no specific law against viewing po nography in India, except child pornography, which is prohibited under the IT Act.[151] In the case of *Kamlesh Vaswani v. Union of India*, the petitioner asked the Supreme Court to direct the government to block all online pornography in India.[152] In the past, the government has informed the Supreme Court that it is not technically feasible to block pornographic sites and that doing so would violate the constitution.[153]

On July 31, 2015, however, the DoT ordered ISPs to block access to 857 URLs for allegedly pornographic content.[154] The notification said that the ebsites were found to be violating morality and decency under Article 19(2) of the Constitution of India, read with Section 79(3)(b) of the IT Act.[155] There was widespread outrage over the ban on social media, and a few days later the government reversed it.[156] Subsequently, the government informed the Supreme Court in the Kamlesh Vaswani matter that it would only block child pornography,[157] on grounds that the government did not want to indulge in "moral policing" or become a totalitarian state.[158]

While the ban was withdrawn, officials old ISPs that they were "free not to" disable any of the 857 URLs, as long as the URLs did not host child pornography,[159] effectively putting the onus on the ISPs to decide on the legality of the content on a case-by-case basis. Most ISPs continued to block the

148 Nikhil Pahwa, Four John Doe orders for blocking websites in the last month alone, Medianama, June 13, 2016, http://www.medianama.com/2016/06/223-john-doe-orders-india/.

149 "Telangana plans anti-piracy policy to save films , Deccan Chronicle, October 29, 2015, http://www.deccanchronicle.com/151029/nation-current-affairs/article/telangana-plans-anti-piracy-policy-save-film

150 Section 67, The Information Technology Act 2000.

151 Section 67(B), The Information Technology Act 2000.

152 W.P.(C).No. 177 of 2013.

153 Chinamyi Arun and Sarvjeet Singh, "Online Intermediaries in India," available at: http://ccgtlr.org/wp-content/uploads/2015/02/CCG-at-NLUD-NOC-Online-Intermediaries-Case-Studies.pdf.

154 Order no. 813-7/25/2011-DS (Vol.-V), available at: http://cis-india.org/internet-governance/resources/dot-morality-block-order-2015-07-31/at_download/fil ; "India blocks access to 857 porn sites", BBC, August 3, 2015, http://www.bbc.com/news/world-asia-india-33754961.

155 http://cis-india.org/internet-governance/resources/dot-morality-block-order-2015-07-31/at_download/fil .

156 Nadia Khomami, "India lifts ban on internet pornography after criticism", The Guardian, August 5, 2015, http://www.theguardian.com/culture/2015/aug/05/india-lifts-ban-on-internet-pornography-after-criticisms; Aditya Kalra, "India withdraws order to block pornography sites," Reuters, August 5, 2015, http://in.reuters.com/article/2015/08/05/india-porn-ban-idINKCN0QA0KK20150805.

157 Sarvjeet Singh, "We are not a totalitarian state and cannot be asked to moral police: AG tells SC in the Porn Petition", CCG-NLU Blog, August 10, 2015, https://ccgnludelhi.wordpress.com/2015/08/10/we-are-not-a-totalitarian-state-and-cannot-be-asked-to-moral-police-ag-tells-the-sc-in-the-porn-petition/.

158 Sarvjeet Singh, "We are not a totalitarian state and cannot be asked to moral police: AG tells SC in the Porn Petition", CCG-NLU Blog, August 10, 2015, https://ccgnludelhi.wordpress.com/2015/08/10/we-are-not-a-totalitarian-state-and-cannot-be-asked-to-moral-police-ag-tells-the-sc-in-the-porn-petition/; Krishnadas Rajagopal, "Not for moral policing: Centre, The Hindu, August 11, 2015, http://www.thehindu.com/news/national/central-government-on-pornography-ban-we-are-not-a-totalitarian-state/article7522036.ece.

159 Leo Mirani, India has lifted its online porn ban-ISPs are going to keep blocking it anyway", Quartz, August 05, 2015, http://qz.com/473063/india-has-lifted-its-online-porn-ban-but-isps-are-going-to-keep-blocking-it-anyway/.

full list,[160] calling the instruction "vague and un-implementable."[161] In January 2016, news reports said telecom companies and ISPs were considering an agreement with New Zealand-based technology company Bypass Network Services to introduce parental controls over pornographic content.[162]

Content Removal

A 2008 IT Act amendment protected technology companies from legal liability for content posted to their platforms by others, with reasonable exceptions to prevent criminal acts or privacy violations.[163] Intermediaries Guidelines issued in 2011 under Section 79 of the IT Act required intermediaries to remove access to certain content within 36 hours of a user complaint.[164] In the 2015 judgment of *Shreya Singhal v. Union of India,* the Supreme Court read down Section 79 and the intermediary guidelines,[165] and companies are no longer required to act on user complaints.[166] Court and government takedown orders, furthermore, are only legitimate if they fall within the reasonable restrictions provided for under Article 19(2) of the constitution. Unlawful content beyond the ambit of Article 19(2) cannot be restricted. Thus, the court restricted the earlier broad grounds for takedown notices.[167]

Intermediaries can separately be held liable for infringing the Copyright Act 1957,[168] under the law and licensing agreements.[169] The Shreya Singhal decision has had no impact on the legal framework on intermediary liability for copyright infringement. A 2012 amendment limited liability for intermediaries such as search engines that link to material copied illegally, but mandated that they disable public access for 21 days within 36 hours of receiving written notice from the copyright holder, pending a court order to remove the link.[170] Rules clarifying the amendment in 2013 gave intermedi-

160 Nikhil Pahwa, Ïndia's porn ban hasn't exactly been lifted: it's conditional & up to the ISPs", Medianama, August 4, 2015, http://www.medianama.com/2015/08/223-porn-india-ban/.

161 Nikhil Pahwa, Ïndia's porn ban hasn't exactly been lifted: it's conditional & up to the ISPs", Medianama, August 4, 2015, http://www.medianama.com/2015/08/223-porn-india-ban/.

162 TNM Staff, "Soon parents in India may be able to prevent their children from watching porn", News Minute, January 19, 2016, http://www.thenewsminute.com/article/soon-parents-india-may-be-able-prevent-their-children-watching-porn-37876.

163 Section 79, The IT (Amendment) Act 2008; Section 72A, IT (Amendment) Act, 2008.

164 Rule 3, Information Technology (Intermediaries Guidelines) Rules, 2011,; Pritika Rai Advavi, "Intermediary Liability in India", http://www.epw.in/special-articles/intermediary-liability-india.html.

165 Shreya Singhal v Union of India, (2015) 5 SCC 1.

166 Shreya Singhal v Union of India, (2015) 5 SCC 1.

167 Shreya Singhal v Union of India, (2015) 5 SCC 1.

168 In the Copyright Act, 1957, Section 51(a)(ii) read with Section 63 of Act the criminalizes use of any place for profit for the communication of the work to the public where such communication constitutes an infringement of the copyright, exempting only those who are unaware or have no reasonable grounds for believing that such communication would constitute infringement of copyright. Moreover, Section 51(b) read with Section 63 also prohibits sale, hire, or distribution to the prejudice of the copyright owner, as well as exhibition in public and import to India of infringing copies also amount to infringement of copyright, with no exemptions. See, Pritika Rai Advani , "Intermediary Liability in India", Economic & Political Weekly, December 14, 2013, Vol. XLVIII No. 50, p. 122.

169 The guidelines and license requirements for intermediaries also prohibit the carrying of communication that infringes copyright or other intellectual property rights. Guideline 1.3(27), Guidelines and General Information for Grant of License for Operating internet Services, http://www.dot.gov.in/data-services/internet-services; Unified License Ag eement, Rule 38, http://www.dot.gov.in/sites/default/files/Amended pe cent20UL percent20Agreement_0.pdf.

170 Specificall , any providers offering "transient or incidental storage of a work or performance purely in the technical process of electronic transmission or communication to the public" through "links, access or integration." See, Pranesh Prakash, "Analysis of the Copyright (Amendment) Bill 2012," Center for Internet and Society, May 23, 2012, http://bit.ly/JSDMLg; Ministry of Law and Justice, "Copyright (Amendment) Act 2012", June 7, 2012, http://bit.ly/Kt1vlQ.

aries power to assess the legitimacy of the notice from the copyright holder and refuse to comply.[171] However, critics said the language was vague.[172]

Separately, private companies disabled content from being viewed within India during the coverage period. Users disputed some of those interventions. In May 2015, the nonprofit o ganization Sikhs for Justice said Facebook had blocked its Indian page;[173] the page was accessible again in 2016. Administrators for the Facebook pages "Indian Atheists," and "Indian Atheists Debate corner" said their pages had been temporarily blocked by the platform in June.[174] The reason for these interruptions is not clear. In November 2015, Facebook users were temporarily unable to share news articles from Facebook pages operated by websites *The Wire*,[175] and *Faking News*,[176] but the content was later reinstated. A Facebook spokesperson said that the content was mistakenly identified as s am.[177]

Several international companies reported receiving a high number of requests to remove content from Indian courts or government representatives. Facebook reported removing over 30,000 pieces of content based on these requests in 2015, up from 11,000 in 2014,[178] but said it would require more formal notification o do so in 2016 based on the Supreme Court's ruling in *Shreya Singhal v. Union of India*.[179]

Google reported receiving 259 content removal requests affecting 1,606 items between July and December 2015, and said it complied with 38 percent of requests based on court orders and 10 percent from government agencies and law enforcement. The reason most commonly cited for the request was defamation.[180]

Twitter received 40 requests for content removal from July to December 2015, of which 1 was court ordered and 39 were from police or government agencies, but said it did not comply.[181]

Media, Diversity, and Content Manipulation

Online media content is diverse and lively. The internet has given a voice to people in remote areas, helping them become a part of the public discourse. During the coverage period, the Dalit Camera

171 Ministry of Human Resource Development, "Copyright Rules 2013", March 14, 2013, http://bit.ly/YrhCS5.

172 Chaitanya Ramachandran, "Guest Post: A Look at the New Notice and Takedown Regime Under the Copyright Rules, 2013", Spicy IP, April 29, 2013, http://bit.ly/16zSzWf.

173 John Ribeiro, 'Facebook sued in US court for blocking page in India", PC World, June 3, 2015, http://www.pcworld.com/article/2930872/facebook-sued-in-us-court-for-blocking-page-in-india.html

174 Sneha Johari, Facebook blocks and unblocks Indian Atheist page in 48 hours; reason?", Medianama, June 8, 2015, http://www.medianama.com/2015/06/223-facebook-blocks-indian-atheists-page/

175 Satyabrata Pal, "When Mr. Modi went to London:, The Wire, November 17, 2015, http://thewire.in/2015/11/17/when-mr-modi-went-to-london-15802/

176 Prachand Patrakar, "When dogs decide not to bark", Faking News, November 14, 2015. http://my.fakingnews.fi stpost.com/2015/11/14/dogs-decide-not-to-bark/

177 Sneha Johari," Facebook blocks certain news articles; transparency?", Medianama, November 19,2015, http://www.medianama.com/2015/11/223-facebook-blocks-news-articles-india/

178 Facebook transparency report, July-December 2015 accessed at: https://govtrequests.facebook.com/country/India/2015-H2/

179 [Note: In 2016, informed by the decision of the Supreme Court of India last year amending the proper interpretation of the Information Technology Act 2000, we ceased acting upon legal requests to remove access to content unless received by way of a binding court order and/or a notification by an authorised agency which conforms to the constitutional safeguards as directed by the Supreme Court.]" http://govtrequests.facebook.com/country/India/2015-H2/

180 Google Tranperancy Report, January to June 2015, accessed at: https://www.google.com/transparencyreport/removals/government/IN/

181 https://transparency.twitter.com/removal-requests/2015/jul-dec

Action YouTube channel was established to address the lack of Dalit voices in the mainstream media.[182] It provides original content and reposts media related to Dalits, a traditionally marginalized group in the Hindu caste system. The mobile news service CGNetSwara allows people in rural areas of central India to submit and listen to audio news reports, averaging 200 calls per day and driving the emergence of online reports on local issues that do not reach the mainstream media.[183] The Delhi-based company Gram Vaani operates a Mobile Vaani initiative using an interactive voice response system to disseminate reports by mobile phone users to different audiences and stakeholders. It enables over 80,000 households across 12 states to create their own media.[184]

In general, self-censorship is not widespread. Internet users in conflict egions may avoid addressing sensitive political or religious issues which other journalists and activists report freely. Some institutions and individual writers self-censor due to fear of reprisal from political organizations.[185] No noteworthy examples of self-censorship were documented during the coverage period, though the issue was discussed. In July 2015, the *Economic Times* took down a news report published in the June 30, 2015 edition of the paper from its website, titled, "Sec 377 maybe scrapped says Gowda."[186] Section 377 of the penal code criminalizes homosexuality. Law Minister Sadananda Gowda said on Twitter that the *Times* had misquoted him in the article,[187] but observers commented on the unusual nature of the retraction, suggesting it indicated self-censorship amid a "drought of progressivism."[188] Writers and other public figu es separately reported being subject to abuse on social media for criticizing what they described as religious intolerance.[189] However, there were no reports of paid commentators manipulating political content.

Social media and communication apps drew some increased scrutiny. In February 2016, news reports said the government was setting up a special media cell, the National Media Analytics Centre (NMAC), to monitor online narratives perceived to be against the government, and counter them with positive press releases and other campaigns.[190]

In an unprecedented move, the District Magistrate of Kupwara, a district in Jammu and Kashmir, issued a notice in April 2016 requiring administrators of WhatsApp groups sharing news to register

182 Amrit Dhillon, "Dalit Voices, loud and clear", The Hoot, February 2, 2016, http://www.thehoot.org/media-watch/media-practice/dalit-voices-loud-and-clear-9148

183 "India: Use Mobile Technology to Bring News to Isolated Tribal Communities", International Centre for Journalists, available at: http://www.icfj.org/knight-international-journalism-fellowships/fellowships/india-using-mobile-technology-bring-news-is-0.

184 "Gram Vaani", http://www.gramvaani.org/; "How Mobile Vaani Works", http://www.gramvaani.org/?page_id=15.

185 "Literary Censorship in the era of Internet," Times of India, February 21, 2015, http://timesofindia.indiatimes.com/city_chandigarh/Literary-censorship-in-the-era-of-internet/articleshow/46319279.cms

186 Scroll Staff, "Not only is BJP refusing to scrap Section 377, it's back to saying gays have a 'genetic disorder'", Scroll.in, June 30, 2015, http://scroll.in/article/737871/not-only-is-bjp-refusing-to-scrap-section-377-its-back-to-saying-gays-have-a-genetic-disorder

187 Sadananda Gowda @DVSBJP tweet on: 10:18 PM, June 29, 2015 accessed at: https://twitter.com/DVSBJP/status/615751206535720960?ref_src=twsrc%5Etfw

188 Vikram Johri, "A strange retraction", The Hoot, July 1, 2015, http://www.thehoot.org/media-watch/media-practice/a-strange-retraction-8420

189 David Barstow and Suhasini Raj, "Indian Writers Return Awards to Protest Government Silence on Violence," New York Times, October 17, 2015, http://www.nytimes.com/2015/10/18/world/asia/india-writers-return-awards-to-protest-government-silence-on-violence.html?_r=0

190 Ministry of Truth: New government cyber cell will weed out 'negative narratives' against state, track those inciting 'trouble', http://www.fi stpost.com/india/ministry-of-truth-new-government-cyber-cell-will-will-weed-out-negative-narratives-against-state-track-those-inciting-trouble-2640812.html?utm_source=fp_hp.

with the local District Social Media Centre.[191] The administrators would be liable for "any irresponsible remarks/deals [sic] leading to untoward incidents" posted by group members, according to the notice,[192] which followed a week of violence after the alleged rape of an underage girl by army personnel.[193] Local media and student organizations objected,[194] and how the notice will be enforced remains unclear.

Digital Activism

Throughout 2015, civil society groups used digital tools to mobilize public opinion on net neutrality, the principle that providers should not discriminate against certain content or data.

In December 2014, Bharti Airtel considered preventing customers with regular mobile data packages from accessing Voice over Internet Protocol (VoIP) applications, angering consumers.[195] Separately in February 2015, Facebook launched Internet.org—later renamed Free Basics—in collaboration with Reliance Communications and other corporations. The service offered limited offline access o certain websites at no cost for Reliance customers without full internet access.[196] Facebook described the program as a means to provide some experience of the internet to communities who would otherwise go without,[197] but consumers feared it would erode net neutrality by establishing companies as the arbiters of which content and services would be available for free.[198] Others criticized the program as interest philanthropy, resulting in profits for articipating companies under the guise of improving access,[199] and questioned the security implications of routing users' personal data and web traffic th ough servers operated by a single company, making them more vulnerable to cyberattack or surveillance.[200] Facebook addressed some of these concerns, opening Free Basics to a wider range

191 Vivek Pai, ""WhatsApp news groups "need to register with Social Media Centre in Kashmir", Medianama, April 19, 2016, http://www.medianama.com/2016/04/223-whatsapp-newsgroups-register-kashmir/; Speed News Desk, "Admins of news WhatsApp groups in Jammu and Kashmir now need a license", Catch News, April 29, 2016, http://www.catchnews.com/national-news/whatsapp-group-admins-need-to-get-license-in-jammu-and-kashmir-1461057064.html

192 Circular No. DCK/PS/2016/(160)297-305, Office of the District Magistrate, Kupawara, Government of Jammu and Kashmir, accessed at: https://www.facebook.com/photo.php?fbid=10209244433244907&set=a.4691370079246.193446.1143830745&type=3&theater

193 Toufiq Rashid, "WhatsApp groups sharing news in Kashmir Valley must register: Govt", Hindustan Times, April 19, 2016, http://www.hindustantimes.com/india/jammu-and-kashmir-whatsapp-groups-spreading-local-news-should-register-with-magistrate-within-10-days/story-ENBuUIoNeFRKLCOIDVX3HN.html

194 PTI, "Mixed views on directive to WhatsApp news groups in Kashmir", India Today, April 20, 2016, http://indiatoday.intoday.in/story/mixed-views-on-directive-to-whatsapp-news-groups-in-kashmir/1/646988.html

195 "For Skype, Airtel will charge Rs 75 for 75MB, postpaid packs soon," *The Financial Express*, December 27, 2014, http://www.financialexp ess.com/article/industry/tech/for-skype-airtel-will-charge-rs-75-for-75mb-postpaid-packs-soon/23571/; "Government to Look Into Airtel's Plan to Charge for Internet Calls: Ravi Shankar Prasad," NDTV, December25, 2014, http://gadgets.ndtv.com/telecom/news/government-to-look-into-airtels-plan-to-charge-for-internet-calls-ravi-shankar-prasad-639713; Yuthika Bhargava, "Airtel drops plans to charge extra for internet voice calls," *The Hindu*, December31, 2014,http://www.thehindu.com/business/Industry/airtel-will-not-charge-extra-for-internet-voice-calls-via-skype-viber/article6735030.ece.

196 Lalatendu Mishra and Sriram Srinivasan, "Facebook launches internet.org in India," The Hindu, February 11, 2015, http://www.thehindu.com/business/Industry/facebook-launches-internetorg-in-india/article6879310.ece.

197 Anuj Srivas, "The Rundown on TRAI, Net Neutrality and How it Affects India", The Wire, February 11, 2016, http://thewire.in/2016/02/11/the-rundown-on-trai-net-neutrality-and-how-it-affects-india-21301/; Sonam Joshi, "Facebook initiates blitzkrieg ad campaign for Free Basics in India ahead of Dec. 31 deadline", Mashable, December 23, 2015, http://mashable.com/2015/12/23/facebook-free-basics-net-neutrality-india/.

198 Prabir Purkayastha, Internet Power to the People, February 10 2016, The Hindu, http://www.thehindu.com/opinion/lead/trai-bats-for-net-neutrality-internet-power-to-the-people/article8214991.ece.

199 Mahesh Murthy, "Facebook is Misleading Indians With its Full-page Ads About Free Basics", December 26, 2015.

200 Andrew McLaughlin, "The Hacker Way Forward: how Facebook Can Fix 'Free Basics' in Two Simple Moves", Medium, March 27, 2016, https://medium.com/@mcandrew/the-hacker-way-forward-how-facebook-can-fix-f ee-basics-in-two-simple-moves-86392758058#.mhkic4s4i .

of content providers, among other measures, but Free Basics remained widely identified with the net neutrality controversy unfolding in parallel over differential pricing.[201]

The TRAI initially supported service providers, and outlined a regulatory framework for consumers to pay for communications applications such as Viber, Skype, and WhatsApp in a March 2015 consultation paper.[202] More than a million people submitted comments opposing the measure, arguing that it violated net neutrality principles.[203] On December 9, 2015, the TRAI conducted a public consultation on the subject,[204] and produced a second consultation paper.[205] This second consultation involved more than half a million people,[206] including academic institutions[207], civil society groups[208], digital activists, and the public,[209] as well as telecommunications companies and a robust counter campaign by Facebook.[210] Following this, the TRAI issued a tariff order on February 8, 2016 explicitly prohibiting differential pricing for data services.[211] This order meant that proposals to charge consumers different prices for select content or applications, including Free Basics, were "effectively declared illegal."[212]

Violations of User Rights

There was a sharp increase in the number of arrests for online speech during the coverage period. Seventeen people were arrested for content distributed on WhatsApp; other cases involved Facebook content. The Supreme Court upheld laws criminalizing defamation, which will impact online speech. The Central Monitoring System was reported to have become operational through regional monitoring centers in New Delhi and Mumbai from May 2016.

Legal Environment

The Constitution of India grants citizens the fundamental right to freedom of speech and expres-

201 Eric Stallman, "Was India right in banning Facebook's Free Basics?" , Quartz, February, 11, 2016, http://qz.com/615342/was-india-right-in-banning-facebooks-free-basics/.

202 See TRAI Consultation Paper on Regulatory Framework for Over-the-top (OTT) services, Consultation Paper No. 2/2015, March 27, 2015, http://www.trai.gov.in/WriteReaddata/ConsultationPaper/Document/OTT-CP-27032015.pdf.

203 "Parliamentary Committee to discuss net neutrality issue on Thursday," DNA, May 20, 2015, http://www.dnaindia.com/india/report-parliamentary-committee-to-discuss-net-neutrality-issue-on-thursday-2087575.

204 "TRAI Consultations Paper on Differential Pricing for Data Services," Consultation paper No. 8/2015, December 9, 2015, http://www.trai.gov.in/WriteReaddata/ConsultationPaper/Document/CP-Differential-Pricing-09122015.pdf.

205 Siddharth Manohar, "TRAI releases Regulations enforcing Net Neutrality, prohibits Differential Pricing", CCG Blog, February 8, 2016, https://ccgnludelhi.wordpress.com/2016/02/08/trai-releases-regulations-enforcing-net-neutrality-prohibits-differential-pricing/.

206 "TRAI Consultations Paper on Differential Pricing for Data Services," Consultation paper No. 8/2015, December 9, 2015, http://www.trai.gov.in/WriteReaddata/ConsultationPaper/Document/CP-Differential-Pricing-09122015.pdf.

207 Centre for Communication Governance at National Law University, Delhi, "Comments on TRAI's Consultation paper on Differential Pricing for Data Services," January 7, 2016, https://drive.google.com/file/d/0B_cAZd9M5_7NNHQxemwxVDBzMnc/view?usp=sharing.

208 Joint academic and civil society counter comment to TRAI's Consultation Paper on Differential Pricing of Data Services, January 14, 2016 (on file with the autho s).

209 www.Savetheinternet.in.

210 "Save Free Basics", https://www.facebook.com/savefreebasics.

211 Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016 accessed at: http://www.trai.gov.in/WriteReadData/WhatsNew/Documents/Regulation_Data_Service.pdf.

212 Rahul Bhatia, "The inside story of Facebook's biggest setback", May 12, 2016, The Guardian, https://www.theguardian.com/technology/2016/may/12/facebook-free-basics-india-zuckerberg.

sion,[213] including the right to gather information and exchange thoughts with others within and outside of India.[214] Press freedom has been read into the freedom of speech and expression.[215] These freedoms are subject to certain restrictions in the interests of state security, friendly relations with foreign states, public order, decency and morality, contempt of court, defamation, incitement to an offense, and the sovereignty and integrity of India. However, these restrictions may only be imposed by a duly enacted law and not by executive action.[216] The right to privacy has been read into the right to life guaranteed by Article 21 of the constitution.[217]

The Indian Penal Code (IPC) criminalizes several kinds of speech, and applies to online content. Individuals could be punished with a jail term ranging from two to seven years for speech that is found to be seditious,[218] obscene,[219] defamatory,[220] "promoting enmity between different groups on ground of religion, race, place of birth, residence, language,"[221] committing acts "prejudicial to maintenance of harmony,"[222] or consisting of statements, rumors, or reports that may cause fear, alarm, disturb public tranquility, or promote enmity or ill will.[223] Internet users are also subject to criminal punishment under the Official Sec ets Act for wrongful communication of information that may have an adverse effect on the sovereignty and integrity of India.[224]

The IT Act criminalizes certain online activity in particular. The act bans the publication or transmission of obscene or sexually explicit content in electronic form, and the creation, transmission or browsing of child pornography.[225]

Section 66A of the IT Act, which criminalized information causing "annoyance," "inconvenience," or "danger," among other ill-defined ca egories, led to several arrests for social media posts from 2012 through early 2015 before it was struck down by the Supreme Court on March 24, 2015.[226] The court affi med that freedom of speech online is equal to freedom of speech offline, and held that Section 66A was an arbitrary and disproportionate invasion of the right to free speech outside the reasonable restrictions specified in A ticle 19(2) of the constitution.[227]

A more recent Supreme Court judgment upheld laws criminalizing defamation (Sections 499 and 500 of the IPC and Section 119 of the Code of Criminal Procedure) as consistent with the Indian

213 Article 19(1)(a), The Constitution of India.
214 Maneka Gandhi v. Union of India, 1978 AIR 597.
215 Report of the Press Commission, Part I, 1954, Government of India, p. 357.
216 Article 19(2), The Constitution of India; Bijoe Emmanuel v. State of Kerala, (1986) 3 SCC 615.
217 R Rajagopal v. State of Tamil Nadu AIR 1995 SC 264; Kharak Singh v. State of UP (1975) 2 SCC 148.
218 Section 124A, The Indian Penal Code, 1860.
219 Section 292 and 293, The Indian Penal Code, 1860.
220 Section 499, The Indian Penal Code, 1860.
221 Section 153A, The Indian Penal Code, 1860.
222 Section 153B, The Indian Penal Code, 1860.
223 Section 505, The Indian Penal Code, 1860.
224 Section 5, Official Sec ets Act, 1923.
225 Section 67, Section 67A, Section 67B The Information Technology Act, 2000.
226 (2015) 5 SCC 1.
227 Ujwala Uppaluri and Sarvjeet Singh, "Supreme Court ruling on Section 66A: As much online as offline" The Economic Times, March 25 2015, http://blogs.economictimes.indiatimes.com/et-commentary/supreme-court-ruling-on-section-66a-as-much-online-as-offline .

Constitution.[228] This judgment has a significant im act on internet freedom, as the sections are often invoked against online speech and dissent.[229]

Prosecutions and Detentions for Online Activities

In a new and worrying trend, multiple people were arrested across India for online speech, including seventeen for content distributed on WhatsApp.[230] This includes three WhatsApp group administrators who were arrested for material posted by third parties in their groups.[231]

Arrests based on social media content have been documented in India in the past under Section 66A of the IT Act, but outstanding prosecutions were dropped after the Supreme Court declared it unconstitutional in March 2015.[232] During the coverage period, charges were filed ins ead under the penal code or other sections of the IT Act, such as Section 67, which prohibits the transmission of obscene content via electronic media, or Section 66D, which prohibits use of computer resources to impersonate someone else to commit fraud.

The following prosecutions involving posts shared on WhatsApp occurred during this coverage period:

- In June 2015, a WhatsApp group administrator was arrested in Nagpur, Maharashtra for posting content that "hurt the religious sentiments" of another member of the group. He was remanded to magisterial custody and later released on bail.[233]
- In July 2015 police in Moradabad, Uttar Pradesh, arrested a school student for objectionable images and text on WhastApp which triggered communal tension; news reports said a

228 Subramanian Swamy v Union of India (2016), http://supremecourtofindia.nic.in/FileSe ver/2016-05-13_1463126071.pdf; Nakul Nayak, "Supreme Court finds Criminal Defamation Constitutional , CCG-NLU Blog, May 13, 2016, https://ccgnludelhi.wordpress.com/2016/05/13/supreme-court-finds-criminal-defamation-constitutional ; Nakul Nayak, "Criminal defamation survives: a blot on free speech", Mint, May 22, 2016, http://www.livemint.com/Opinion/Zx8Qs60DFFqJ7bjYBoaGjO/Criminal-defamation-survives-a-blot-on-free-speech.html.

229 Chinmayi Arun, "A question of power", Indian Express, May 25, 2016, http://indianexpress.com/article/opinion/columns/criminal-defamation-law-supreme-court-2817406/; SC upholds law on criminal defamation, The Hindu, May 13 2016 , http://www.thehindu.com/news/national/criminal-defamation-does-not-have-chilling-effect-on-free-speech-sc/article8594163.ece.

230 See: WhatsApp admin held for hurting religious sentiment, Nagpur Today, June 2015, http://www.nagpurtoday.in/whatsapp-admin-held-for-hurting-religious-sentiment/06250951; Class XI student nabbed for objectionable post, The Times of India, July 6 2015, http://timesofindia.indiatimes.com/city/lucknow/Class-XI-studen -nabbed-for-objectionable-post/articleshow/47951424.cms; Milind Ghatwani, Timeline: Story of the Vyapam scam, July 8 2015, The Indian Express, http://indianexpress.com/article/explained/across-the-board-vyapams-spread/; Siddharth Ranjan Das, 4 Arrested for WhatsApp Messages on Shivraj Singh Chouhan Granted Bail, NDTV, July 28 2015, http://www.ndtv.com/india-news/4-arrested-for-whatsapp-messages-on-shivraj-singh-chouhan-granted-bail-1201375; Ishita Mishra, Maharashtra cops arrest UP teen for Whatsapp text that stirred riot, The Times of India, November 8 2015, http://timesofindia.indiatimes.com/city/agra Maharashtra-cops-arrest-UP-teen-for-Whatsapp-text-that-stirred-riot/articleshow/49705130.cms; WhatsApp group admin arrested for objectionable content, The Hindu , October 8 2015, http://www.thehindu.com/news/national/other-states/whatsapp-group-admin-arrested-for-objectionable-content/article7738538.ece. .

231 Whatsapp admin held for hurting religious sentiment, Nagpur Today, June 2015, http://www.nagpurtoday.in/whatsapp-admin-held-for-hurting-religious-sentiment/06250951;Siddharth Ranjan Das, 4 Arrested for WhatsApp Messages on Shivraj Singh Chouhan Granted Bail, NDTV, July 28 2015, http://www.ndtv.com/india-news/4-arrested-for-whatsapp-messages-on-shivraj-singh-chouhan-granted-bail-1201375; Pavan Dahat, WhatsApp admin held for post on Gandhiji, The Hindu, August 30 2015, http://www.thehindu.com/todays-paper/tp-national/whatsapp-admin-held-for-post-on-gandhiji/article7594991.ece.

232 Shreya Singhal v Union of India, Writ Petition (Criminal) No. 167 of 2012; What next: What happens to Section 66A now, The Indian Express, March 26 2015, http://indianexpress.com/article/india/india-others/what-next-what-happens-to-section-66a-now/.

233 Whatsapp admin held for hurting religious sentiment, Nagpur Today, June 2015, http://www.nagpurtoday.in/whatsapp-admin-held-for-hurting-religious-sentiment/06250951.

court sent the student to a remand home.[234] In the same month, in Hadra, Madhya Pradesh, police arrested four men for allegedly posting derogatory remarks against the Chief Minister on WhatsApp.[235] They were charged with 'promoting disharmony' and released on bail a day later.[236]

- In November 2015, the Maharashtra police ordered the arrest of a 17-year-old from another state for circulating a message on WhatsApp which they said had sparked a riot in the town of Amravati. The boy was arrested in his home in Uttar Pradesh and brought to Maharashtra, where he was charged with hurting religious sentiment under Section 295A of the IPC and denied bail because his family could not prove his age.[237]

- In December 2015, a textile shop owner in Tamil Nadu was arrested for sharing a satirical image depicting the Chief Minister in an undergarment on WhatsApp. He was charged with Section 346 of Indecent Representation of Women (Prevention) Act and Section 3 of Harassment of Women Act.[238]

- In March 2016, a journalist was arrested in Chhattisgarh for allegedly posting an obscene message about a senior police officer on a WhatsApp g oup. He was charged with publishing obscene material under Section 67 of the IT Act and Section 292 of the IPC. The journalist accused the police of abuse in custody.[239] The journalist was released on bail in June.[240]

- In May 2016, a person was arrested in Jharkhand for allegedly posting religiously inflamm - tory content in a WhatsApp group. Charges were filed under Section 295A f the IPC and Section 66D of the IT Act. A case was also registered against the group administrator.[241]

A handful of Facebook users were also charged based on posts:

- Eight charges based on Facebook content were reported in Uttar Pradesh in July 2015; news reports did not specify the ages of those charged but described all eight as youths. One individual in Sambhal was arrested under Sections 153A, 505, and 504 of the IPC for allegedly sharing an "objectionable" post about a politician on Facebook.[242] Separately, charges were

234 Class XI student nabbed for objectionable post, The Times of India, July 6 2015, http://timesofindia.indiatimes.com/city lucknow/Class-XI-student-nabbed-for-objectionable-post/articleshow/47951424.cms.

235 Vyapam Recruitment Scam pertains to massive irregularities in recruitments done by Madhya Pradesh Professional Examination Board or 'Vyapam'. See here: Milind Ghatwani, Timeline: Story of the Vyapam scam, July 8 2015, The Indian Express, http://indianexpress.com/article/explained/across-the-board-vyapams-spread/.

236 Siddharth Ranjan Das, 4 Arrested for WhatsApp Messages on Shivraj Singh Chouhan Granted Bail, NDTV, July 28 2015, http://www.ndtv.com/india-news/4-arrested-for-whatsapp-messages-on-shivraj-singh-chouhan-granted-bail-1201375.

237 Ishita Mishra, Maharashtra cops arrest UP teen for Whatsapp text that stirred riot, The Times of India, November 8 2015, http://timesofindia.indiatimes.com/city/agra/Maharashtra-cops-ar est-UP-teen-for-Whatsapp-text-that-stirred-riot/articleshow/49705130.cms.

238 Man held for 'indecent' use of Jayalalithaa's photo, The Hindu, December 8 2015, http://www.thehindu.com/news/national/tamil-nadu/man-held-for-indecent-use-of-jayalalithaas-photo/article7958708.ece.

239 Dipankar Ghose, Chhattisgarh: Journalist arrested for allegedly taking a dig at a cop on WhatsApp, The Indian Express, March 23 2016, http://indianexpress.com/article/india/india-news-india/latest-journalist-arrest-in-chhattisgarh-is-for-a-whatsapp-dig-at-a-cop/.

240 Chhattisgarh: Journalist held for WhatsApp message gets bail, June 23 2016, The Indian Express, http://indianexpress.com/article/india/india-news-india/chhattisgarh-journalist-arrest-whatsapp-message-gets-bail-prabhat-singh-2870169/.

241 Jaideep Deogharia, Jharkhand police arrest one for posting 'inflamma ory' text on whatsapp, Times of India, May 2 2016, http://timesofindia.indiatimes.com/city/ranchi/Jharkhand-police-ar est-one-for-posting-inflamma ory-text-on-whatsapp/articleshow/52079583.cms.

242 http://www.thehoot.org/freespeech/CategoryDetailsRecord/1142/34/2015/1; http://www.newindianexpress.com/nation/Youth-Arrested-for-Objectionable-Facebook-Post-Against-SP-Leader/2015/07/03/article2900364.ece.

filed against se en people in Bahraich, Uttar Pradesh for hurting religious sentiment on Facebook. At least one who posted the comment was detained; police were also investigating the other six who had liked or commented on the content. Charges were filed under Sections 153B, 295A, and 504 of the IPC, and the IT Act.[243]

- In February 2016, a Facebook user reported that he had been arrested two hours after posting about a local leader. Though the post did not name the leader, a politician from the Trinamool Congress, the ruling party in the state of West Bengal, said he planned to prosecute the man for defamation.[244] Police said the man had been arrested to maintain peace.[245]

All these cases are currently pending. Various prosecutions initiated in the previous reporting period were dropped for lack of evidence.[246]

Surveillance, Privacy, and Anonymity

There is limited opportunity for anonymity on the internet in India. Prepaid and postpaid mobile customers have their identification erified befo e connections are activated.[247] There is a legal requirement to submit identification at cybe cafes[248] and when subscribing to internet connections.

The effective implementation of privacy rights remains a significant issue. Communications su - veillance may be conducted under the Telegraph Act,[249] as well as the IT Act,[250] to protect defense, national security, sovereignty, friendly relations with foreign states, public order, and to prevent incitement to a cognizable offense. Section 69 of the IT Act appears to add another broad category, allowing surveillance for "the investigation of any offence."[251]

The home secretary at the central or state level issues interception orders based on procedural safeguards established by the Supreme Court and rules under the Telegraph Act.[252] These are reviewed by a committee of government officials f a certain rank, and carried out by intermediaries.[253] A similar framework applies to the IT Act.[254] Interception orders are not reviewed by a court and are lim-

243 http://timesofindia.indiatimes.com/city/allaha ad/7-booked-for-objectionable-post-on-FB/articleshow/47910045.cms

244 Youth held in West Bengal for Facebook post 'against TMC leader', Hindustan Times, February 7 2016, http://www.hindustantimes.com/india/youth-held-in-west-bengal-for-facebook-post-against-tmc-leader/story-RH0lXa2flgDqt1JE_AXxXN.html.

245 Indrajit Kundu, Bengal: Man arrested for 'defamatory Facebook post' against Trinamool leader, India Today, February 6 2016, http://indiatoday.intoday.in/story/man-arrested-for-posting-defamatory-remark-against-trinamool-leader-on-facebook/1/589630.html.

246 See, for example, Yahya Hallare, Bhatkal: Anti-Modi MMS - AAP member released, all charges withdrawn, May 28, 2014,http://www.daijiworld.com/news/news_disp.asp?n_id=23787; Amresh Sent to Jail on Remand, The Pioneer, May 16, 2014, http://archive.dailypioneer.com/state-editions/lucknow/amresh-sent-to-jail-on-remand.html; Supreme Court seeks UP government response on Facebook post in support of Durga Sakthi Nagpal, August 16, 2013, The Economic Times, http://articles.economictimes.indiatimes.com/2013-08-16/news/41417800_1_section-66a-facebook-post-shreya-singhal.

247 Press Release, Ministry of Communication and Information Technology, Government of India, March 13, 2013, http://pib.nic.in/newsite/erelease.aspx?relid=93584.

248 Rule 4, Information Technology (Guidelines for Cyber Cafe) Rules, 2011, http://deity.gov.in/sites/upload_files/dit/file GSR315E_10511(1).pdf.

249 Section 5(2), Indian Telegraph Act, 1885.

250 Section 69, Information Technology Act, 2000.

251 Section 69, Information Technology (Amendment) Act, 2008.

252 Rule 419A, The Indian Telegraph Rules, 1951.

253 Rule 419A, The Indian Telegraph Rules, 1951; S 69, Information Technology Act, 2000.

254 Chinmayi Arun, "Way to Watch", The Indian Express, June 26, 2013, http://indianexpress.com/article/opinion/columns/way-to-watch/.

ited to 60 days, renewable for a maximum of 180 days.[255] In emergencies, phone tapping may take place for up to 72 hours without this clearance, but records must be destroyed if the home secretary subsequently denies permission.[256] Eight separate intelligence bodies are authorized to issue surveillance orders to service providers under these circumstances.[257] Around 7,500 to 9,000 telephone interception orders are issued by the central government alone each month, according to a 2014 report citing information revealed in a right to information request.[258]

Online intermediaries are required by law to "intercept, monitor, or decrypt" or otherwise provide user information to officials [259] Where the Telegraph Act levied civil penalties for non-compliance with an interception order,[260] while also creating the possibility of loss of license, the IT Act carries a possible seven year jail term.[261] Unlawful interception is punishable by just three years' imprisonment.[262]

Some improvements to the framework have been made. On January 2, 2014, the government issued "Standard Operating Procedures (SOP) for Lawful Interception and Monitoring of Telecom Service Providers," which were viewed by journalists but not publicly available.[263] The procedures restricted interception to a service provider's "chief nodal office ," and mandated that interception orders be in writing.[264] Rules issued in 2011 under the IT Act increased protection of personal data handled by companies.[265] However, they do not apply to the government; critics say they create a burden on multinational companies, particularly in the context of the outsourcing industry.[266]

These improvements failed to address the framework's inconsistencies. In 2012, a government-appointed group of experts said the Telegraph and the IT Acts are inconsistent with regard to "permitted grounds," "type of interception," "granularity of information that can be intercepted," the degree of assistance from service providers, and the "destruction and retention" of intercepted material." These differences, it concluded, "have created an unclear regulatory regime that is not transparent, prone to misuse, and that does not provide remedy for aggrieved individuals."[267]

255 Rule 419A, The Indian Telegraph Rules, 1951; S 69, Information Technology Act, 2000.

256 Privacy International, "Chapter III: Privacy Issues," in India Telecommunications Privacy Report, October 22, 2012, https://www.privacyinternational.org/reports/india/iii-privacy-issues#footnoteref1_ni8ap74.

257 Research and Analysis Wing, the Intelligence Bureau, the Directorate of Revenue Intelligence, the Enforcement Directorate, the Narcotics Control Bureau, the Central Bureau of Investigation, the National Technical Research Organization and the state police. See, Privacy International, "Chapter iii: Privacy Issues," in India Telecommunications Privacy Report, October 22, 2012, https://www.privacyinternational.org/reports/india/iii-privacy-issues#footnoteref1_ni8ap74.

258 "India's Surveillance State", SFLC, http://sflc.in/wp-con ent/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf.

259 Section 69(4), Information Technology (Amendment) Act, 2008.

260 Sunil Abraham and Elonnai Hickok, "Government Access to Private Sector Data in India, International Data Privacy Law", 2012, Vol. 2, No. 4, p. 307, http://idpl.oxfordjournals.org/content/2/4/302.full.pdf+html

261 Information Technology Act, 2000, Section 69(4).

262 Indian Telegraph Act, 1885, Section 26.

263 Shalini Singh, "Centre issues new guidelines for phone interception", The Hindu, January 10, 2014, http://www.thehindu.com/news/national/centre-issues-new-guidelines-for-phone-interception/article5559460.ece.

264 Divij Joshi, "New Standard Operating Procedures for Lawful Interception and Monitoring", Centre for Internet and Society, March 13, 2014, http://cis-india.org/internet-governance/blog/new-standard-operating-procedures-for-lawful-interception-and-monitoring.

265 Bhairav Acharya, "Comments on the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011", Centre for Internet and Society, March 31, 2013, http://cis-india.org/internet-governance/blog/comments-on-the-it-reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information-rules-2011.

266 Kochhar & Co., "2011 Indian Privacy Law", Outsourcing.net, July 13, 2011, http://www.outsourcing-law.com/2011/07/2011-indian-privacy-law/.

267 "Report of the Group of Experts on Privacy", Planning Commission of India, 7: 19, p. 60-61, October 16, 2012, http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf.

In 2015, the government was finalizing the dra t of the Privacy Bill to be tabled in the Parliament.[268] This may be delayed pending another deliberation, however. In August 2015, a three-judge bench of the Indian Supreme Court requested the Chief Justice to formulate a larger bench to decide whether privacy is a fundamental right in India.[269]

License agreements require service providers to guarantee the designated security agency or licensor remote access to information for monitoring;[270] ensure that their equipment contains necessary software and hardware for centralized interception and monitoring; and provide the geographical location, such as the nearest Base Transceiver Station, of any subscriber at a given point in time.[271] Under a 2011 Equipment Security Agreement that did not appear on the DoT website, telecom operators were separately told to develop the capacity to pinpoint any customer's physical location within 50 meters.[272] "Customers specified by security agencies" ere prioritized for location monitoring, with "all customers, irrespective of whether they are the subject of legal intercept or not," to be monitored by June 2014.[273] The agreement remains effective, though various GSM operators lobbied for the clause to be removed from the license agreement because of compliance issues.[274] In 2014, an amendment to licensing conditions mandated government testing for all telecom equipment prior to use, effective in 2015.[275]

Cybercafe owners are required to photograph their customers, arrange computer screens in plain sight, keep copies of client IDs and their browsing histories for one year, and forward this data to the government each month.[276]

ISPs setting up cable landing stations are required to install infrastructure for surveillance and key-

268 Yatish Yadav, "Centre Giving Final Touches to Right to Privacy Bill", March 17 2015, http://www.newindianexpress.com/nation/Centre-Giving-Final-Touches-to-Right-to-Privacy-Bill/2015/03/17/article2717271.ece..

269 Amit Anand Choudhary, "Five-judge constitution bench to adjudicate on right to privacy", August 11 2015, http://timesofindia.indiatimes.com/india/Fi e-judge-constitution-bench-to-adjudicate-on-right-to-privacy/articleshow/48437244.cms; Sidharth Pandey , "Is Privacy a Fundamental Right? Constitution Bench of Supreme Court to decide", August 11 2015, http://www.ndtv.com/india-news/is-privacy-a-fundamental-right-constitution-bench-of-supreme-court-to-decide-1206100.

270 Saikat Datta, "A Fox On A Fishing Expedition," Outlook India, May 3, 2010, http://www.outlookindia.com/article.aspx?265192.

271 Guideline 8, Guidelines and General Information for Grant of License for Operating internet Services, Department of Telecommunication, Ministry of Communication and Information and Technology, Government of India, August 24, 2007.

272 Amendment to the Unified Access Se vice License Agreement for security related concerns or expansion of Telecom Services in various zones of the country, Item 9, Department of Telecom, September 7, 2011, http://www.dot.gov.in/access-services/amendments-access-service-licences; Nikhil Pahwa, "New Telecom Equipment Policy Mandates Location Based Services Accuracy Of 50Mtrs: COAI," Medianama, June 17, 2011, http://bit.ly/keKNxY.

273 "Additional Cost Implication for the Telecom Industry as Government Mandates Location Based Services to Meet its Security Requirements," Cellular Operators Association of India Press release, June 16, 2011, http://www.indiainfoline.com/article/print/news/additional-cost-implication-for-the-telecom-industry-5179349791_1.html; "Operators Implementing Location-based Services: Govt," Press Trust of India via NDTV, August 9, 2012, http://bit.ly/S4zNcT. In June 2014, outside the coverage period of this report, the DoT issued a letter to all Cellular Mobile Telephone Service Licensees, Unified Access Licensees and Unified Licensees, asking them o submit the status of implementation of location based services within seven days of receipt. Department of Telecom, Implementation of Location Based Services with Time Frame and Accuracy as Mandated by License Amendment dated 31.05.2011 to UASL – Reg, June 19, 2014, http://www.dot.gov.in/sites/default/files_DOC240614-005.pdf.

274 "GSM operators ask DoT to remove 'location based service' clause in licence", The Business Standard, January 21, 2013, http://www.business-standard.com/article/economy-policy/gsm-operators-ask-dot-to-remove-location-based-service-clause-in-licence-113012100610_1.html.

275 Amendment to Unified Licensing Guidelines, No ember 13 2014, http://www.dot.gov.in/sites/default/files/Amended%2UL%20Guidelines%2013112014.PDF; Sandeep Dixit, "Testing of Telecom Equipment in India Mandatory from next year", The Hindu, 11 August 2014, available at: http://www.thehindu.com/news/national/testing-of-telecom-equipment-in-india-mandatory-from-next-year/article6304138.ece?utm_source=RSS_Feed&utm_medium=RSS&utm_campaign=RSS_Syndication&utm_reader=feedly.

276 Rule 4, Information Technology (Guidelines for Cyber Cafe) Rules, 2011.

word scanning of all traffic assing through each gateway.[277] The ISP license bars internet providers from deploying bulk encryption; restricts the level of encryption for individuals, groups or organizations to a key length of 40 bits;[278] and mandates prior approval from the DoT or a designated officer to install encryption equipment.[279]

Since 2011, officials ha e sought to prevent international providers from encrypting user communications,[280] and required some, such as Nokia and BlackBerry, to establish local servers subject to Indian law under threat of blocking their services.[281] In 2013, BlackBerry confi med their "lawful access capability" met "the standard required by the Government of India," though business customers would not be affected.[282]

The Indian government also seeks user information from international web-based platforms. Google reported that the government made 3,081 user data requests and 4,820 requests to access accounts between January and June 2015, the highest number of requests from any single government.[283] Google made disclosures in 44 percent of the cases.[284] The government requested access to 5,115 Facebook accounts between January and June 2015 and data was produced by Facebook in 45 percent of cases.[285] The government made 141 account information requests to Twitter between June and December 2015, the highest by any government so far; Twitter said it produced data in 4 percent of cases.[286]

Besides retrieving data from intermediaries, the government's own surveillance equipment is becoming more sophisticated. The Central Monitoring System (CMS) allows government agencies to intercept any online activities, including phone calls, text messages, and VoIP communication directly using Lawful Intercept and Monitoring (LIM) systems on intermediary premises.[287] In May 2016, the Minister for Communications and IT stated that the monitoring centers in Delhi and Mumbai are now operational, and that centers across the country are being put into operation in a phased manner.[288]

In 2015, news reports said a lab under the Defence Research and Development Organisation (DRDO)

277 Guideline 42, Guidelines and General Information for Grant of License for Operating internet Services, Department of Telecommunication, Ministry of Communication and Information and Technology, Government of India, August 24, 2007.

278 Guideline 13(d)(vii), Guidelines and General Information for grant of License for Operating internet Services, Department of Telecommunication, Ministry of Communication and Information and Technology, Government of India, August 24, 2007.

279 Guidelines and General Information for grant of License for Operating internet Services, Department of Telecommunication, Ministry of Communication and Information and Technology, Government of India, August 24, 2007.

280 Joji Thomas Philip, "Can't Track Blackberry, Gmail: DoT," Economic Times, March 16, 2011, http://bit.ly/1bhkFo8; Joji Thomas Philip and Harsimran Julku, "E-services like Gmail, BlackBerry, Skype Can't be Banned for Lack of Scrutiny: Telecoms Security Panel," Economic Times, June 16, 2011, http://bit.ly/16TBotD.

281 Thomas K Thomas, "Despite India Server, IB Unable to Snoop into Nokia E-mail Service," The Hindu, July 14, 2011, http://bit.ly/1fRqjAt.

282 Anandita Singh Mankotia, "Government, BlackBerry Dispute Ends," Times of India, July 10, 2013, http://timesofindia indiatimes.com/tech/tech-news/Government-BlackBerry-dispute-ends/movie-review/20998679.cms;

283 Google Transparency Report 2015, available at: https://www.google.com/transparencyreport/userdatarequests/IN/.

284 Google Transparency Report 2015, available at: https://www.google.com/transparencyreport/userdatarequests/IN/.

285 Facebook Government Requests Report, January-June 2015, available at: https://govtrequests.facebook.com/country/India/2015-H1/#

286 Twitter Transparency Report July- December 2015, https://transparency.twitter.com/country/in.

287 Melody Patry, "India: Digital freedom under threat? Surveillance, privacy and government's access to individuals' online data", November 21, 2013, http://www.indexoncensorship.org/2013/11/india-online-report-freedom-expression-digital-freedom-3/.

288 Government setting up centralised monitoring system for lawful interception: Ravi Shankar Prasad, The Economic Times, May 4 2016, http://articles.economictimes.indiatimes.com/2016-05-04/news/72832003_1_centralised-monitoring-system-rmc-ravi-shankar-prasad.

was preparing to launch "NETRA," short for Network Traffic Analysis, a sys em to sweep online content for keywords like "bomb."[289] The timing for the release is unknown.

Spotlight on Marginalized Communities

Freedom on the Net 2016 **asked researchers from India, Indonesia, Kenya, Kyrgyzstan, Jordan, Mexico, Nigeria, and Tunisia to examine threats marginalized groups face online in their countries. Based on their expertize, each researcher highlighted one community suffering discrimination, whether as a result of their religion, gender, sexuality, or disability, that prevents them using the internet freely.**

In India, Japleen Pasricha conducted a survey of 500 social media users and interviewed ten of the respondents to highlight harassment of women on social media.[1] The study found:

- Online abuse is a serious issue in India, affecting more than half of survey respondents, yet women and other targets lack support and understanding to respond effectively.
- Thirty-six percent of respondents who had experienced harassment online took no action at all. Twenty-eight percent reported that they had intentionally reduced their online presence after suffering online abuse.
- Some respondents found it hard to think of online harassment on par with violence, even though 30 percent of those who had experienced it found it "extremely upsetting" and 15 percent reported that it lead to mental health issues like depression, stress, and insomnia.
- Though avid users of social media, respondents lose trust in popular platforms because of harassment against them or someone they know. Over half want stricter community standards for content, and the ability to escalate reports of abuse.
- Mechanisms to report abuse on social media platforms fall short. Victims are more likely to block abuse than to report it, yet blocking is ineffective against organized, sustained campaigns using multiple accounts.
- Assailants readily exploit mechanisms to report abuse, alleging their victims have violated platform guidelines to disable their accounts.
- Thirty percent of survey respondents said they were not aware of laws to protect them from online harassment.
- Only a third of respondents had reported harassment to law enforcement; among them, 38 percent characterized the response as "not at all helpful."

1 Japleen Pasricha, *"Violence" Online: Cybercrimes against Women and Minorities in India"* research paper, August 2016, on file with F eedom House.

Intimidation and Violence

While there was no systematic violence against internet users in the coverage period, some users have been periodically targeted in reprisal for online activities. In June 2015, a murder related to online content was reported in Uttar Pradesh. Joginder Singh, a freelance journalist who managed two Facebook pages was set alight during a raid on his home by local police office s shortly after he posted details of an investigative report accusing a state minister of involvement in illegal mining and land seizure online. He died of burn injuries after giving a statement about the attack, saying the office s questioned him about the posts, beat him, and poured petrol over him before setting him on fi e.[290]

289 Mackenzie Sigalos, "Has World's Biggest Democracy got a Big Brother Problem?" CNN, February 17 2015, available at: http://edition.cnn.com/2015/02/16/asia/india-internet-freedom/.

290 The Associated Press, "Indian journalist set on fi e after accusing minister over land grabs," *The Guardian,* June 10, 2015, https://www.theguardian.com/media/2015/jun/10/indian-journalist-joginder-singh-set-on-fi e; Nassim Benchaabane, "Indian Journalist Dies after Police Raid," *Global Journalist,* http://globaljournalist.org/2015/06/indian-journalist-dies-after-police-raid/.

On December 27, 2015, photographer Rafeeque Taliparamba's studio in Kerala was burnt down after he questioned certain Islamic practices in a WhatsApp group.[291]

Technical Attacks

According to one report, cybercrime affects nearly half of India's net users.[292] India had a conviction rate of just 0.7 percent for cybercrime in 2014.[293] However, most cybercriminals appear to act for economic motives, rather than to suppress online speech.

291 Shaju Phillip, Kerala: Studio set on fi e over owner's purdah remark, The Indian Express, December 28 2015, http://indianexpress.com/article/india/india-news-india/kerala-muslim-owners-studio-burned-down-after-provocative-comments/.

292 Cybercrime hit half of India's Net users, says study, http://www.thehindu.com/todays-paper/tp-national/cybercrime-hit-half-of-indias-net-users-says-study/article7898210.ece.

293 Asheeta Regidi, Internet immunity? Why does India have an abysmal 0.7% conviction rate for cyber crimes?, http://www.fi stpost.com/india/internet-immunity-why-does-india-have-an-abysmal-0-7-conviction-rate-for-cyber-crimes-2566380.html.

Freedom House

Indonesia

	2015	2016
Internet Freedom Status	Partly Free	Partly Free
Obstacles to Access (0-25)	11	11
Limits on Content (0-35)	12	14
Violations of User Rights (0-40)	19	19
TOTAL* (0-100)	42	44

* 0=most free, 100=least free

Population:	257.6 million
Internet Penetration 2015 (ITU):	22 percent
Social Media/ICT Apps Blocked:	Yes
Political/Social Content Blocked:	Yes
Bloggers/ICT Users Arrested:	Yes
Press Freedom 2016 Status:	Partly Free

Key Developments: June 2015 – May 2016

- ISPs blocked websites including Vimeo, Netflix, Imgur and eddit under authority granted to them by a 2014 regulation banning "negative" content, while the government said it would automate fil ering through a national domain name system (see **Blocking and Filtering**).
- The Ministry of Communication and Information warned over the top (OTT) providers of social media, communications, and other apps to censor negative content and caused the LINE messaging service to remove emojis supporting LGBTI rights (see **Content Removal**).
- In August 2016, a North Sumatran court sentenced Dodi Sutanto to 14 months in prison for defamation, based on a news report that appeared on his Facebook wall after a friend tagged him, about a local businessman's alleged corruption (see **Prosecutions and Detentions for Online Activities**).

Introduction

Internet freedom declined in 2016, as restrictions on "negative" content affected more websites without transparency or oversight.

The internet has challenged the dominant role of traditional media, and has gradually been accepted as a reliable source of information among Indonesians. With more than 100 million internet users, Indonesia could become the fourth largest online market by 2020, according to a 2016 study by Google and Temasek.[1] The impact of social media in the presidential election won by Joko Widodo in 2014 encouraged people to use web-based platforms for crowdsourced local election monitoring and other initiatives in 2015 and 2016. Citizens have used digital tools to respond to problems ranging from natural disasters to inequality. Campaigners in Bali and Java, among others, have successfully combined online and offline mobilization, bringing longstanding ad ocacy efforts to a wider online audience.

However, the internet's potential to facilitate change is undermined by increasing government control over online content on grounds of national security and morality. A 2014 decree issued by the Ministry of Communication and Information (MCI) allows internet service providers (ISPs) to block "negative" content at their own discretion, resulting in highly uneven and opaque censorship practices affecting entire platforms, including Vimeo, Netflix, Imgur and eddit. Government officials also pressured social media and communications app providers to monitor and restrict content, in one case causing LINE to remove stickers depicting LGBTI themes from its online store.

Abuse of the defamation clause in the Information and Electronic Transactions (ITE) law continues to represent a serious threat to internet freedom. Often resulting in pre-trial detention, charges facilitate retaliation for online expression, even in cases that never make it to a court.

Obstacles to Access

While smartphone use is increasing, the total internet penetration in Indonesia remained under 30 percent. This low access rate is mainly due to the geographic conditions of the country, which consists of 17,000 islands and a population that is concentrated in the major islands, namely Java and Sumatera.

Availability and Ease of Access

Internet penetration continued to increase over the past year, which the International Telecommunication Union (ITU) estimated at 22 percent in 2015, up from 17 percent in 2014.[2] The Indonesia Association for Internet Providers (APJII) reported 88.1 million people online, with 52 million users accessing the internet from Java, compared to about 5.9 million users from Papua and Nusa Tenggara, Papua and Maluku combined.[3] This highlights the archipelago's uneven connectivity, which is partly due to inadequate infrastructure.

Interestingly, the APJII survey recorded that women accounted for 51 percent of the total number of

1 Keusgen, Tony, "Indonesia, SE Asia's digital powerhouse," *The Jakarta Post*, September 8, 2016, http://bit.ly/2dhbgJa

2 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1cblxxY.

3 APJII, Center for Communication Studies University of Indonesia (Puskakom UI), research report (Bahasa Indonesian), http://bit.ly/1oBVCbn

people with internet access. Previously, in 2014, only 45 percent of women had access, according to the National Statistics Centre (BPS).[4] The internet is most popular among users under 25.[5]

The increase in internet penetration is especially due to the rapid expansion of mobile subscriptions. As in past years, fi ed-line subscriptions continued to decline during this reporting period.[6] Most users access the internet through mobile phones (95 percent), while only 13 percent rely on personal computers, according to the APJII.[7] In 2014, the number of mobile subscriptions surpassed the total population, reaching 129 percent penetration.[8] That number continued to increase during 2015, reaching 132 percent.[9] It's common for users to own multiple SIM cards and devices, as many shop around for better signal quality and lower connection prices.[10]

Affordable devices are available, and phones with Android operating systems start at US$30. Prepaid internet packages for smartphones range from US$0.50 a day to $2.50 a month. In urban areas, most shops and cafes provide free Wi-Fi, as do public libraries and schools.

In July 2015, activist Djali Gafur started an online petition calling on the MCI to review its regulation on telecommunication tariffs, in particular pricing for mobile internet access in Eastern Indonesia, which costs twice as much as in Java and Sumatera. Companies have said the high price is due to the relative lack of telecommunication infrastructure. Supported by 16,000 people online, the petition prompted Telkomsel to review and reduce its prices for users in Eastern Indonesia. The MCI also responded, committing to issue a ministerial regulation for allocating Universal Service Obligation Funds to subsidize internet access for users in the eastern part of the country.[11]

Although access is available, there has been little progress in improving connection speeds, which averaged 3.0 Mbps in 2015, far below some Asia Pacific countries such as Singapo e, Sri Lanka, and Malaysia, and below the global average of 5.1 Mbps.[12] In December 2015, the government launched faster 4G services, which are accessible from major telecom providers, including the three largest, Telkomsel, Indosat, and XL-Axiata, though poor network infrastructure makes service quality unreliable.

Restrictions on Connectivity

Internet infrastructure in Indonesia is decentralized, with several connections to the international internet.[13] The fi st internet exchange point, the Indonesia Internet Exchange, was created by APJII

4 For BPS statistics, see http://bit.ly/1Rhfid

5 See http://bit.ly/1QrL5Wf

6 ITU recorded slightly decrease in the number of fi ed-broadband subscription from 3,251,800 in 2013 to 3,009,185 in 2014, while fi ed-line telephone subscription is decrease from 30,722,651 to 26,224,974 respectively; accessible at ITU statistics, http://bit.ly/1oyspxq and http://bit.ly/1OroLdU and

7 See, APJII and Puskakom UI, 2015, "Profil engguna Internet Indonesia 2014," 20.

8 The number of mobile subscriptions varies according to different sources. We Are Social cited a 125 percent penetration rate http://bit.ly/1XEROBW.

9 International Telecommunication Union, "Mobile-cellular subscriptions," http://bit.ly/1cblxxY.

10 Redwing, "Indonesia's Mobile Driven Telecoms Market," http://redwing-asia.com/market-data/market-data-telecoms/.

11 Nadine Freischlad, "Indonesians pressure the country's largest telco to lower data cost," *Tech in Asia,* July 28, 2015, https://www.techinasia.com/indonesians-pressure-countrys-largest-telco-data-costs.

12 Akamai, "State of the Internet," Q3 2015, http://bit.ly/1oZfvZY.

13 Citizen Lab, "IGF 2013: An Overview of Indonesian Internet Infrastructure and Governance (Part 1 of 4)," October 25, 2013, https://citizenlab.org/2013/10/igf-2013-an-overview-of-indonesian-internet-infrastructure-and-governance/.

to allow member ISPs to interconnect domestically;[14] since 2011 the service has been extended to non-members.[15] Another independent internet exchange point, Open IXP, launched in 2005.[16]

Internet access continues to be concentrated in major cities such as Jakarta and Sumatera due to poor infrastructure in rural areas, particularly in the eastern part of the archipelago.[17] By 2012, there were 41 fibe -optic backbone cables, of which 60 percent were located in Java. Less than 2 percent reached Bali and the group of nearby Nusa Tenggara islands.[18] Since 1998, the government has issued plans for developing backbone fibe -optic infrastructure called the Palapa Ring Project, comprised of seven small rings of backbone connecting 33 provinces and 460 regencies.[19] However, as the project completely depends on private investment, it risks prioritizing connectivity based on an area's potential market value. The initiative faced difficulties due o lack of investment until 2013, but broke ground with the development of the Moluccan Ring cable system to connect Papua and other parts of Eastern Indonesia with the existing broadband network.[20] As part of the Moluccan Ring program, Telkomsel launched the Sulawesi Maluku Papua Cable System (SMPCS) in 2015, an undersea fibe -optic cable which aims to provide access to 34 million users, connecting 8 provinces and 34 regencies in the east, areas formerly served only by satellite connections with limited bandwidth.[21] Government and business interests agreed to move ahead with the Central and West Ring package in March 2016.[22]

Most base transceiver stations (BTS) which facilitate mobile 3G internet connections are built by private providers, who determine the number and location based on the market. Most BTS are owned by the biggest three telecom companies. Telkomsel reported having 103,000 BTS across the country in 2015, with plans to add 13,000 more in 2016.[23] Telkomsel was followed by XL with 52,000 BTS, and Indosat with 40,756.[24]

The MCI has prioritized the development of telecommunication infrastructure since 2010, establishing 5,956 PLIK, or subdistrict internet service providers, 709 regencies with Wi-Fi connections, and 33 184 *desa berdering* villages with internet connections.

14 Alam, Johar, "Indonesia Internet Exchange," http://www.iix.net.id/library/Iix_history.pdf.

15 See, http://inet.detik.com/read/2011/12/15/155758/1792092/328/indonesia-internet-exchange-membuka-diri.

16 Robbie Mitchell, "IDSeries: An Open exchange: history of Indonesia's IXP, APNIC, August 26, 2015, https://blog.apnic.net/2015/08/26/an-open-exchange-history-of-indonesias-ixp/

17 Global Business Guide Indonesia, "Improving Internet Access in Indonesia," 2013, http://bit.ly/1hkyBzU.

18 Ministry of Communication and Information, "2012 Indonesia ICT White Paper."

19 Ministry of Communication and Information, http://bit.ly/2eP5765

20 Ardhi Suryadhi, "Tifatul Resmikan Pembangunan Palapa Ring Indonesia Timur," detik inet, May 28, 2013, http://bit.ly/1eiA9qE. See, Kementrian Komunikasi dan Informasi, "Palapa Ring Percepat Pembangunan KTI," May 13, 2015, http://bit.ly/1laI8Pc.

21 Lintas Teknologi Indonesia, "Jokowi Resmikan Kabel Optik Bawah Laut Sulawesi-Maluku-Papua Rp 3,6 Triliun, "http://bit.ly/1mU7eoz; "The President of the Republic of Indonesia inaugurates the Sulawesi Maluku Papua Cable System (SMPCS)," press release, *Jakarta Globe,* http://jakartaglobe.beritasatu.com/press-release/president-republic-indonesia-inaugurates-sulawesi-maluku-papua-cable-system-smpcs/.

22 The central ring developed by Len Telekomunikasi Indonesia will connect Kalimantan, Sulawesi and North Molluca via a 2700 km undersea fiber optic cable. The est package developed by Mora Telematika Indonesia will connect Riau, Riau Island and Natuna via a 2000 km undersea fiber optic cable. See, " alapa Ring undersea cable projects to start this year," *The Jakarta Post*, March 8, 2016, http://bit.ly/1RAQvBR

23 Telkomsel, http://bit.ly/2e4efSY,

24 Achmad Rouzni Noor, Indosat Salip XL, Juaranya masih Telkomsel, Detikinet, June 17, 2015, http://bit.ly/2efxn0Y. The number of BTS has doubled in the last three years. See, "Data Statistik Direktorat Jenderal Sumber daya Pos dan Telekomunikasi," Semester I, 2013, http://bit.ly/2dm3UmB, 52-54.

ICT Market

Internet and mobile service is generally provided by large telecom companies. While there are about 340 ISPs in operation, ten major providers dominate the market, and three of them, Telkomsel, Indosat, and XL-Axiata, serve almost 85 percent of the mobile market.[25] Telkomsel and Indosat are 51 percent and 14 percent state-owned, respectively.[26] In the third quarter of 2015, Telkomsel reported gains of IDR 16.5 billion (US$ 1.2 million) in net revenue, retaining its position as the largest telecom company. It was also the fi st company to launch 4G-LTE services commercially.[27]

In 2014, the Internet Defender Front (FPI) and APJII filed a equest for a constitutional review of the Law on Post and Telecommunication due to the high cost it prescribes for an ISP license.[28] In March 2015, the Indonesian Constitutional Court rejected the claim and upheld the existing law.[29] However, APJII continues its campaign to revise the law, including calls for parliament to review it.[30] Commission XI of the House of Representatives, which oversees finance, p oposed an amendment as part of the 2015-2019 national legislative program in February 2015, before the Constitutional Court's judgement.[31] While it was listed in position 31 in terms of legislative priorities for 2016, deliberation had yet to take place by mid-year.

In 2013, the Attorney General's Office filed corruption ch ges against one ISP, IM2, for selling bandwidth under a public frequency licensed only to its parent company, Indosat.[32] Although this practice is common and in line with regulations, and the charge was opposed by both the MCI and the APJII, IM2 was accused of avoiding a private tax rate on the frequency, causing state losses of IDR 1.3 trillion (US$134 million). A court sentenced IM2's CEO Indar Atmanto to four years in prison, [33] increased to eight on appeal.[34] Judicial review had not overturned that judgement by mid-2016, and the case set a troubling precedent for others in the telecommunications industry. An APJII representative has estimated that about 200 ISPs in the country operate under the same business cooperation agreements.[35]

Regulatory Bodies

The Directorate General Post and Telecommunication Resources and Directorate General Post and Informatics oversee internet services under the MCI. Their mandates include regulating the allocation of frequencies for telecoms and data communications, satellite orbits, ISP licenses, and overseeing private telecom providers.

25 Redwing, "The Structure of Indonesia's ISP Industry," http://bit.ly/1oZpBtF; Indonesia Investments, "Telecommunications in Indonesia: Telkom, Indosat & XL Axiata," April 20, 2015, http://www.indonesia-investments.com/business/business-columns/telecommunications-in-indonesia-telkom-indosat-xl-axiata/item5480.

26 Citizen Lab, "IGF 2013: An Overview of Indonesian Internet Infrastructure and Governance (Part 1 of 4)," October 25, 2013, https://citizenlab.org/2013/10/igf-2013-an-overview-of-indonesian-internet-infrastructure-and-governance/.

27 See, http://bit.ly/1QyR7KZ

28 Twelve ISPs were closed down by the government in 2012 after failing to produce the fee. See, "FPI dan APJII Gugat Biaya Tinggi Usaha Telekomunikasi," *Jurnal Parlemen*, January 17, 2014, http://bit.ly/1nYlxSW.

29 Denny Mahardy, "Gugatan PNBP Ditolak MK, APJII Merasa Tak Masalah," *Liputan 6*, March 19, 2015, http://bit.ly/1Q28wXI.

30 Dewan Perwakilan Rakyat Republik Indonesia, "Program Legislasi Nasional," http://www.dpr.go.id/uu/prolegnas.

31 "Amendment to Law No. 20," February 2, 2015, http://bit.ly/1OusEFU.

32 Mariel Grazella, "IM2 Preparing Defense Ward Internet Doomsday," *The Jakarta Post*, January 15, 2013, http://bit.ly/15CrmNm.

33 Mariel Grazella, "Telco Firms Rattled by IM2 Verdict," *The Jakarta Post*, July 9, 2013, http://bit.ly/1LtXvAs.

34 "Indosat Tempuh Kasasi dan Bawa Kasus IM2 ke Arbitrase Internasional," *Kompas*, January 5, 2014, http://bit.ly/1n57Ct8.

35 Aditya Panji, "BRTI: 'Kiamat Internet' di depan mata, Kompas tekno," http://bit.ly/29MWeb0.

In 2003, a more independent regulator, the Indonesia Telecommunication Regulatory Body (BRTI), was established to oversee fair competition among telecommunications business entities, to resolve industry conflicts, and o develop standards for service quality. The appointment of the head of the MCI's Directorate General Post and Telecommunication as chair raised concerns over its independence,[36] though its composition has been balanced. In May 2015, new BRTI members for 2015-2018 were announced, including three government officials and the emaining six from civil society.[37] Despite this, the body lacks executive power, and can only make recommendations. As a result, it fails to intervene in relevant fraud or corruption cases,[38] and its effectiveness remains challenged.[39]

Limits on Content

During the period covered by this report, the Ministry of Communication and Information said it was strengthening the government's powers to block "negative" content online by requiring ISPs to route traffic through a national domain name system, though sites and platforms continued to be blocked in an arbitrary and inconsistent manner by individual service providers. The ministry also urged companies providing over-the-top (OTT) services like communication apps or media streaming services to censor content, singling out LGBTI stickers offered in the LINE messenger online store, which the company withdrew at the ministry's request. Digital activists attracted attention to social and political causes, and achieved some notable successes.

Blocking and Filtering

Internet censorship has been undergoing some procedural changes in the past two years. Overbroad restrictions on pornography and other content perceived as negative have long affected legitimate websites. The government has generally signaled which sites ISPs should block by including them in a database known as Trust+ or Trust Positive. In 2014, a decree detailing the blocking process allowed under the ITE law gave ISPs leeway to assess and block sites over and above those listed by Trust Positive. Transparency and avenues for appeal were reduced as a result, and in 2015 and 2016, several information-sharing platforms were entirely blocked by one or more ISP, affecting thousands of users based on subjective perceptions that a few had infringed the law.

At the same time, in a meeting with ISPs in March 2015, the MCI announced it was developing a national domain name system (DNS) to automate the blocking process.[40] A domain name system translates a web address or URL into an IP address pointing to a server which returns the requested content. If all Indonesian ISPs route traffic th ough a national DNS, instead of using the standard international DNS, then control of website blocking could pass from the ISPs to the national DNS. If the national DNS blocked the existing database of sites in Trust Positive, the ISPs would automatically reflect the same censo ship. In May 2015, news reports citing ministry officials said that four ISPs

36 In November 2005, the MCI issued Ministerial Regulation no. 25/2005 justifying the appointment of a directorate general representing the government to chair the body. See, Peraturan Menteri Komunikasi Dan Informatika, No. 25, November 2005, http://bit.ly/1OTK79s; Badan Regulasi Telekomunikasi Indonesia, "Overview Tentang BRTI," April 5, 2010, http://bit.ly/1cEejla and Badan Regulasi Telekomunikasi Indonesia, "Fungsi dan Wewenang," March 29, 2010, http://bit.ly/1hdI1ON.

37 Reska K. Nistanto, "Ini Dia Nama-nama Anggota BRIT 2015-2018," *Kompas*, May 20, 2015, http://bit.ly/1OipRy0.

38 Examples include a high profile case f SMS fraud involving the PT Colibri Network CEO and the vice director of Telkomsel Antara. See, "Kasus Pencurian Pulsa Mandeg, Ini Penyebabnya," *GresNews*, March 12, 2014, http://bit.ly/1GsTmW4.

39 Amal Nur Ngazis and Agus Tri Haryanto, "Disorot, Regulator Telekomunikasi Tak Independen," July 28, 2015, http://bit.ly/1NhjKKe.

40 Dyta, "Kominfo Finalisasi DNS Nasional," accessible at http://bit.ly/29XjqTM and http://bit.ly/2a9BCuu.

were piloting a national DNS, affecting 75 percent of internet traffic in Indonesia, though without providing further detail.[41] However, blocking continued to be implemented unevenly by different providers through mid-2016.

The governmnt's authority to block content is granted by the Information and Electronic Transactions Law (ITE Law), provided that limitations are in the public interest and intended to maintain public order.[42] In general, blocking in Indonesia has targeted websites hosting pornographic content, gambling, and religious radicalism as part of the government's counter-terrorism policy. In 2015, the MCI reported 766,394 sites blocked, mostly due to pornographic content (753,497), gambling (1164), fraud and illegal trading (452) and content promoting radicalism. In the same year, the MCI also unblocked 248 websites.[43]

In practice, blocking tends to be arbitrary, as the wording lacks clarity in its articulation of what is considered as "forms of disturbance," "abuse of electronic information," "public interest," and "public order." Another statute provides a legal framework to block content considered pornographic, which can affect websites serving the LGBTI community among other categories of information.[44]

In 2014, the MCI issued a decree titled Permenkominfo 19/2014, a technical regulation for implementing the ITE law. However, instead of clarifying the scope of prohibited content, the regulation added confusion by introducing the new technical term "negative content," defined as con ent involving pornography and other activities considered illegal under existing laws. No further limits are placed on this broad category. The regulation also detailed procedures for the public to report negative content online or via email.

The regulation specified the existing se vice Trust Positive as the government's "blocking service provider," or database of websites with negative content for Indonesian ISPs to block. Operational since 2010, Trust Positive is a fil ering application managed directly by the ministerial office, with a dat - base of continuously updated websites.[45] Members of the public or website owners can file co - plaints to remove the website's URL address from the Trust Positive database of banned sites, and the complaint must be resolved in 24 hours. However, while all ISPs refer to Trust Positive, each can also employ different software for blocking and create independent databases. As a result, content restrictions are inconsistent, creating uncertainty for users seeking redress when content is wrongfully blocked.

The 2014 decree compounded that uncertainty by providing a legal basis for any third party to independently block websites.[46] According to Article 7 of the decree, "[members of] society can participate in providing blocking facilities" which contain "at least" sites listed in the Trust Positive database.[47] This has increased the practice of arbitrary blocking, since it does not prevent ISPs from blocking more sites without oversight.

Several information-sharing platforms were blocked by ISPs taking their own initiative during the

41 Reska, N, Nistanto, "DNS Nasional untuk Blokir Pornografi Sedang Diuji Co a," *Kompas,* http://bit.ly/1LkcDw7

42 Law No. 11/2008, Article 40.

43 See http://bit.ly/1PViOYA

44 Civil society and cultural groups challenged the law before the Constitutional Court in 2009 for its narrow and obscure definition f pornography and pornographic content, which includes LGBTI content and folk traditions which expose the female form, such as the Jaipongan folk dance from West Java and Papuan traditional clothes; the Court upheld the law.

45 Trust Positif, website, http://trustpositif.kominfo.go.id/.

46 Article 7(1), "Permenkominfo 19/2014," http://bit.ly/UZlkY5.

47 Article 7(1), "Permenkominfo 19/2014," http://bit.ly/UZlkY5.

coverage period of this report. At least one service provider had blocked Reddit and Imgur in January 2016, even though neither site is in the Trust Positive database.[48] On January 26, 2016, Netflix users reported through social media that the website was inaccessible. One day later, Telkomsel officially announced it was blocking Netflix on ounds that the company had failed to comply with national legislation on multimedia content accessible to Indonesian audiences. In its press statement, Telkom said the measure would protect its users from violent and pornographic scenes prohibited by law.[49] The MCI supported Telkom's action, but for different reasons, saying that Netflix had not co - plied with a law requiring foreign companies operating in Indonesia to establish a local entity (see Surveillance, Privacy and Anonymity). As of mid-2016, the MCI has not yet issued a clear decision on Netflix. While it was not fficially bloc ed, the MCI has not interfered to prevent private companies from blocking it.

Shortly after the controversial Netflix case, MCI announced that it had issued an instruction o introduce Tumblr into the Trust Positive database, on the grounds that the social networking platform was hosting pornographic content. Internet users protested the decision (see Digital Activism). Under mounting public pressure, MCI released a clarification sta ement (17/2), saying that the instruction had yet to be officially issued, pending consultation with umblr.[50] In mid-2016, the site was still accessible.

In 2014, a group of NGOs submitted a request to the Supreme Court to review the constitutionality of the ministerial regulation, but the court refused to consider it while a separate case was being decided. The NGOs characterized digital content as a nontangible object, and argued that disrupting access to it amounted to confiscation under the criminal p ocedural code. The article on confiscation was facing a concurrent challenge before the constitutional court.[51] While that issue was resolved in April 2015, a constitutional review of the blocking rules had yet to be undertaken in mid-2016.

Responding to public criticism regarding the lack of accountability of the blocking mechanism, the MCI established four panels representing various digital stakeholders, including NGOs and private entities.[52] The four panels cover pornography, child abuse, and internet security; terrorism and ethnic, race and religion (SARA); illegal investment, fraud, gambling and food and medicines; and intellectual property rights. The panels are ad hoc in nature, and function to provide recommendations regarding requests to block or unblock content, either from individuals or groups within society, or from government agencies.[53] Although they do not have executive power, their advice has infl - enced MCI decisions. For example, in January 2016, MCI blocked nine websites for promoting radicalism and religious violence based on a recommendation put forward by the panel on terrorism.[54]

The establishment of the panels got mixed reactions. Some NGOs saw them as an opportunity to

48 In a test conducted on January 28, 2016, found Telkomsel blocked both sites; they were accessible through First Media. Both had been patchily accessible since 2014, when Vimeo was also reported blocked.

49 Law No. 33/2009, http://bit.ly/1VrnObk, requires movies screened for Indonesian audiences to pass though a censorship procedure.

50 KOMINFO, "Klarifikasi Kemkominfo mengenai Rencana Pemblokiran Situs Tumblr," February 17, 2016, http://bit.ly/1OtGwZZ

51 For the decision, see http://bit.ly/29OrPon.

52 See on the establishment of the panel http://bit.ly/1Oj1ElH; on panel decision which lead to blocking: http://bit.ly/2129igX.

53 Under Article 5 of the decree, members of society and government agencies can submit blocking requests to the MCI Directorate General.

54 Koran Tempo, "Kominfo Blokir lagi 9 Situs Radikal," ini daftarnya, January 28, 2016, http://bit.ly/1V6oQvM.

improve the process. Others, such as the ICJR, believe the existence of such panels lends legitimacy to a fundamentally unconstitutional blocking procedure.[55]

Though it makes up the smallest percentage of content affected by blocking, religious websites were the focus of public attention in 2015 and 2016. In March 2015, MCI blocked 22 websites reported to promote radicalism after a request was submitted by the National Body on Counterterrorism (BNPT).[56] The blocking prompted widespread debate; ultimately under public pressure, MCI unblocked 12 of the listed sites.[57] Shortly after a terrorist attack in the shopping and entertainment district on Thamrin street, Jakarta, on January 14, 2016, the MCI blocked 34 more websites on the grounds that they were promoting radical content supporting the attack. Some Twitter accounts and YouTube videos sending similar messages were also reported to have been blocked.[58]

Content Removal

Administrative requests to delete or take down content were less common in the past than blocking. However, as the MCI moved to strengthen control over companies providing "over-the-top" (OTT) services, administrative requests have been used to require companies to self-censor. OTT includes social media and communication apps, as well as other providers of apps that rely on an internet connection.

In February 2016, stickers displayed in the LINE messaging service app store spurred a debate on LGBTI rights in Indonesia.[59] The stickers, elaborate emojis depicting LGBTI themes, were criticized for overtly promoting same-sex relationships in Indonesia. After public complaints, the MCI brought the case to a multistakeholder advisory panel to determine whether the stickers should be subjected to blocking and fil ering.[60] Ultimately, LINE fil ered the stickers at the MCI's request.[61]

Also in February, the MCI invited other OTT companies such as Facebook, Blackberry, WhatsApp, and Twitter for a consultation, calling for them to be more proactive in censoring negative content on their services.[62] Representatives of the companies agreed to do so in accordance with local laws, according to news reports.[63]

In March 2016, the MCI issued a circular letter warning OTT providers to fil er content which does not comply with Indonesian laws and regulations.[64] The warning targeted providers of games, videos, music, animation, images, and other forms of content available via streaming and download, and

55 ICJR, "Unlawful Blocking Action on LGBT website should be stopped," August 3, 2016, http://bit.ly/1OyxNwK.

56 BNPT letter no 149/K.BNPT/3/2015 requested blocking of 22 websites. See Dewi Widyaningrum, 'Kominfo blokir 22 Situs yang dianggap radikal," http://bit.ly/1KGoaKK.

57 Widiartanto, Y, 'Kominfo Kemenkominfo Buka Blokir 12 dari 19 Situs "Radikal", *Kompas*, http://bit.ly/1KGpkpy.

58 In addition, MCI claimed to have blocked 78 videos uploaded to YouTube for promoting support for ISIS since 2015, though blocking URLs is ineffective on encrypted connections using https. Officials did not clari y if the content was created or uploaded in Indonesia. See, *Majalah ICT* 41, January 2016, 20-22, http://bit.ly/21bRfF1.

59 Associated Press, "Indonesia bans gay emoji and stickers from messaging apps," *The Guardian*, http://bit.ly/240h1uO.

60 See http://bit.ly/1RPDzcQ

61 See http://bit.ly/210nqaq also http://bbc.in/1R9dJhP

62 see http://bit.ly/1oA9geG

63 "Twitter, Line, dan Blackberry siap lakukan sensor mandiri," *Tempo*, February 18, 2016, http://bit.ly/1R5cRb1.

64 MCI Circular letter no 3/2016, Point 5.5, http://bit.ly/2dhCS0x.

said providers must establish domestic business entities and allow legal interception for law enforcement purposes.[65] Officials said fu ther, binding regulations would follow.[66]

Media, Diversity, and Content Manipulation

Media freedom has been improving since the beginning of the political transition in 1998, and since then, interference from state agencies has significantly declined. Ho ever, while traditional printed media is perceived to have better protection under the press law, online media face substantial challenges with the enforcement of ITE Law, particularly the threat of criminal sanctions in reprisal for information posted online.

One of the most popular online media outlets in Atjeh, *Atjeh Post*, announced its voluntary closure in early 2015. Atjeh police had been investigating a defamation charge filed by the ffice f the Atjeh Governor against the editor, prompting speculation that the closure was related. An attempt by the Press Council to bring the case into its dispute mechanism failed, in part due to the complexity of the case, and the perception that the website was operating with a political agenda. Nevertheless, the Council denounced the use of criminal sanctions against a media outlet.[67] In August 2016, the case was settled, and charges against the editor were dropped after he issued a public apology in local media.[68]

There is no precise account of the numbers of journalists facing criminal sanctions under the ITE law, but some incidents suggest an increase in defamation charges targeting online journalists, driven by the rapidly expanding online news market. At the local level many online news outlets have become the extension of certain political parties, hampering their credibility, and increasing the possibility of retaliatory criminal charges under the ITE Law, which does not affect their print and broadcast counterparts. The quality of these outlets varies widely, and less than 10 percent are registered with the Press Council, which is less likely to intervene to defend them in criminal cases as a result.[69] Of the 1,586 media outlets recorded in the Press Council national media database in 2015, only 68 operated online,[70] in part because many online operations fall short of official equirements for establishing a media company, such as a legal entity like a limited liability company, a cooperative or a foundation.

Indonesia has enjoyed a thriving blogosphere since around 1999. The rapid increase of a tech-savvy urban middle class, fervent users of social media and communication apps, has fueled a diversity of applications and platforms. YouTube, Facebook, Twitter and international blog-hosting services are freely available. Local blog and website-hosting services are either free or inexpensive. Tools to circumvent censorship are subject to some blocking, though in practice some remain accessible.[71] In

65 KK Advocates, "Guidance For Ott Service Providers In Indonesia Is Finally Issued," April 11, 2016, http://www.kk-advocates.com/site/guidance-for-ott-service-providers-in-indonesia-is-finally-issued .

66 Anton Hermansyah, "Govt calls on foreign OTT content providers to obey law," *The Jakarta Post,* April 1, 2016, http://www.thejakartapost.com/news/2016/04/01/govt-calls-on-foreign-ott-content-providers-to-obey-law.html;

67 Interview with press council member Nezar Patria, February 26, 2016.

68 Information based on a mediation agreement on August 2, 2016. Nurlis published an apology in Atjeh media outlet Serambi Indonesia on August 3. For coverage of the apology, see *Kanalaceh*, http://bit.ly/2dd8YIF; Atjeh Jaringan National Network (AJNN), http://bit.ly/2dHC1Fe.

69 Interview with press council member Nezar Patria, February 26, 2016.

70 Dewan Pers, 2015, "Data Pers National 2015," http://bit.ly/2adDIWU.

71 Ronald J. Deibert et al., "Indonesia," in *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*, (Massachusetts Institute of Technology, 2012).

one 2013 test, they were "heavily fil ered on Telkmonet's IGF network while generally available on the other two networks."[72]

For sensitive issues such as corruption, social media have proven to be an important alternative source of information. However, the rapid increase in social media use and influence in public issues has brought new challenges regarding the manipulation of content. As anonymous and pseudonymous accounts are not prohibited on microblogging platforms such as Twitter, these accounts often circulate controversial information, rumors, and even blackmail threats against prominent figu es, particularly during the presidential election in 2014.

Digital Activism

With urban middle class expanding, digital activism has become a popular form of organizing support for social and political change. In 2015, the crowdsourcing initiative *kawalpilkada* helped to promote fair regional elections held nationwide on December 9, tallying votes and voter registration data in 57 regencies.[73]

Digital activism has proven to be an effective means of supporting offline mobilization. ecent examples include the #savekpk movement, which combined online and offline cam aigning in defense of the Corruption Eradication Commission, known by its acronym KPK. Police had launched criminal investigations against three KPK chairmen for offences including orchestrating witness statements, apparently in reprisal for a corruption investigation that named high level office s in the National Police. An online petition called for the police chief's dismissal in July 2015;[74] in September he was transferred to lead an anti-drug agency.[75]

Conservationists increasingly take advantage of online tools. Digital activists supported a local community in central Java protesting against a PT Semen Indonesia cement plant in the groundwater basin Watuputih area, culminating in a protest by nine women who cemented their feet outside the presidential palace in Jakarta in April 2016. President Joko Widodo subsequently commissioned a study of the plant's environmental impact. Advocacy around the issue has been ongoing in various forms since 2010, but intensified in the ast two years when the hashtag #savekendeng helped bring the case to national attention.[76]

The *Bali Tolak Reklamasi* or ForBALI campaign followed a similar trajectory.[77] The longstanding advocacy movement by civil society organizations in Bali has opposed a huge development project

72 Citizen Lab, "IGF 2013: Analyzing Content Controls in Indonesia (Part 2 of 4)," October 25, 2013, https://citizenlab.org/2013/10/igf-2013-analyzing-content-controls-indonesia/.

73 Website is accessible at http://bit.ly/21lvfrl. Collaboration between Code4Nation, Turun Tangan, Perludem, and Data Science Indonesia (DSI), and Indonesia Corruption Watch (ICW). There are about 300 volunteers registered through their online registration system, and about 150 volunteers from the 'turun tangan' a crowd-source initiative sending people See http://bit.ly/1LF7z7U

74 "Indonesia's Police Overstep in Anti-KPK Campaign," *Asia Sentinel,* July 17, 2015, http://www.asiasentinel.com/politics/indonesia-police-overstep-anti-kpk-campaign/

75 "Budi Waseso Appointed as BNN Chief," *Tempo,* September 8, 2015, http://en.tempo.co/read/news/2015/09/08/055698733/Budi-Waseso-Appointed-as-BNN-Chief.

76 "Cemented female protestors continue to fight against cement plants" *The Jakarta Post*, April 14, 2016, http://bit.ly/1W4aUn7

77 Bali tolak Reklamasi, see http://bit.ly/2djnEWn

planned for land reclaimed from Benoa Bay for more than four years.[78] Online support has grown since around 2014, attracting national and international attention and empowering further community mobilization against the development, which has caused the bay's protected status as a conservation area to be revoked.[79]

Activists have also used online petitions to promote internet freedom, with several successes during the coverage period of this report. A July 2015 online petition resulted in more affordable mobile data service in Eastern Indonesia (see Availability and Ease of Access). In October, internet user Adlun Fikri was released from police custody after a social media campaign with the hashtag #saveadlunfiqri, and an online petition with nearly 2,000 signatu es. He was arrested for sharing an online video alleging misconduct by traffic police (see P osecutions and Detentions for Online Activity). And in February 2016, netizens mobilized to fight the MCI s decision to block Tumblr under the hashtags #BloggerMelawan, #TolakBlokirTumblr, #savetumblr, and an online petition signed by more than 13,000 people;[80] the ministry ultimately backtracked (see Blocking and Filtering).

In August 2015, hackathon@istana, which included the government and the IT industry, was organized to address pressing social issues through innovation. The initiative launched a number of software solutions and applications in the public interest, such as tools to monitor the allocation of state funds. Another hackathon@istana was organized in December, extending outreach to the Indonesian diaspora in Malaysia, Australia, Japan, and Singapore.[81]

Violations of User Rights

Prosecutions under the ITE Law, often to intimidate and to silence critics, continued with high profile cases drawing widespread public outrage. People frequently use the law for their own agenda, misguidedly mixing public and private digital space. A promised revision to the ITE Law had yet to materialize in mid-2016. Without proper training for Indonesian law enforcement and the judiciary, prosecutions are likely to continue to serve as retaliation for online speech.

Legal Environment

Freedom of expression was initially protected through the stipulation of the Law on Human Rights, shortly after the 1998 reformation, which was strengthened through the second amendment of the constitution in 2000. The third amendment guarantees freedom of opinion.[82] The constitution also includes the right to privacy and the right to obtain information and communicate freely.[83] These

78 Jewel Topsfield and Amilia osa, "$3 billion islands project for Bali's Benoa Bay has locals up in arms," *Sydney Morning Herald,* February 29, 2016, http://www.smh.com.au/world/3-billion-islands-project-for-balis-benoa-bay-has-locals-up-in-arms-20160228-gn5m1p.html

79 Johnny Langenheim, "Battle for Bali: campaigners fight ack against unchecked development," *The Guardian,* October 22, 2014, https://www.theguardian.com/environment/the-coral-triangle/2014/oct/22/battle-for-bali-campaigners-figh -back-against-unchecked-development

80 https://www.change.org/p/menkominfo-rudiantara-id-kita-tolak-pemblokiran-tumblr

81 On hackathon@istana, the history and its current development, see, Merdeka dengan Kode (MDK), accessible at http://bit.ly/1hNatLH

82 Constitution of 1945, Article 28E(3).

83 Constitution of 1945, Articles 28F and 28G(1).

rights are further protected by various laws and regulations.[84] Indonesia also ratified the In ernational Covenant on Civil and Political Rights (ICCPR) in 2005.[85]

However, the wording of the amended constitution also introduced limitations by which state can limit rights based on political, security, morality, and religious considerations.[86] This provides broad space for interpretation by policymakers.[87]

Other laws passed since then have infringed on user rights, despite legal experts' opinions that they conflict with the constitution [88] The anti-pornography law introduced in 2008 contains a definition f pornography which can be loosely interpreted to ban art and cultural expression perceived as explicit.[89] A 2011 State Intelligence Law introduced penalties of up to ten years' imprisonment and fines f over US$ 10,000 for revealing or disseminating "state secrets," a term which is vaguely defined in the legislation.[90] Some civil society groups challenged this law in the Constitutional Court, which rejected their petition in 2012.[91] This framework provides authorities with a range of powers to penalize internet users, even though not all are regularly implemented.

Provisions of the 2008 ITE law have been used repeatedly to prosecute Indonesians for online expression. The law's penalties for criminal defamation, hate speech, and inciting violence online are harsh compared to those established by the penal code for similar offline ffenses. Sentences allowed under Article 45 of the ITE law can extend up to six years in prison; the maximum under the penal code is four years, and then only in specific ci cumstances—most sentences are less than a year and a half.[92] Financial penalties show an even more surprising discrepancy. While the ITE law allows for fines f up to IDR one billion (US$80,000), the equivalent amounts in the penal code have apparently not been adjusted for inflation. A ticle 310, for example, allows for paltry fines f IDR 4,500 (US$0.37) for both written and spoken libel.[93]

In 2016, an amendment to the ITE Law, supposedly to curb excessive prosecution of online speech, was under discussion in the House of Representatives. Three amendments would reduce the maxi-

84 Among others, "Law No. 39 of 1999 on Human Rights," "Law No. 14 of 2008 on Freedom of Information," and "Law No. 40 of 1999 on the Press."

85 The ICCPR was ratified th ough Law No. 12/2005. However, to date the government has yet to review and reform laws to comply with the covenant's human rights standards.

86 Art 28 (J) of 1945 Constitution, as amended in 2000, "In exercising his/her right and freedom, every person must submit to the restrictions stipulated in laws and regulations with the sole purpose to guarantee the recognition of and the respect for other persons' rights and freedom and to fulfill fair demand in acco dance with the considerations of morality, religious values, security, and public order in a democratic society" retrieved on 2,February, 2016 from http://bit.ly/2dmpFAa

87 The interpretation has initially established by the constitutional court in 2009, which generally affi med that all set of human rights are subjected to limitation as far as the limitation is provided by the law, in in particular to prevent any form of power abuse by power holders. see http://bit.ly/2cKuKPU, However, as no limitation is set for interpreting public morals and religious values. A number of decision issued by the Court such as in the review of Law on Intelligent, see http://bit.ly/2d5vOyO and pornography law, see http://bit.ly/2cJLgVf did not further elaborate unexhausted list and therefore left for interpretation.

88 Wahyudi Djafar et al., "*Elsam, Asesmen Terhadap Kebijakan Hak Asasi Manusia dalam Produk Legislasi dan Pelaksanaan Fungsi Pengawasan DPR RI*" [Assessment of the Human Rights Policy in Legislation and the Implementation of Parliament Monitoring], Institute for Policy Research and Advocacy, 2008.

89 An art installation in Yogyakarta was shut down for allegedly pornographic content. See, "Dianggap porno, patung akar setengah manusia dibongkar," February 10, 2014, http://bit.ly/1JSuzei; and, "Indonesian Parliament passes controversial intelligence bill," *EngageMedia*, October 25, 2011, http://bit.ly/1VEN6Bt.

90 "Indonesian Parliament Passes Controversial Intelligence Bill," *Engage Media*, October 25, 2011, http://www.engagemedia.org/Members/emnews/news/indoneisan-parliament-passes-controversial-intelligence-bill.

91 The decision is available at, Nomor 7/PUU-X/2012, Demi Keadilan Berdasarkan Ketuhanan Yang Maha Esa Mahkamah Konstitusi Republik Indonesia, http://bit.ly/1L6iB2t.

92 Human Rights Watch, *Turning Critics Into Criminals,* May 4, 2010, http://www.hrw.org/node/90020/section/6.

93 "*Kitab Undang-Undang Hukum Pidana"* [Criminal Law], available at *Universitas Sam Ratulangi*, http://bit.ly/1KZOGuY.

mum prison terms from six years to four years; adjust the wording of the law in line with the criminal code; and require a complaint to be filed befo e police can investigate violations. In its current form, the law allows police to initiate investigations independent of any report from a victim.[94] Revisions to the amendment, initially scheduled for completion in July, were ongoing in late 2016.[95]

Prosecutions and Detentions for Online Activities

Safenet, the regional freedom of expression network, recorded nine new charges under the ITE Law involving online expression in January and February 2016, and a total of 144 ongoing cases.[96] The Jakarta-based Institute for Policy Research and Advocacy (ELSAM) recorded 50 criminal cases in 2015 alone.[97] As most cases are tried at the district court level, it is believed that the numbers could be higher.

In many cases, the accusation of online defamation was followed by pre-trial detention, which can extend up to 110 days, according to the criminal procedural code,. Although this detention should only be implemented in in cases where there is strong potential for the suspect to eliminate evidence or flee the jurisdiction, many suspects accused f defamation online were detained soon after the report was lodged with police, meaning the charges functioned as a retaliatory measure, whether or not they had any merit.

One case from North Maluku province exemplified this t end. On September 26, 2015, Adlun Fikri posted a video online that he said documented misconduct by traffic police. The video was wid - ly viewed, and on September 28, police arrested him for defamation under the ITE law.[98] Netizens supported him on social media with the hashtag #saveadlunfiqri, and an online petition with nearly 2,000 signatures.[99] He was released after six days, a result which observers said was the result of public attention paid to the case.

In one particularly troubling case from 2016, the defamation clause was extended to apply to Facebook users whose privacy settings allow content tagged by third parties under their name to appear on their timeline. In August, a court in Medan, the capital of North Sumatra province, sentenced Dodi Sutanto to 14 months in prison and fine f IDR 5 million (US$380) after a friend tagged a news report with his name, essentially disseminating it to Dodi's connections.[100] The report detailed corruption allegations against Anif Shah, a local businessman, who filed the defamation cha ge on grounds that people could access the report from Dodi's Facebook page. Local news reports said that other who shared or were tagged in the post were named as suspects and that their cases were ongoing. The prosecutor in Dodi's case had called for a sentence of two years in prison.[101]

As criminal charges under the ITE Law have steadily increased, the geographical spread of individuals

94 See, Achmad Rouzni Noor, II, Pembahasan Revisi RUU ITE terus di geber, 20/4/2016, detikinet, detik.com, accessible at http://bit.ly/1U1gjtp

95 http://www.thejakartapost.com/news/2016/08/03/house-sets-different-target-for-ite-law-revision.html

96 see, Safenet, Daftar kasus Netizen Indonesia yang terjerat UU ITE, accessible at http://bit.ly/2avQWxW

97 Pusat informasi dan dokumentasi ELSAM, Data kriminalisasi UU ITE 2008 – 2016, no online version is available

98 For chronology of the case, see, Fajar Pratama, *Kronologi Drama Adlun Videokan Polantas Terima Uang Hingga Dipidana*, Detik.com, accessible at http://bit.ly/29UQtW0

99 The online petition was made by Munadi Kilkoda from Ternate, on 2 October 2015, see http://chn.ge/2a1FCvc

100 see News Desk, *Medan man gets 14 months' imprisonment for Facebook tag*, Jakarta Post, accessible at http://bit.ly/2dGQC4w

101 as contained in the court proceeding; prosecution note submitted and was delivered before the trial by the prosecutor office on 2 th of July 2016, p33

exploiting the article for repercussion against other individuals is alarming. The number of cases reported corelates with the rate of internet penetration in the region—in other words, the more internet users there are, the more criminal cases filed against them.

While defamation charges have long been used by public officials o punish criticism, since 2014 more cases have involved personal defamatory statements. The case of Ervani E, a Yogyakarta housewife, attracted attention from netizens across the country in 2014; she was ultimately acquited of charges filed in esponse to a complaint she posted about her husband's former workplace on Facebook.[102] The scope of the defamatory statements subject to penalty expanded in 2015 so that members of any particular community or group can exploit the law to retaliate against any expression on the group's behalf. In March, Florence Sihombing was sentenced to two months in prison for offending the city of Yogyakarta.[103]

The clause is also periodically used to prosecute alleged religious defamation. In March 2015, Nando Irwansyah Ma'ali, an internet user in Bali, was reported to the police for religious defamation online by a local organization, Cakrawayu and Pusat Koordinasi Hindu Indonesia (Puskor Hindunesia).[104] The case was triggered by a Facebook status complaining about the disruption of a few services due to the observance of the Hindu day of silence, or Nyepi.[105]

In October 2015, the Indonesia's national police chief issued a circular letter warning citizens not to commit hate speech online or offline, including defamation and exp essions considered to incite hatred against religion or belief.[106] In mid-2015, the national police reported monitoring and investigating 180,000 social media account holders for posting alleged hate speech.[107]

Surveillance, Privacy, and Anonymity

Anonymity and pseudonymous activity in cyberspace are not formally prohibited by law. However, they engendered huge public debate in 2015, particularly after the national police cybercrime units prosecuted some social media account holders for using pseudonyms to conduct blackmail.[108]

Mobile phone users are technically required to register their numbers with the government by text message when they buy a phone since the MCI introduced the requirement in 2005. In the past, this obligation was widely ignored, but in 2014, under the pretext of combatting criminal activity orches-

102 Ervani, a housewive in Bantul, Yogaykarta was reported to the police for her facebook status by Emy Handayani, who accused her for public humiliation online. Ervani wrote on her disappointment of her husband, Alfa Janto 's dismissal from Jollie Jewellery, a company where Emy works as Alfa's supervisor and was belief that Evi's childish character was behind the dismissal. Because of her status Emmy was sent for months at the pre-trial detention. The detention was criticised as an exaggerated action by the police and was suspected as a fishy case.

103 Terakhir Kali, "Menghina Melalui Media Sosial, Mahasiswi UGM Divonis 2 Bulan Penjara," *Voice of America*, March 31, 2015, http://bit.ly/1jNWyqp.

104 a complaint made by one of local organisation to the police against Nando, a teenager complaining the disruption of electricity service due to Nyepi. Based on this, the Provincial Police (Polda) launched criminal investigation against him under the ITE law on the allegation of religious defamation. However, no update is available as to whether the case was finally send o the court and the person is criminally charged under the ITE Law, see http://bit.ly/29QOcyJ also http://bit.ly/29WTA0N

105 Gede Nadi Jaya, Polda Bali Usut kasus Nando hujat perayaan Nyepi di Facebook, merdeka.com, accessible at http://bit.ly/29QOcyJ also http://bit.ly/29V5hbp

106 Detail Circular letter accessible at http://bit.ly/1TmQzak

107 See, Luqman Rimadi, Kapolri: 180 Ribu Akun Medsos Terdeteksi Sebarkan Hate Speech, Liputan enam, 4/11/2015, accessible at http://bit.ly/24YFq3w

108 See, Kompas, 22/4/2015, 'Edi Administrator Akun @triomacan2000 Divonis 1,5 Tahun Penjara', accessible at http://bit.ly/20XZEGS

trated using mobile phones, the ministry increased pressure on providers to register their customers.[109] In September 2015, BRTI issued a circular letter to telecommunication providers outlining new procedures for registering pay-as-you-go as well as post-paid customers. [110]

A government regulaton on telecommunications operations issued in 2000 requires telecommunications providers to retain records of customer usage for at least three months.[111] Some telecommunications companies are known to have complied with law enforcement agencies' requests for data. In 2011, amid concerns that Blackberry's encrypted communication network would hinder antiterrorism and anticorruption efforts, the company reportedly cooperated with the authorities in isolated incidents, and agreed to establish a local server, though in Singapore, not in Indonesia.[112] The government introduced a regulation in 2012 requiring electronic system providers offering "public services" to build local data centers, and a draft regulation in 2014 laid out technical requirements for any entity offering "information technology-based services" to comply.[113] In March 2016, an MCI circular letter instructed providers of over-the-top (OTT) services to establish domestic business entities and allow legal interception for law enforcement purposes (see Content Removal).[114]

Article 40 of the Law No. 46/1999 on Post and Telecommunications prohibits the interception of information transmitted through any form of telecommunications channel. [115] Yet there are at least 10 laws, including the ITE law, and seven executive regulations, which allow certain government or law enforcement agencies to conduct surveillance, including electronically.[116] The agencies include the Indonesia Corruption Commission, the National Narcotic Board, National Intelligence Service, among others. However, the laws do not clearly explain the scope of interception, despite the fact that the Constitutional Court issued a decision in 2010 requiring that detailed interception procedures be regulated by law.[117] In addition, the legal framework lacks judicial or parliamentary oversight, and does not provide a remedy for possible abuse.

In October 2015, the University of Toronto-based Citzien Lab reported Finfisher spywa e had been

109 Lihat http://www.postel.go.id/berita-penertiban-registrasi-pelanggan-26-2174 juga http://kominfo.go.id/index.php/content/detail/4014/Kominfo+Minta+Operator+Telepon+lakukan+Penertiban+Register+Pelanggan/0/berita_satker#.VVB5gKblfl

110 for the circular letter from BRTI to provider on the obligation to register pre-paid simcard users see http://bit.ly/1TJ48NJ also http://bit.ly/1TriMNk

111 http://www.iclg.co.uk/practice-areas/telecoms-media-and-internet-laws/telecoms-media-and-internet-laws-and-regulations-2016/indonesia

112 Arientha Primanita and Faisal Maliki Baskoro, "Pressure on BlackBerry Maker to Build Servers in Indonesia," *Jakarta Globe*, December 14, 2011, http://bit.ly/1Lk7iCY.

113 Linklaters, "Indonesia," http://bit.ly/1Meng2a; Regulation of the Government of the Republic of Indonesia, Number 82 of 2012 Concerning Electronic System and Transaction Operation, http://bit.ly/1L6lK2m; "Indonesia May Force Web Giants to Build Local Data Centers," *Asia Sentinel*, January 17, 2014, http://bit.ly/1j3E0g0; Vanesha Manuturi and BAsten Gokkon, "Web Giants to Build Data Centers in Indonesia?" *Jakarta Globe*, January 15, 2014, http://bit.ly/1VDExMJ; Anupam Chander and Uyên P. Lê, "Data Nationalism," *Emory Law Journal* 64, no. 3 (2015): 677-739, http://bit.ly/1jd7CgT.

114 http://www.kk-advocates.com/site/guidance-for-ott-service-providers-in-indonesia-is-finally-issued .

115 See, Andylala Waluyo, "Pemerintah Selidiki Telkomsel dan Indosat Terkait Isu Penyadapan," *Voice of America*, February 19, 2014, http://bit.ly/1laudZg.

116 For a full list of the laws, see Supriyadi, W, "Komentar Atas Pengaturan Penyadapan Dalam Rancangan," KUHAP, ICJR, policy paper, April 2013, http://bit.ly/1fdXN7W.

117 An excerpt of the decision is available in English at, "Excerpt From Decision of the Constitutional Court of the Republic of Indonesia," 2010, http://bit.ly/1hqGcCf; For the full decision (in Bahasa Indonesia), see, Nomor 5/PUU-VIII/2010, http://bit.ly/1VDFggJ.

actively used by an Indonesian intelligence agency known as the National Encryption Body at some point in 2015.[118] The body disguised its activity using a data server in Sydney, Australia.[119]

Intimidation and Violence

During the coverage period of the report, there were no reports of violence, travel restrictions, or torture as a result of online activities.

Spotlight on Marginalized Communities

Freedom on the Net 2016 **asked researchers from India, Indonesia, Kenya, Kyrgyzstan, Jordan, Mexico, Nigeria, and Tunisia to examine threats marginalized groups face online in their countries. Based on their expertize, each researcher highlighted one community suffering discrimination, whether as a result of their religion, gender, sexuality, or disability, that prevents them using the internet freely.**

In Indonesia, Haris Azhar examined internet freedom for religious minority communities in Indonesia.[1] The study found:

- Indonesia is home to diverse ethnic groups, religious beliefs, and languages, but government policies often contain discriminatory provisions against some ethnic and religious groups. In particular, indigenous religions lack formal recognition, and expressions of atheism are subject to criminal punishment, including online. In 2012, former civil servant Alexander Aan was sentenced to two and a half years in prison for inciting religious hatred and blasphemy after he publicly acknowledged his membership of a Facebook group for atheists.
- Online platforms allow minority groups to organize activities and document discrimination. One local leader of Jamaah Ahmadiyah, a Muslim group with beliefs that some other Muslims consider heretical, said that websites are a useful tool for tracking incidents of violence against his community. Activist Bona Sigalingging uses Facebook to agitate for Christian rights in Bogor, a town in West Java.
- Yet online harassment also disproportionately targets religious minority groups, threatening free expression. Oase, an organization of Shi'a Muslims, a minority in Indonesia, say that police have failed to respond to their complaints of continuous online harassment.

1 Haris Azhar, Research paper, November 2016, on file with F eedom House.

Technical Attacks

Politically-motivated cyberattacks against civil society groups have not been reported in Indonesia, though government and commercial sites are frequently targeted. ID SRTI (Indonesia Security Incident Response Team on Internet Infrastructure) reported 40 million incidences of cyberattacks in 2014, or approximately 100 attacks a day.[120]

118 https://citizenlab.org/2015/10/mapping-finfish s-continuing-proliferation/

119 See, ABC 730 program, 26/1/2016, "Indonesian government 'using Sydney server for spyware program'" , transcript of the talk is accessible at http://ab.co/1Q5HeRm

120 See http://bit.ly/1XPhtrI

Freedom House

Iran

	2015	2016
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	20	19
Limits on Content (0-35)	31	31
Violations of User Rights (0-40)	36	37
TOTAL* (0-100)	**87**	**87**

* 0=most free, 100=least free

Population:	**79.1 million**
Internet Penetration 2015 (ITU):	**44 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- Internet access improved in Iran, mainly on the back of higher internet speeds and the expansion of mobile internet (See **Availability and Ease of Access**).
- Telegram, the instant messaging app used by an estimated 20 million Iranians, came under pressure from the authorities to cooperate in censorship or face blocking (see Blocking and Filtering and **Content Removal**).
- Cartoonist Hadi Heidari spent around eight months in prison for posting a cartoon on Facebook in which he expressed sympathy with the French after the November 2015 terrorist attacks in Paris (see **Prosecution and Detentions for Online Activities**).
- Internet freedom activist Nizar Zakka and tech entrepreneur Arash Zad were arrested in September and July 2015, respectively, while visiting the country from abroad. Both remained in pretrial detention on murky charges. Canadian resident Saeed Malekpour has been imprisoned in similar circumstances since 2008 (see **Prosecution and Detentions for Online Activities**).
- Hossein Ronaghi Maleki, Vahid Asghari, and fi e Facebook users secured early releases from lengthy prison sentences amid mixed displays of clemency and repression in the country (see **Prosecution and Detentions for Online Activities**).
- The Supreme Council on Cyberspace gave foreign messaging companies like Telegram one year to store data on Iranian users within the country in a move to increase monitoring and censorship (see **Surveillance, Privacy, and Anonymity**).

Introduction

In Iran, greater access was offset by lengthy prison sentences and arbitrary detentions, keeping the country's internet one of the least free in the world.

The implementation of the Joint Comprehensive Plan of Action, commonly referred to as the Iran nuclear deal, brought hope of a more free and open internet. Indeed, the internet has become faster and more widely available in recent years given the government's investment in technology and regulatory moves to increase competition. However, President Hassan Rouhani's promises to introduce greater personal and social freedoms have been checked by more conservative factions within the state, principally the judiciary and Islamic Revolutionary Guards Corps (IRGC), whose leaders control most companies in the ICT sector. News websites on all sides of the political spectrum have been censored for failing to adhere to strict guidelines on how to cover political events, such as the nuclear deal.

Tensions between so-called reformists and conservatives regularly play out on the digital sphere, often with devastating consequences for innocent users. Conservatives have fought against all manner of liberalization, opposing everything from higher mobile internet speeds to the messaging app Telegram. Fretful that the nuclear deal will lead to the "infiltration of Iranian society by Western ideas,[1] conservatives have cracked down on group chat administrators, tech entrepreneurs, and even Instagram models. Several security agencies aggressively monitor social media for anything perceived as insulting to public leaders or contrary to conservative religious values. Indeed, authorities regularly spread fear among users by announcing intentions to step up surveillance, such as in preparation for the February 2016 elections to the parliament (*Majlis*) and Assembly of Experts—the body that will eventually appoint a replacement for the ageing supreme leader, Ayatollah Ali Khamenei.

Despite these limitations, the internet remains a vital resource for Iranian citizens. Access to information is improving through the use of virtual private networks (VPNs) and other circumvention tools that allow access to blocked content. Iranians are also communicating with each other at unprecedented levels. Encrypted messaging apps afford some degree of privacy to average users, although authorities are constantly attempting to undermine privacy through spyware and data localization laws. In many ways, internet use in Iran remains a cat-and-mouse game in which tech savvy individuals try to push red lines and circumvent the harsh restrictions imposed on them by state security.

Obstacles to Access

Most improvements to internet freedom that have come under the presidency of Hassan Rouhani relate to access and the ICT market. The ICT ministry's budget reached its highest level in history, reflecting increasing investments in both internet infrastructure and censorship tools. Internet speeds remain slow, although a significant rise was noted over the past year.

1 See for example, "IRGC blocks the enemy's infiltration" Speech by Ayatollah Khamenei on September 16, 2015, http://english.khamenei.ir/news/2155/IRGC-blocks-the-enemy-s-infiltratio , and "Negotiation with US 'very fact of infiltration'," Mehr News Agency, November 2, 2015, http://en.mehrnews.com/news/111595/Negotiation-with-US-very-fact-of-infiltratio .

Availability and Ease of Access

Internet penetration statistics in Iran are notoriously contested and unreliable. According to Morteza Mousavian, head of the Digital Media and Information Technology Center (SARAMAD), internet penetration in Iran was at 53 percent by 2015. This would mean 40 million people are connected to the internet in the country, including 11 million people accessing the internet on their mobile devices.[2] However officia statistics covering the fi st quarter of the Iranian year 1394 (March 21- June 21, 2015) place the figu e at 82.12 percent.[3] Meanwhile, a report from the Internet Society argued that Iran's internet penetration rate was only 31.4 percent, ranking it 112th internationally behind Thailand, Algeria, Indonesia and India.[4]

Internet prices are high, particularly relative to the low quality of service provided. This is partially due to the fact that the state-owned Telecommunications Infrastructure Company (TIC) holds an effective monopoly on bandwidth in the country, which they sell on to internet service providers (ISPs) at a considerable markup. In addition, the demand for bandwidth far outstrips what is available.[5]

Despite constant promises to improve the speed and quality of internet connectivity, poor service persists. In October 2015, Deputy ICT Minister Nasrollah Jahangard acknowledged that the actual speed of an internet connection advertised at 2 Mbps is only 100 Kbps.[6] According to Akamai, the leading global content delivery network, Iran had one of the Middle East's lowest average peak connection speeds in early 2016.[7] However, average speeds improved by 44 percent over 12 months.

The Rouhani administration has demonstrated a consistent commitment to developing SHOMA, the national information network. In addition to frequent statements declaring SHOMA a top priority, the government has devoted a considerable share of the ICT budget to SHOMA. Iran's overall ICT budget for 2016-17 is higher than it has ever been, and funding for SHOMA is up 44 percent from last year.[8]

While SHOMA increases bandwidth and improves browsing speeds when accessing government approved websites,[9] it also enables the authorities to strengthen their grip over the flo of internet traffi in the country. Moreover, it gives the government the ability to throttle connection speeds during politically sensitive periods without crippling critical services. However, it may be a while before SHOMA has any significan impact on internet access in Iran, as the implementation period for SHOMA has recently been extended to March 2020.[10]

2 Small Media, *Iranian Internet Infrastructure and Policy Report: October 2015,* https://smallmedia.org.uk/news/iiip-october-2015.

3 Small Media, *Iranian Internet Infrastructure and Policy Report: November 2015,* https://smallmedia.org.uk/news/iiip-november-2015.

4 See "Global Internet Maps," Internet Society, accessed October 2016, http://bit.ly/2fCoeg5.

5 "Check the price and quality of Internet access in Iran," Iran's Majlis research Center, http://rc.majlis.ir/fa/report/show/879513.

6 See http://bit.ly/2fRaUt3.

7 Akamai, *State of Internet: Q1 2016 Report*, https://www.akamai.com/uk/en/multimedia/documents/state-of-the-internet/akamai-state-of-the-internet-report-q1-2016.pdf.

8 Small Media, *Iranian Internet Infrastructure and Policy Report: January 2016,* https://smallmedia.org.uk/news/iiip-january-2016

9 "Minimum speed on SHOMA reportedly 2mbps," [Farsi] Mehr News Agency, http://bit.ly/2eSXVSz.

10 "Minimum speed on SHOMA reportedly 2mbps," [Farsi] Mehr News Agency, http://bit.ly/2eSXVSz.

Restrictions on Connectivity

The Telecommunications Infrastructure Company (TIC) retains a monopoly on internet traffi flowin in and out of Iran.[11] The TIC is a state-owned enterprise under the ICT ministry. The arrangement affords the Iranian authorities with total control over the internet backbone, as well as the ability to limit access or throttle speeds during sensitive political moments, which last occurred in the lead-up to the 2013 presidential elections. The heavy influenc of the TCI in the ICT market also grants the security apparatus the ability to control third-party ISPs and to monitor online activities, since the TCI's majority shareholder is the Islamic Revolutionary Guard Corps (IRGC).[12]

ICT Market

The telecommunications industry in Iran is tightly controlled by the government or related entities. In recent years, the role of the IRGC—a politically important branch of the security forces that also controls large sections of the economy—in the ICT sector has notably increased.[13] In September 2009, for example, the IRGC purchased a controlling stake in the Telecommunications Company of Iran (TCI), the country's main provider of internet and mobile phone services. Other providers must purchase bandwidth from the Data and Communication Company (DCC). Direct access to the internet via satellite is only permitted for certain institutes and is prohibited for personal use.

The mobile phone market is under similar state influence MTN IranCell, the second largest mobile operator behind the TCI, is owned in part by a web of proxy companies controlled by the government and IRGC.[14] According to statistics released by the ICT ministry in November 2015, MTN IranCell and the TCI controlled a combined 97 percent of the mobile market in Iran.[15]

Yet even this quasi-duopoly indicates an improvement. Last year, the ICT Ministry did not renew an exclusive 3G contract issued to IRGC-affilia ed mobile provider RighTel, allowing other carriers to enter the mobile market.[16]

Regulatory Bodies

There is no independent regulatory body for ICTs in Iran. The Communications Regulatory Authority (CRA), which falls under the ICT Ministry, is responsible for telecommunications licensing. Its head is appointed by the ICT minister.[17] The CRA has taken several actions to improve quality of service and reduce prices for Iranian users. For example, the CRA awarded licenses that allowed new ISPs to enter the market, thereby increasing consumer choice.[18] Furthermore, in December 2015, the CRA

11 Small Media, *Iranian Internet Infrastructure and Policy Report: July 2015,* https://smallmedia.org.uk/media/articles/files_IIIP_Jul15.pdf#page=9, pg. 9-11.

12 Sreberny and Khiabany, *Blogistan: The Internet and Politics in Iran,* (London: IB Tauris, 2010), pg. 5.

13 "The Revolutionary Guards is entering the IT market," [Farsi] *Digarba*n, December 12, 2011, http://www.digarban.com/node/3715.

14 Steve Stecklow, "Exclusive: Iranian cell-phone carrier obtained banned U.S. tech," Reuters, June 4, 2012, http://www.reuters.com/article/us-iran-mtn-sanctions-idUSBRE8530SO20120604.

15 "72 million mobile phones in the hands of Iranians," [Farsi] Mehr News, http://bit.ly/2fR6Qcm.

16 "Iran ranks fi st in the Middle East for hosting information," [Farsi] Mehr News, http://bit.ly/2f848Pj.

17 Communications Regulatory Commission of Iran, officia website, accessed July 31, 2012, http://bit.ly/1Lum12y.

18 "The entry of new operators into the internet market from September," [Farsi] Mehr News, http://bit.ly/2eRXs3Y.

compelled ISPs to implement quality control measurements on the services they offer to customers.[19] The CRA has also pushed for internet infrastructure development, including increasing the number of IP addresses available in Iran[20] and pushing to expand internet access to thousands of rural villages.[21]

The country's top internet policy body, however, is the Supreme Council of Cyberspace (SCC). The SCC was established by decree of the Supreme Leader Khamenei in March 2012. It is intended to provide a centralized focal point for policymaking and the regulation of Iran's virtual space, effectively minimizing the roles of the executive, legislative, and judicial branches of the government and bringing internet policy under Khamenei's direct control. Observers believe this reflec ed Khamenei's dwindling trust in former president Mahmood Ahmadinejad to lead such an important area of policy.

Over the past year, the SCC has been routinely criticized for being disorganized,[22] not holding enough meetings,[23] and has even been rebuked by Ayatollah Khamenei for not doing enough to encourage Iranians to use the Internet in a "clean" and Islamic fashion.[24] In September 2015, Supreme Leader Khamenei consolidated the SCC's power over internet policy and made some personnel changes to the council. In April, the SCC dissolved and assumed the powers of the High Council of Informatics, the Supreme Council of Information, and the Supreme National Security Council of Information Exchange (AFTA).[25]

Limits on Content

Significant restrictions on content have been in place since 2009. Platforms like Facebook and Twitter remain blocked, although newer social media and communication apps such as Telegram and Instagram are generally accessible. Censorship decisions remain highly politicized, with both conservative and reformist news sites censored for failing to adhere to strict guidelines on how to report on sensitive political, social, and international issues. Self-censorship remains pervasive and overt digital activism is limited.

Blocking and Filtering

The Iranian authorities continued to restrict access to tens of thousands of websites, particularly those of international news sources, the opposition, ethnic and religious minorities, and human rights groups.[26] Websites are also fil ered if they differ from the officia doctrine of the state's Islam or its chosen narrative on domestic or international politics, such as relations between Iranian political institutions or the nuclear deal. Internet censorship is highly politicized in the country, often reflectin tensions between conservatives and reformists in the country. Days before the February

19 "Launch of control system for operators of internet usage," [Farsi], Itmen, http://www.itmen.ir/index.aspx?pid=99&articleId=88741.

20 "Internet access is provided in the aircraft, Fiber optic network modernization" [Farsi] Mehr News, http://bit.ly/2eMxFL2.

21 "Start of Internet Directory to 37,000 village," [Farsi] Mehr News, http://bit.ly/2eRX2L2.

22 "Labor system remained pending at the Supreme Council of Cyberspace," [Farsi] Mehr News, http://bit.ly/2ebyRGm.

23 "Zarghami criticized the lack of meetings of the Supreme Council of Cyberspace," [Farsi] Itmen, http://itmen.ir/index.aspx?pid=99&articleId=85338.

24 "The Supreme Leader complains about the Supreme Council of Cyberspace and Communications Ministry," [Farsi] Alef, http://alef.ir/vdcamwnea49nmu1.k5k4.html?350258.

25 See http://bit.ly/2eKimUk.

26 Small Media, "April 2016," *Filterwatch*, https://smallmedia.org.uk/media/articles/files/IIIP_APRIL16.pd .

26, 2016 elections, List-e Omid (The Hope List), a website promoting reformist candidates backed by President Rouhani, was blocked. [27]

Facebook and Twitter remained blocked in the country. Despite apparently being used by a number of prominent officials including the office of the president, foreign minister, and supreme leader, these platforms have not been available without circumvention tools since 2009. After authorities blocked Viber, Telegram became the most widely used instant messaging app in the country with an estimated 20 million users, surpassing even Facebook.[28] Following last year's tense standoff between Rouhani's ICT ministry and the Committee to Determine Instances of Criminal Content (CDICC) over proposals to block WhatsApp, Telegram seems to have created a new venue for conflict

In October 2015, Telegram CEO Pavel Durov claimed that the ICT Ministry demanded the company provide them with "spying and censorship tools." After Telegram refused, users reported temporary disruptions to the app.[29] The CDICC voted against blocking the app—likely over the public outcry the decision would create—but Telegram has reportedly agreed to cooperate in removing accounts belong to Islamic State (IS) figh ers from the site, and in one case, also removed a channel which advocated boycotting the February 2016 elections.[30] There were also reports of brief disruptions to Instagram access in mid-2015, apparently due to technical errors in the country's "intelligent fil ering" system.[31]

Websites are also fil ered on an ad hoc basis, often with no explanation. For example, authorities blocked "Kheft Giri," a crowdsourcing website designed to map crime incidents in Tehran, just two days after its officia launch in November 2015. This move forced the founders to shut down the site.[32] Similarly, authorities blocked Gershad, a mobile app used to crowdsource the location of the so-called morality police and to notify users in real-time.[33]

Since taking office the administration of President Hassan Rouhani has sought to assume more direct control over ICT policy in Iran. However, such moves have been met with fie ce opposition from hardliners such as Sadeq Larijani, head of Iran's judiciary. Larijani has emphasized that the main decision-maker regarding internet censorship in Iran is the CDICC, not the government, and highlighted that the law determines which websites and services must be blocked.[34] The Computer Crimes Law (CCL) of 2009 specifie violations that might result in a website being marked for fil ering. These are

27 "New App Lets Iranians Download Information Via Satellite and Bypass State's Internet Censorship," International Campaign for Human Rights in Iran, March 18, 2016, https://www.iranhumanrights.org/2016/03/toosheh-mehdi-yahyanejad/.

28 Saeed Kamali Dehghan, "Telegram: the instant messaging app freeing up Iranians' conversations," *The Guardian*, February 8, 2016, https://www.theguardian.com/world/2016/feb/08/telegram-the-instant-messaging-app-freeing-up-iranians-conversations.

29 BBC Persian, "Telegram temporarily blocked after lack of cooperation with Iran," [Farsi] October 2015, http://www.bbc.com/persian/iran/2015/10/151019_u04_telegram_iran.

30 Amir-Esmaeil Bozorgzadeh, "Updated; Telegram's Troubled Times in the Middle East," *Tech Crunch*, January 12, 2016, https://techcrunch.com/2016/01/12/telegrams-troubled-times-in-the-middle-east/.

31 "A New Round of Intimidation, Arrests, and Prosecution of Social Media Users in Iran," International Campaign for Human Rights in Iran, June 14, 2015, https://www.iranhumanrights.org/2015/06/intimidation-arrests-social-media-users/.

32 See [Farsi] http://bit.ly/2eMzHL4.

33 Shima Shahrabi, "Morality Police App Blocked Hours after Launch," Iran Wire, February 10, 2016, https://en.iranwire.com/features/7076/.

34 "Larijani criticizes Rouhani over Internet policies," [in Farsi] *BBC Persian*, accessed March 29, 2015, http://bbc.in/1OwuSn1.

define very broadly and range from insulting religious figu es and government official to distributing pornographic content and the use of illegal circumvention tools.[35]

In an effort to show that content fil ering is based on a legal framework, institutions have been created to oversee internet fil ering. The Committee for Determining Instances of Criminal Content (CDICC) is empowered to identify sites that carry forbidden content and report such information to the TCI and other major ISPs for blocking. The committee is headed by the prosecutor general, and its members are representatives from 12 governmental bodies. Little information is available about the inner workings of the committee, and censorship decisions are often arbitrary and nontransparent.

Internet fil ering, which began toward the end of the Khatami presidency in 2005, has become more severe since the disputed presidential election in June 2009. Iranian authorities currently employ a centralized fil ering system that can effectively block a website within a few hours across the entire network in Iran. However, ICT Minister Mahmoud Vaezi recently suggested that Iran may restore censorship power to ISPs in the future.[36] Private ISPs are forced to either use the bandwidth provided by the government or route traffi containing site-visit requests through government-issued fil ering boxes developed by software companies inside Iran. The fil ering boxes inspect unencrypted HTTP requests looking for banned text strings—either keywords or domain names—in the URL requests submitted by users, and block access accordingly.

Official continue to call for an "intelligent fil ering" system, using deep-packet inspection (DPI) to allow for the blocking of specifi pages within a site rather than blocking the entire site. However, blocking individuals pages sent over an encrypted connection (HTTPS) will be technically very resource intensive, if not impossible. For instance, after the ICT minister announced that intelligent fil ering had been successfully applied to Instagram, Instagram enabled a default SSL encryption on its entire platform, resulting in blocked pages becoming available again. As it stands today, Instagram pages cannot be blocked individually, due to the platform's default use of SSL. However some images might not available because they are hosted on Facebook's servers, which are blocked in the country.

These developments have not gone unnoticed by some authorities. CDICC Secretary Abdolsamad Khoramabadi noted in September 2015 that the "intelligent fil ering" program had failed in light of developments in web encryption.[37] This has done little to dampen the Rouhani government's enthusiasm for intelligent fil ering, with ICT Minister Mahmood Vaezi announcing a further investment of US$66 million into the program in the past year alone.[38]

Content Removal

Aside from fil ering, Iran also employs administrative measures to remove unwanted content from the web. Website owners must register their sites with the Ministry of Culture and are then subject to requests to remove particular posts deemed unacceptable by the government. The 2009 Comput-

35 "Islamic Republic of Iran: Computer Crimes Law," Article 19, 2012, https://www.article19.org/data/files medialibrary/2921/12-01-30-FINAL-iran-WEB[4].pdf, and "12 members of Committee in Charge of Determining Unauthorized Sites," [in Farsi] *Weblognews*, December 16, 2009, http://bit.ly/1Owwpcu.

36 "Launch of the National Information Network in 1395," [Farsi] Mehr News, http://bit.ly/1ROD4Ot.

37 "Intelligent fil ering of Instagram failed," [Farsi] Fars News Agency, http://www.farsnews.com/newstext.php?nn=13940616000464.

38 "200 million dollars allocated for smart fil ering," [Farsi] Mehr News, http://bit.ly/2eGWJ5o.

er Crime Law (CCL) makes service providers, such as blogging platforms, responsible for any content that appears on their sites. This has led to the suspension of blogs or shuttering of news websites hosted on platforms inside Iran, under orders from government officials News websites are consistently warned how to cover controversial political or social topics, such as Iran's nuclear deal[39] or former reformist president Mohammad Khatami.[40] The website of state-owned Iranian Labor News Agency was blocked for two days in June 2015 and fi e journalists lost their jobs for refusing to censor coverage of labor protests.[41]

In a recent operation dubbed "Spider II," police reportedly identifie 170 models, photographers, and make-up artists involved in posting pictures of women not wearing a headscarf. Many of the targeted individuals had their Facebook or Instagram pages removed or were pressured into closing the pages themselves.[42] Telegram has also agreed to cooperate with the government in taking down IS channels from the messaging app, although in at least one case, political channels were also reportedly removed (See "Blocking and Filtering" for more on Telegram).

Media, Diversity, and Content Manipulation

Self-censorship is extensive, particularly on political matters. Widespread arrests and harsh sentences meted out to journalists, activists, and ordinary citizens, as well as perceptions of pervasive surveillance, have increased fear. Many online journalists and bloggers abandoned their online activities or used pseudonyms after the 2009 crackdown, resulting in a palpable drop in the amount of original content produced by users based inside the country. The situation slightly improved after Rouhani assumed the presidency, especially among reformist journalists. Nevertheless, the same restrictions remain in place, and journalists continue to be prosecuted.

In addition to fil ering, censorship, and intimidation, the state counters critical content and online organizing efforts by extending regime propaganda into the digital sphere. The government has backed numerous initiatives to promote blogging among its supporters and members of the Basij paramilitary group.[43]

Furthermore, the majority of independent content producers lack the financia resources to operate in such a hostile environment. The online advertising market in Iran is exclusively limited to apolitical and pro-government websites. Even businesses based outside Iran avoid political websites to maintain trading relationships with the country. Although the United States adjusted its sanctions against Iran to enable American internet companies to provide services to Iranian users, Google Advertising

39 See "11.08.2015 – Conservative weekly closed for third time," in *Press freedom violations recounted in real time January-December 2015*, Reporters Without Borders, https://rsf.org/en/news/press-freedom-violations-recounted-real-time-january-december-2015.

40 Rick Gladstone, "Iran Editor Is Charged With Defying Ban on Covering Ex-President," *The New York Times,* December 8, 2015, http://www.nytimes.com/2015/12/09/world/middleeast/iran-editor-is-charged-with-defying-ban-on-covering-ex-president.html.

41 See "24.06.2015-State news agency fi es fi e journalists for covering strike," in *Press freedom violations recounted in real time January-December 2015*, Reporters Without Borders, https://rsf.org/en/news/press-freedom-violations-recounted-real-time-january-december-2015.

42 "Iran arrests female models for posing without hijabs," *Al Jazeera*, May 16, 2016, http://www.aljazeera.com/news/2016/05/iran-arrests-fashion-girls-posing-hijabs-160516131844774.html.

43 "Computer Crimes in Iran: Risky Online Behaviour," Article 19, 2015, https://www.article19.org/data/files_medialibrary/38039/Risky-Online-Behaviour--final-English.pd .

still does not allow an ad campaign to target Iran as a country,[44] disadvantaging domestic content producers as well as content producers in the diaspora seeking to cultivate an audience inside Iran. Any Iranian-linked company or individual who wishes to use Google AdSense must apply for a specifi license, which is not a convenient process for the majority of Iranian content producers.

Iranian authorities actively support Iranian social networks and mobile app developers by offering free bandwidth and hosting, with the aim of attracting Iranian users to these platforms over those based outside of Iran. In the past year, a number of Iranian apps have been launched.[45] In addition, the Iranian government has launched several domestic search engines, and has agreed to collaborate with Russia to establish other domestic platforms.[46]

Digital Activism

Despite ongoing blocks on Facebook and Twitter, Iranians use social media to communicate, raise awareness of societal issues, and even campaign in elections, particularly on the app Telegram. Younger candidates took to the messaging app to reach potential voters and share candidate lists ahead of the February 2016 elections.[47] Prominent blogger "Vahid Online" runs a Telegram group with some 20,000 followers that was called "must follow for journalists, media workers and anyone interested in news and information about Iran's political and social events." Vahid Online won Deutsche Welle's People's Choice Award for Citizen Journalism.[48]

Gershad, an app that uses crowd-sourced information to alert Iranians of the whereabouts of the moral police, won the Jury's Prize in the "Tech for Good" category. Finally, one recent Twitter campaign gave Iranians the opportunity to discuss how they have been affected by sanctions on online platforms and services, using the hashtag #فنآتحریم (#TechSanctions).[49]

Violations of User Rights

Despite hopes that the nuclear agreement might lead to a more open climate for internet users, hardliners have responded to the deal by cracking down on criticism and Western "infiltration." Authorities have upped their monitoring of social media and technical attacks against opposition voices. There have been some positive steps, such as the early release of several activists and journalists, but user rights remain perilous in Iran today.

Legal Environment

Iran continues to be an extremely dangerous environment for internet users. Iranian laws heavily restrict what is acceptable speech online and specify harsh punishments for those who deliberately

44 "Google Traffi is here but what does it maen for Iran?" Techrasa, December 26, 2015, http://techrasa.com/2015/12/26/google-traffic-mean-iran .

45 "Viber and WhatsApp messenger rival Iran's Saina," [Farsi] Fars News Agency, http://www.farsnews.com/newstext.php?nn=13931115001225.

46 "Russian search engine's launch," [Farsi] Mehr News, http://bit.ly/2ebyN9t.

47 Christopher Miller, "Messaging app Telegram is shaking up Iran's elections," February 25, 2016, *Mashable*, http://mashable.com/2016/02/25/iran-elections-telegram-app/#8UCotmNtqkq6.

48 "Best of Online Activism," Deutsche Welle, 2016, https://thebobs.com/english/category/2016/?only_winners=true.

49 See Twitter hashtag, http://bit.ly/2fYG7K7.

flou restrictions, as well as those who have inadvertently drawn the ire of authorities. The constitution provides for limited freedom of opinion and expression, but numerous, haphazardly enforced laws restrict these rights in practice. The 2000 Press Law, for example, forbids the publication of ideas that are contrary to Islamic principles or detrimental to public rights, none of which are clearly defined The government and judiciary regularly invoke this and other vaguely worded legislation to criminalize critical opinions.

The 2009 CCL outlines punishments for spying, hacking, piracy, phishing, libel, and publishing materials deemed to damage "public morality" or to be a "dissemination of lies." Punishments are severe and include the death penalty for offenses against public morality and chastity, as well as long prison sentences, draconian fines and penalties for service providers who fail to enforce government content restrictions. [50]

Prosecutions and Detentions for Online Activities

Amid domestic political tensions between reformists and conservatives, hardliners within the judiciary and IRGC have conducted a campaign against the country's "infiltration by Western ideas, individuals, and companies. Numerous dual citizens active in journalism, human rights, or ICT development work have been jailed by the authorities, often with little explanation.[51]

Nizar Zakka, a Lebanese citizen with permanent residency in the U.S., was detained in September 2015 after giving a talk at a state-sponsored conference in Tehran, for which he received an officia invitation.[52] Zakka heads the Arab internet freedom organization IJMA3, which has received hundreds of thousands of dollars of funding from the U.S. State Department and USAID for projects in support of internet freedom.[53] One year after his arrest, he was sentenced to 10 years in prison and fine US$4.2 million.[54] Iranian state television claimed he had "deep ties to the U.S. intelligence and military establishment."

In July 2015, tech entrepreneur and blogger Arash Zad (editor and contributor at *Weblogina*, *Arashzad*, and *Ladybug*) was arrested. Phishing emails were reportedly sent out to his contacts while he was in custody.[55] In September, human rights blogger Mohsen Sadeghinia (*Openeyes*) was arrested. Both of their blogs were also blocked.[56]

In February 2016, a court ruled to confi m long prison sentences issued to four individuals working for the technology review website *Narenji based in the city of Kerman.* Ali Asghar Honarmand, Hossien Nozari, Ehsan Paknejad, and Abass Vahedi were sentenced to 11, 7, 5, and 2.5 years respec-

50 Islamic Republic of Iran: Computer Crimes Law Article 19, January 30, 2012, www.article19.org/data/files medialibrary/2921/12-01-30-FINAL-iran-WEB[4].pdf.

51 "Former BBC Persian journalist 'detained in Iran'," BBC News, February 4, 2016, http://www.bbc.co.uk/news/world-middle-east-35492065.

52 Associated Press, "Iranian state TV claims US resident in custody is a spy," *The Guardian,* November 3, 2015, http://www.theguardian.com/world/2015/nov/03/iran-state-tv-american-spy-nizar-zakka .

53 Mahsa Alimardani, "Reality, Conspiracy and the US 'Internet Freedom' Agenda: Deconstructing Iran's Case Against Nizar Zakka," Global Voices, October 10, 2016, https://advox.globalvoices.org/2016/10/10/reality-conspiracy-and-the-us-internet-freedom-agenda-deconstructing-irans-case-against-nizar-zakka/.

54 Associated Press, "Iran sentences US resident to 10 years in jail over spying claims," *The Guardian*, September 20, 2016, https://www.theguardian.com/world/2016/sep/20/iran-sentences-us-resident-to-10-years-in-jail-after-spying-claims.

55 Mahsa Alimardani, "The Arrest of Arash Zad, Iran's Sart-Up Kid," Global Voices, September 23, 2015, https://advox.globalvoices.org/2015/09/23/the-arrest-of-arash-zad-irans-start-up-kid/.

56 See "16.09.2015 - Two bloggers arrested," in *Press freedom violations recounted in real time January-December 2015*, Reporters Without Borders, https://rsf.org/en/news/press-freedom-violations-recounted-real-time-january-december-2015.

tively on charges of "designing sites, websites, and creating content for media hostile to the regime" according to one report. They had been initially arrested in December 2013 along with 10 colleagues, seven of which received suspended sentences. [57]

Saeed Malekpour, a permanent resident of Canada, has been in prison since 2008 for writing open source software that third parties had used for sharing pornographic photos. He was sentenced to death on charges of "threatening the nation's Islamic ideals and national security via propaganda against the system," allegedly tortured, and forced to publicly confess.[58]

On June 8, 2015, the IRGC arrested "several individuals" for social media activity deemed as "against national security." As Reporters Without Borders (RSF) noted, the individuals included internet activists Mahmud Moussavifarand and Shayan Akbarpour, who ran the Facebook page "Rahian" and a blog called Rahi.[59]

Several women were arrested on suspicions of not adhering to conservative dressing guidelines. Eight women were arrested in May 2016 for not wearing headscarves in modeling photos posted to Instagram. The woman who manages "Persian Blog," a publishing tool, was also detained. Some were made to go on live television and repent.[60] After winning a seat in the February elections, reformist parliamentarian Minoo Kaleghi was banned from holding offic by the judiciary after a picture emerged of her on social media without her headscarf. A few days earlier, the Telegram group admin who posted the photos—which Kaleghi claimed are fake—was arrested.[61]

Artist Hadi Heidari was arrested in November 2015 after he posted his cartoon on Facebook expressing sympathy after the Paris attacks. He was not released until April 2016, when he celebrated by posting another cartoon to Instagram.[62] In October 2015, Hassan Shikhaghai, the editor of news site *Ruwange*, was arrested and kept in prison until December 2015, when he was released pending trial.[63] In February 2016, journalist Bahman Daroshafaei was arrested by authorities, who then took over his Telegram account and sent phishing messages his contacts in a bid to reveal sensitive information. A researcher with the ICHRI contacted Telegram to have his account disabled. A similar situation occurred with Issa Saharkhiz in November 2015.[64]

Journalist and blogger Mohammad Reza Fathi was sentenced to 444 lashes in April 2016. Fathi had

57 See "18.02.2016 – Four Narenji website employees returned to prison," in "Press freedom violations recounted in real time January 2016," Reporters Without Borders, https://rsf.org/en/news/press-freedom-violations-recounted-real-time-january-2016, and "Technology Website Staffers Rushed to Prison Before Appeals Court Verdict," International Campiagn for Human Rights in Iran, February 18, 2016, https://www.iranhumanrights.org/2016/02/four-it-professionals-imprisoned-in-kerman/.

58 Mahsa Alimardani, "Help End the Imprisonment of Iranian Web Developer Saeed Malekpour," Global Voices, October 3, 2016, https://advox.globalvoices.org/2016/10/03/help-end-the-imprisonment-of-iranian-web-developer-saeed-malekpour/.

59 "Revolutionary Guards target Internet activists," Reporters Without Borders, June 22, 2015, http://en.rsf.org/iran-revolutionary-guards-target-22-06-2015,48020.html.

60 Thomas Erdbrink, "Iran's Hard-Liners Crack Down on Models Not Wearing Head Scarves," *The New York Times*, May 16, 2016, http://www.nytimes.com/2016/05/17/world/middleeast/irans-hard-liners-crack-down-on-models-not-wearing-head-scarves.html?_r=0.

61 Thomas Erdbrink, "She Won a Seat in Iran's Parliament, but Hard-Liners Had Other Plans," *The New York Times*, May 11, 2016, http://www.nytimes.com/2016/05/12/world/middleeast/iran parliament-minoo-khaleghi.html.

62 Tori Egherman, "Imprisoned Iranian Cartoonist Hadi Heidari Goes Free," Global Voices, April 27, 2016, https://advox.globalvoices.org/2016/04/27/imprisoned-iranian-cartoonist-hadi-heidari-goes-free/.

63 See "29.03.2016 - Two journalists freed pending trial." "Press freedom violations recounted in real time January 2016," Reporters Without Borders, https://rsf.org/en/news/press-freedom-violations-recounted-real-time-january-2016.

64 Lorenzo Franceschi-Bicchierai, "Iran Appears to Have Taken Over an Arrested Journalist's Telegram Account," *Motherboard,* February 5, 2016, https://motherboard.vice.com/read/iran-telegram-account-bbc-journalist.

posted an article critical of the Saveh municipal government on his blog[65] and was convicted of "defamation and publishing false information." He was arrested in August 2012 and subsequently released on bail, although his trial did not begin until April 2015.[66]

Authorities have also targeted individuals for running popular groups on chat apps. In June 2015, cyber police announced the arrest of an individual they claim managed 23 WhatsApp and Line groups that allegedly published false and immoral content.[67] Five months later, the IRGC announced it had arrested more than 20 Telegram group admins for sharing "immoral content… insulting to Iranian officials as well as "satire and sexual advice." Telegram has an estimated 20 million users in the country.[68]

There have been some positive developments from over the past year. In June 2016, fi e activists who had been serving lengthy prison terms were released early. Amir Gholestani, Fariborz Kardarfar, Masoud Ghasemkhani, Seyyed Masoud, Seyyed Talebi, and Amin (Faride) Akramipour will still have to perform monthly visits to the authorities as part of their fi e-year suspended sentences. All fi e had been arrested in September 2013 due to posting about human rights abuses on Facebook and, along with three others, were convicted of "insulting what is sacred" and "insulting the Supreme Leader of the Revolution."[69] Two of those three others were released previously, while a third, Roya Saberi Negad Nobakht, remained in prison.

Cartoonist Atena Farghadani, who in August 2015 had been sentenced to 12 years in prison, was released in May 2016 after spending 18 months in detention. Earlier, an appeals court had acquitted her of "assembly and collusion against the state" and suspended her sentence for "insulting the supreme leader."[70] She had been originally arrested on charges of insulting state official and spreading propaganda for posting an image of a parliamentary vote on reproductive rights, in which she depicted members of parliament as animals. She was released in December 2015, only to be rearrested one month later after uploading a video describing the abuse she faced at the hands of prison guards.[71]

Hossein Ronaghi Maleki, a blogger arrested in December 2009 for helping Iranians circumvent censorship, was released on bail in May 2016 after a hunger strike protesting his 15-year imprisonment for "spreading propaganda against the regime," "membership of the Internet group Iran Proxy, and "insulting the Iranian supreme leader and the president."[72] Observers are concerned he may be called back to prison unless charges are dropped.

65 See http://www.pooria6.blogfa.com/

66 See "22.08.2016 – Court upholds decision to flo blogger." "Press freedom violations recounted in real time January 2016," Reporters Without Borders, https://rsf.org/en/news/press-freedom-violations-recounted-real-time-january-2016

67 "A New Round of Intimidation, Arrests, and Prosecution of Social Media Users in Iran," International Campaign for Human Rights in Iran, June 14, 2015, https://www.iranhumanrights.org/2015/06/intimidation-arrests-social-media-users/.

68 Bozorgmehr Sharafedin and Sam Wilkin, "Iran's Revolutionary Guards target popular messaging app in widening crackdown," Reuters, November 15, 2015, http://www.reuters.com/article/us-iran-rights-socialmedia-idUSKCN0T40MU20151115.

69 See "15.06.2016 – Five Internet activists freed conditionally," in "Press freedom violations recounted in real time January 2016," Reporters Without Borders, https://rsf.org/en/news/press-freedom-violations-recounted-real-time-january-2016.

70 "Young Artist Who Lampooned Iranian MPs Released From Prison, International Campaign for Human Rights in Iran, May 4, 2016, https://www.iranhumanrights.org/2016/05/atena-farghadani-released/.

71 International Campaign for Human Rights in Iran, "Iran Sentences Atena Faraghdani to 12.5 Years for Cartoons," *Global Voices*, June 3, 2015, http://bit.ly/1ANI5lH.

72 Netizen Report Team, "Netizen Report: Facebook and Twitter Disappear in Uganda Amid Election Tensions," May 12, 2016, https://advox.globalvoices.org/2016/05/12/netizen-report-facebook-and-twitter-disappear-in-uganda-amid-election-tensions/.

Citizen journalist Vahid Asghari was released on April 4, 2016 after he had originally been given a death sentence for "publishing false information with the aim of stirring up public opinion," "activities threatening national security," and "hosting anti-Islamic and counter-revolutionary websites and collaborating with foreign media." After an international outcry, his sentence had twice been reduced.[73]

Soheil Arabi had his death sentence overturned by the Supreme Court, but was sentenced to 7.5 years for "insulting the Prophet" on Facebook in June 2015. He was originally arrested in November 2013 by the IRGC. According to a source, Soheil "must read 13 books on theology and religious awareness" and make monthly presentations to the court on the topic as part of his sentence. He is also serving a three-year sentence for "insulting the Supreme Leader" and "waging propaganda against the state."[74]

Surveillance, Privacy, and Anonymity

The online sphere is heavily monitored by the state in Iran. In preparation for elections to the legislature and Assembly of Experts, Iran's deputy interior minister for security announced a new "Elections Security Headquarters" would be established "to monitor cyberspace."[75] Similarly, the IRGC launched a military exercise named "Eghtedare Sarallah" in September 2015, which included the monitoring of social media activities.[76] In June 2015, Iran's Cyber Police (FATA) created a new unit for monitoring computer games.[77]

It remains unclear how the authorities can technically monitor the content of messages on foreign social networks, given that some apps encrypt their messages. However, all platforms and content hosted in Iran are subject to arbitrary requests by various authorities to provide more information on their users. Local equivalents of international platforms do not guarantee an adequate level of protection for users, which may explain users' hesitancy to adopt domestic platforms. An August 2015 survey of 904 Iranian internet users found that they felt less comfortable using Iranian social networks.[78]

In a troubling development, the Supreme Council on Cyberspace announced in May 2016 that all foreign messaging apps must move all data on Iranian users to servers located within the country.[79] The order seemed targeted at Telegram, used by some 20 million Iranians, which has been under increased pressure by the authorities over the past year. Storing data on local servers would make it easier for the authorities to compel the company to hand over data on government critics and censor unfavorable views.[80]

73 "07.04.2016 - Two journalists freed," in "Press freedom violations recounted in real time January 2016," Reporters Without Borders, https://rsf.org/en/news/press-freedom-violations-recounted-real-time-january-2016.

74 "Facebook Activist Sentenced to Seven Years in Prison for 'Insulting the Prophet'," International Campaign or Human Rights in Iran, October 1, 2015, https://www.iranhumanrights.org/2015/10/soheil-arabi-4/.

75 "A New Round of Intimidation, Arrests, and Prosecution of Social Media Users in Iran," International Campaign for Human Rights in Iran, June 14, 2015, https://www.iranhumanrights.org/2015/06/intimidation-arrests-social-media-users/.

76 "Cyber army exercises held," [Farsi] Itmen, http://www.itmen.ir/index.aspx?pid=99&articleid=82120.

77 "Cyber Police launches gaming unit," [Farsi] Mehr News, http://bit.ly/2dXpvAe.

78 Small Media, *Iranian Internet Infrastructure and Policy Report: July 2015,* https://smallmedia.org.uk/media/articles/files_IIIP_Aug15.pdf.

79 "Iran orders social media sites to store data inside country," Reuters, May 29, 2016, http://www.reuters.com/article/internet-iran-idusl8n18q0in.

80 Adario Strange, "Iran's new data policy could mean end of local access to Telegram app," Mashable, May 31, 2016, http://mashable.com/2016/05/31/iran-telegram-app/#k3nf4Sy43mqY.

The legal status of encryption in Iran is somewhat murky. Chapter 2, Article 10 of the Computer Crimes Law prohibits "concealing data, changing passwords, and/or encoding data that could deny access of authorized individuals to data, computer and telecommunication systems."[81] This could be understood to prohibit encryption, but enforcement is not common. Nonetheless, the Iranian authorities have periodically blocked encrypted traffi from entering the country through international gateways, particularly during contentious moments such as elections.[82]

Meanwhile, the Iranian government has continued its cat-and-mouse game against the use of circumvention tools, the legal status of which is also relatively opaque. The *use* of VPNs does not appear to be criminalized, unlike the selling or promoting of VPN use. For example, several individuals were arrested in late 2015 for promoting, selling, or training individuals to use circumvention tools. [83]

Intimidation and Violence

Extralegal intimidation and violence by state authorities is prevalent in Iran. In 2012, blogger Sattar Beheshti was killed while in prison. More recently, groups such as the IRGC have pressured or coerced detained activists into giving up login details to their social media accounts, which the authorities have then used for surveillance and phishing attacks. For example, after the arrest of former BBC Persian journalist Bahman Daroshafaei, Iranian activists living in the diaspora reported receiving suspicious messages from his Telegram account.[84] This appears to be part of a broader pattern, as a number of activists have reported phishing attempts that appear to have been sponsored by the Iranian government.[85]

Technical Attacks

Over the past year, Iran has launched a series of attacks including phishing emails aimed at internet freedom activists[86] and cyberattacks targeting US government officials In the latter case, the *New York Times* noted that "Iranian hackers identifie individual State Department official who focus on Iran and the Middle East, and broke into their email and social media accounts, according to diplomatic and law enforcement official familiar with the investigation." In some cases, the victims were only made aware of the state-sponsored attacks after Facebook had alerted them.[87] In August 2015, the Citizen Lab uncovered a sophisticated phishing campaign aimed at Iranian activists in the diaspora, which sought to circumvent the protections offered by two-step authentication in Gmail.[88]

81 https://www.article19.org/data/files/medialibra y/2921/12-01-30-FINAL-iran-WEB%5B4%5D.pdf

82 "April 2016," *Filterwatch*, Small Media, https://smallmedia.org.uk/media/articles/files/IIIP_APRIL16.pd , pg. 7-9.

83 See "Individual arrested for "teaching circumvention," [Farsi] Radio Zamaneh, http://www.radiozamaneh.com/251407 and "Administrators arrested for sale of proxy sites in Ahvaz," Khoorna, http://bit.ly/2fgn8ue.

84 Lorenzo Franceschi-Bicchierai, "Iran Appears to Have Taken Over an Arrested Journalist's Telegram Account," *Motherboard,* February 5, 2016, http://motherboard.vice.com/read/iran-telegram-account-bbc-journalist.

85 Lorenzo Franceschi-Bicchierai, "The Iranian Hacking Campaign to Break into Activists' Gmail Accounts," *Motherboard,* August 27, 2015, http://motherboard.vice.com/read/inside-the-iranian-hackers-campaign-to-break-into-activists-gmail-accounts.

86 Lorenzo Franceschi-Bicchierai, "The Iranian Hacking Campaign to Break into Activists' Gmail Accounts," *Motherboard,* August 27, 2015, http://motherboard.vice.com/read/inside-the-iranian-hackers-campaign-to-break-into-activists-gmail-accounts.

87 David E. Sanger and Nicole Perlroth, "Iranian Hackers Attack State Dept. via Social Media Accounts," *The New York Times,* November 24, 2015, http://www.nytimes.com/2015/11/25/world/middleeast/iran-hackers-cyberespionage-state-department-social-media.html?_r=0.

88 John Scott-Railton and Katie Kleemola, "London Calling: Two-Factor Authentication Phishing from Iran," Citizen Lab, August 27, 2015, https://citizenlab.org/2015/08/iran_two_factor_phishing/.

In addition, a 2015 report by Cylance uncovered an Iranian state-sponsored hacking campaign targeting sensitive material from government agencies and critical infrastructure companies in a number of countries, including England, France, Germany, and the United States.[89] Moreover, a report by Checkpoint found evidence that an Iranian cyber espionage group known as "Rocket Kitten" has been engaged in a series of spear-phishing and targeted-malware attacks against Iranian dissidents.[90]

89 *Operation Cleaver,* Cylance, accessed October 2016, http://cdn2.hubspot.net/hubfs/270968/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf.

90 *Rocket Kitten: A Campaign with 9 Lives,* Check Point Software Technologies, November 2015, https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf .

Freedom House

Italy

	2015	2016
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	4	4
Limits on Content (0-35)	6	6
Violations of User Rights (0-40)	13	15
TOTAL* (0-100)	**23**	**25**

* 0=most free, 100=least free

Population:	**60.8 million**
Internet Penetration 2015 (ITU):	**66 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2016 Status:	**Partly Free**

Key Developments: June 2015 – May 2016

- Online journalists and bloggers continued to face legal threats and intimidation, notably for reporting on sensitive stories such as organized crime in some parts of the country (See **Prosecutions and Detentions for Online Activities** and **Violence and Intimidation**).
- In July 2015, leaks surrounding Italian company Hacking Team revealed extensive cooperation with authoritarian regimes. After considerable media scrutiny, the Italian government suspended its global license to export its software outside of the European Union in April 2016 (See **Technical Attacks**).
- Italy was the fi st European country to produce a "Declaration of Internet Rights" in July 2015, in a bid to increase awareness of digital rights and inspire legislative actions. The nonbinding declaration includes provisions that promote net neutrality and establish internet access as a fundamental right (See **Legal Environment**).

Introduction

Italy's internet environment declined slightly during this period, as online writers have occasionally faced legal intimidation and other threats for covering sensitive stories.

For a country with an advanced economy, Italy's internet penetration lags behind that of many other European countries at around 65 percent of the population. Italian authorities do not generally engage in political censorship of online speech, and, as in previous years, no bloggers or social media users were imprisoned during the coverage period. However, defamation remains a criminal offense in Italy, and civil libel suits continue to threaten online writers.

Marking its "Internet day" on April 30, Italy celebrated the thirtieth anniversary of its first internet connection in 1986.[1] Italy's first computer network emerged in 1980, when a group of nuclear physicists connected all of the country's nuclear research institutes. Access to the internet was available to private users after 1995, and the number of internet service providers (ISPs) soared within a short period of time. Some obstacles to access remain, however, including a lack of familiarity with computers and the English language, as well as the dominance of commercial television, and the diversion of consumers' telecommunications spending to mobile telephony. Showcasing efforts to reduce the digital divide and promote the current government's optimism for the digital agenda, the premier recently appointed Amazon vice-president Diego Piacentini as "commissioner for digitalization."[2]

After a year of consultations led by a parliamentary commission, Italy was the first European country to present a crowdsourced "Declaration of Internet Rights" in July 2015. The nonbinding document includes provisions that promote net neutrality and establishes internet access as a fundamental right. While generally seen as a positive development, the text has also raised some criticism for falling short on certain issues such as anonymity, encryption, and data retention.

Several other legislative discussions have taken place over the past year. Presented to parliament in April 2015, Prime Minister Renzi revived the idea of a previously shelved tax on e-commerce, the so-called "Google Tax." If approved, the proposal would impose a 25 percent tax levy on multinational companies selling digital services and operating longer than six months in Italy with revenues of over five million euros.[3] Meanwhile, parliament discussed a bill related to net neutrality, which would require ISPs to treat all internet traffic equally, regardless of its source. However, other aspects of the text sparked criticism for potentially allowing "loopholes" in the prioritization of traffic.[4]

Obstacles to Access

Since the 1990s, the Italian government has supported the internet as a catalyst for economic growth, increased tourism, and more efficient government operations. This attitude continued to prevail in 2016, though aspirations for a fully connected Italy remained unfulfilled.

1 Luca Annunziata, "30 aprile 2016, 30 anni di Internet in Italia" [April 30, 2016, 30 years of Internet in Italy], *Punto Informatico,* April 29, 2016, http://bit.ly/1SBn7xb.

2 Claudio Tamburrino, "Piacentini, un asso per il digitale in Italia" [Piacentini, an ace for the digital in Italy], *Punto Informatico,* February 11, 2016, http://bit.ly/2f56oqs.

3 Federico Guerrini, Italy's prime minister flaunts the idea of a 'digital tax' to get web giants to pay up," ZDNet, September 17, 2015, http://zd.net/1LAJtao; and Giuditta Mosca, "Digital tax, ecco cos'è e come funzionerà" [Digital tax, what it is and how it will work], *Wired*, September 16 2015, http://bit.ly/2eDtIaz.

4 EDRi, "Loopholes creeping into the Italian proposal on net neutrality," March 23, 2016, http://bit.ly/2dkGxWo.

Availability and Ease of Access

According to the International Telecommunication Union (ITU), Italy had an internet penetration rate of 65.6 percent in 2015, an increase from 62 percent in 2014.[5] The Italian National Institute of Statistics (ISTAT) reported slightly lower internet penetration figu es than the ITU, at 60.2 percent in 2015 (compared to 57.5 percent in 2014). Of these, nearly 40 percent went online every day, and 16.8 percent once a week. The internet is particularly popular among Italian youth, with over 91 percent of people between 15 and 24 surfing the eb.[6]

Italians prefer to access fi ed-line internet from home, with the workplace being the second most common access point, followed by schools and universities. Some 70 percent of men use the internet, compared to 62 percent of women.[7] Cost is not a significant arrier to access. The price for a broadband connection may range from €20 to €40 (US$26-52) per month, compared to average monthly per capita income of around US$2,700.[8]

While Italy's internet penetration rate is higher than the global average, it is much lower than the overall rate in Western Europe and lags behind in many ICT indicators in Europe.[9] Several factors have impacted Italy's relatively low penetration rate, including infrastructural limitations, overall household internet penetration, and unfamiliarity with the internet among older generations. In addition, Italy's devastating financial crisis 2008 still everberated in 2015-2016, impacting consumer disposable incomes. Recent figu es pointed to a slight decrease in home internet connections via desktop computers, compared to the constant growth of mobile devices with internet access.[10] In general, mobile phone use is much more widespread than internet access, with the penetration rate reaching 151 percent in 2015.[11] The majority of subscriptions are still prepaid, but flat tariffs a e on the rise.[12]

ADSL (fi ed) broadband connections (which reach up to 2 Mbps when advertised as "basic service") are available in about 98 percent of Italy's territory. However, fast broadband (more than 30 Mbps) is only slated to reach 50 percent of the territory in 2016-17. Italy has one of lowest coverage rates of high speed broadband in the EU,[13] covering only 21 percent of households compared to a European average of 62 percent.[14] In 2015, the average connection speed was 7.4 Mbps, with only 5.2 percent of Italians enjoying speeds over 15 Mbps.[15] There is no plan by telecom companies to achieve ultra-fast broadband (over 100 Mbps) anytime soon.

5 International Telecommunication Union (ITU), "Percentage of individuals using the Internet, 2000-2015," accessed October 7, 2016, http://bit.ly/1cblxxY.

6 Istituto Nazionale di Statistica (ISTAT), "Citizens, enterprises and the ICTs," December 22, 2015, accessed October 7, 2016, http://bit.ly/2dyjIUw.

7 ITU, "Gender ICT Statistics 2015," accessed October 7, 2016, http://bit.ly/1cblxxY.

8 For a recent comparison (April 2016) see for instance, SOS Tariffe, "Connessioni a Banda Larga," [Connections to broadband], http://bit.ly/1Ou3hCV.

9 ITU, "ICT Facts and Figures: the world in 2015," http://bit.ly/1FOoa6p; See also: The Digital Economy & Society Index (DESI), 2016, http://bit.ly/1UPeUWV.

10 Audiweb, "Sintesi dei dati sulla diffusione di internet in Italia" [Summary of data on the spread of the Internet in Italy], December 2015, accessed October 7, 2016, http://bit.ly/2eBI51U.

11 ITU, "Mobile-cellular subscriptions 2000-2015," accessed October 7, 2016, http://bit.ly/1eKDWOQ.

12 Autoritá Per Le Garanzie Nelle Comunicazioni (AGCOM), *Communication Market Monitoring System,* January 2016, http://bit.ly/2dQ9N8b.

13 The EU Digital Agenda calls for 100 percent of the territory covered with 30Mbps and at least 50 percent with ultrafast (over 100Mbps) by 2020;

14 Telecom Italia Mobile, *Italia Connessa 2014: Agende Digitali Regionali*, 47-48.

15 Akamai, State of the Internet, Q4 2015 Report, http://akamai.me/1UthiDG.

The ambitious infrastructural plan, "Growth 2.0", was announced in 2012 to close Italy's digital divide between those areas that are served by high-speed connections and those that are not, but targets were repeatedly delayed through 2015.[16] The same plan also launched the "Digital Agenda" initiative (based on the EU Agenda 2020), intended to expand broadband access and e-government functions (including "digital identity," public e-services, "intelligent communities," and so on).[17] In a similar attempt to showcase progress in Italy's digital agenda, the government in February 2016 approved a decree to cut costs for laying cables and established the Networks Register for Infrastructures (SINFI).[18] With this stop-and-go approach, however, it remains unclear whether Italy will fulfill the EU goal.

Restrictions on Connectivity

The government does not impose restrictions on ICT connectivity and access to social media and communication platforms. Telecom Italia, the former state telecom monopoly that owns the physical network, continues the process of "externalizing" the infrastructure since May 2013, as required by EU legislation to provide fair access to competitors (see ICT Market).[19]

ICT Market

Access to the internet for private users is offered by 13 different ISPs. Telecom Italia has the largest share of the market, followed by Vodafone, Fastweb, and Tiscali. Telecom Italia Mobile (TIM), Vodafone, Wind, and 3 Italia are the major carriers, and all of them operate third-generation (3G) networks. As elsewhere, sales of tablet computers have been on the rise among the younger generation since 2010 and are likely to keep growing in the coming years. The French media giant Vivendi has further raised its stake in Telecom Italia to just under 25 percent, the threshold for making a mandatory bid for Telecom Italia.[20]

One of the most noticeable changes in early 2016 was Italy's biggest power company ENEL's entrance into the market with its "Open Fiber" program, challenging Telecom Italia's own plans for high-speed broadband.[21] ENEL aims to install fiber optic cables o private homes via new broadband (30 Mbps) for 7.5 million households. Because of the physical proximity of electricity switches to houses and buildings, the company has a strong advantage.[22] Some 224 Italian cities would be connected via "fiber o the home" (FTTH) in the next three years, with a price tag of 2.5 billion Euros. Telecom giants such as Vodafone and Wind have already partnered with ENEL.[23] Some obstacles re-

16 Alessandro Longo, "Lombardo (Infratel): 'Banda larga fra le pastoie della burocrazia'," *Corriere Digitale*, April 18, 2014, http://bit.ly/1VOtBGO.

17 Italian text at: D.L. 179/2012 in G.U. 46/2012, [in Italian] http://bit.ly/1jsm8AT; See also Agenzia per l'Italia Digitale, "Agend Digitale italiana," http://bit.ly/1PpZcP9. *Achieving the Objectives of the Digital Agenda for Europe (DAE) in Italy: Prospects and Challenges*. The six "strategic areas of the "Digital Agenda" include infrastructure and cyber security, e-commerce, e-government, e-learning (e-books, digital policy literacy and e-participation), research and innovation in ICT, and smart cities and communities

18 Legislative decree of February 15, 2016, n. 33, http://bit.ly/2cXO558.

19 Telecom Italia, "Telecom Italia: CDA approva il progetto di societarizzazione della rete di accesso," Press release, May 30, 2013, http://bit.ly/1PaTZf5.

20 "Vivendi ups Telecom Italia stake to just below bid threshold," *Reuters,* March 11, 2016, http://reut.rs/1V5H4gs.

21 Repubblica "Enel: piano da 2,5 miliardi per la fibra in 224 città" [Enel: 2.5 billion for fiber in 224 cities], *Repubblica,* March 23, 2016, http://bit.ly/1UEYIs6/.

22 The electricity grid reaches 32 million household customers, compared to the 21 millions of Telecom Italia fi ed line network.

23 "Enel, c'è l'accordo con Wind e Vodafone per la fibra, [Enel agreement with Wind and Vodafone for fiber], *Reppublica*, April 6, 2016, http://bit.ly/1PUedF1.

main, however: first, ENEL's network would have to be connected to the Telecom Italia infrastructure; and second, in those areas where this operation will not be profitable (some 20 percent of the territory), the state will have to bear the costs, provided it finds the necessary funds.

Regulatory Bodies

The main regulatory body for telecommunications is the Authority for Communications (AGCOM), an independent agency that is accountable to the parliament. Its responsibilities include providing access to networks, protecting intellectual property rights, regulating advertisements, and overseeing public broadcasting. The parliament's majority party appoints AGCOM's president. In recent years, AGCOM has paid particular attention to digital copyright issues. In December 2015, Italy's Constitutional Court dismissed an appeal that challenged the constitutionality of AGCOM's online copyright enforcement regulation issued in 2014, which empowers the regulatory authority to order internet or hosting providers to block websites or remove allegedly infringing content (See Blocking and Filtering and Content Removal).[24]

Another important player governing the ICT sector is the Italian Data Protection Authority (DPA). Set up in 1997, the DPA is tasked with supervising compliance with data protection laws by both governmental and nongovernmental entities. It also has the authority to ban or block "processing operations that are liable to cause serious harm to individuals."[25] It is generally viewed as professional and fair in carrying out its duties.

Limits on Content

The Italian authorities do not engage in significant blocking or filtering of internet content, although measures to block illegal materials without a court order have worried digital rights activists.

Blocking and Filtering

Italy does not block or filter content of a political, social, or religious nature, while Facebook, Twitter, YouTube, and international blog-hosting sites are all freely available. However, certain websites related to gambling, copyright infringement, and terrorism are subject to blocking or removals (see Content Removal). The 2014 antiterrorism law voted in the Senate on April 15, 2015 also allows the public prosecutor to order the blocking or removal of terrorist websites. Similar to the system used to block child pornography sites, the Interior Ministry compiles a blacklist of terrorist websites for ISPs to block.[26]

Since 2006, online gambling has been permitted only via state-licensed websites, and ISPs are required to block access to international or unlicensed gambling sites identified on a blacklist compiled by the Autonomous Administration of State Monopolies (AAMS). The list of banned sites is available on the AAMS website and updated regularly.[27] A similar blacklist system is in place for

24 EDRi, "Italian Constitutional Court avoids decision on blocking," January 26, 2016, http://bit.ly/2d03zR7.

25 The Italian Data Protection, "The Italian Data Protection Authority: Who We Are," November 17, 2009, http://bit.ly/1Lr0vvy.

26 Sghirinzetti, "Italy: Anti-terrorism decree to strengthen government surveillance," EDRi, April 22, 2015, http://bit.ly/1RCR0KR.

27 The blacklist is available (in Italian) at http://www.aams.gov.it/site.php?id=2484.

websites containing child pornography. A law passed in February 2006 (Law No. 6) called for the establishment of a National Center for the Fight against Child Pornography on the Internet within the Postal and Communications Police Service. Based on its own research and on complaints from citizens, the center maintains a list of sites deemed inappropriate and forwards it to ISPs for blocking.[28] As with the AAMS list, the child pornography blacklist is publicly available, though some child advocates have raised concerns that this encourages visits to the sites by users with circumvention tools. ISPs also offer subscribers "family internet" packages that block access to adult pornography and sites with violent content, in exchange for a small premium.

Decisions related to the blocking of websites for copyright violations are implemented by the *Guardia di Finanza* (Finance Guard or GdF), a law enforcement agency that handles issues of cybercrime, fraud, and trafficking [29] A 1941 law explicitly amended by the Berlusconi government in 2005 to include online communication has led to a few cases in which websites containing news were blocked for copyright.[30]

A controversial resolution on online copyright enforcement enacted in March 2014 enables AGCOM to issue administrative blocking orders to ISPs for specific ebsites that infringe on copyright, even those that only contain links for downloading copyright protected content. The regulation also gives AGCOM the power remove content upon review by an internal panel but without prior judicial approval if a copyright violation is detected.[31] In September 2014, consumer organizations and ISP associations challenged the regulation, although a definiti e decision was still pending.[32]

Content Removal

The Italian authorities sometimes request the removal of specific con ent, though the amount is limited. According to Google's latest Transparency Report, the government sent 125 content removal requests between July to December 2015, including 59 percent of them for "defamatory" content, 22 percent for privacy and security reasons, and 10 percent for bullying and harassment.[33]

Foreshadowing the May 2014 Court of Justice of the European Union (CJEU) ruling in favor of the so-called "the right to be forgotten," in April 2012 the Italian Supreme Court imposed an obligation on publishers to update their online archives to ensure that outdated facts do not inadvertently damage a person's reputation. But the court also pointed out that online news outlets cannot be held liable for stories deemed damaging to a person's reputation if events recounted in the article are true, even if they are incomplete or outdated.

28 Polizia di Stato,"Centro nazionale per il contrasto alla pedopornografia sulla ete," [National Center for the Fight against Child Pornography on the Internet] May 10, 2010, http://bit.ly/1LFdZQ4.

29 The Italian Police, acting on order by a judge in Rome, who ruled in favor of a film distribution com any (Sunshine Pictures), ordered 27 Italian and international ISPs to proceed with a DNS blockade to prevent Italian users to see a French movie "Un Monstre à Paris" distributed by the company. Mauro Vecchio, "Italia, maxisequestro dello sharing in corso," *Punto Informatico*, April 15, 2013, http://bit.ly/1L85TCA.

30 Altalex, "L. 633/1941 in G.U. July 16, 1941, http://bit.ly/1Lh2qPS; and in particular it is art. 171/a/bis, amended by the D.L. 7/2005 in G.U. April 1, 2005, http://www.altalex.com/index.php?idnot=5918.

31 AGCOM, "Regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica," December 12, 2013, http://bit.ly/1WXMfys; See also: European Parliament, "Subject: Internet censorship in Italy—via administrative procedure," July 13, 2011, February 2, 2013, http://bit.ly/1MsIZrQ.

32 : Italian Constitutional Court avoids decision on blocking," EDRi, January 26, 2016, http://bit.ly/2d03zR7.

33 Google, "Removal Request by Country," *Transparency Report,* July-December 2015, accessed October 7, 2016, http://bit.ly/2dYvB1P.

Since the CJEU's 2014 "right to be forgotten" ruling, Italian courts have ruled in favor of the new right. On December 3, 2015, for example, a Civil Court of Rome upheld the CJEU's reasoning on the "right to be forgotten" but rejected the plaintiff's request, in a case that sought to balance such a right with the right to information in the public interest.[34] Separately in June 2016, the Supreme Court upheld a 2013 court decision in favor of the removal of an inconvenient news article from a website's archives after two years, deeming that the time elapsed between the publication date and the request for removal "sufficed to satisfy the public interest as far as its right to be informed was concerned."[35]

Because of Italy's civil-law system, some judges may occasionally still issue rulings imposing responsibilities on intermediaries to regulate user-generated content, though judges have repeatedly affirmed that intermediaries should not be liable for the content posted by users. Many in the Italian legal community now believe that, based on existing jurisprudence and thanks also to the provisions laid out in the EU's e-Commerce Directive,[36] service providers should not be required to censor search results. Likewise, at the end of 2011, Italy's Supreme Court declared that editors of online magazines are not responsible for defamatory comments posted by readers (thus taking into account the difference between the printed and electronic press). Attempts at introducing bills that would require websites to engage in pre-publication censorship have mostly stalled.

Media, Diversity, and Content Manipulation

Even in the absence of legal requirements, content hosts may exercise some informal self-censorship regarding content that could prove controversial or create friction with powerful entities or individuals. Online writers also exercise caution to avoid libel suits by public officials, whose litigation—even when unsuccessful—often takes a significant financial toll on defendants. Individuals writing about the activities of organized crime in some parts of the country may be especially at risk of reprisals. The Italian government does not proactively manipulate news websites.

Blogging is very popular in Italy, though television remains a leading medium for obtaining news. Most policymakers, popular journalists, and figures in the entertainment industry have their own blogs, as do many ordinary citizens. Social-networking sites, especially Facebook and Twitter, have emerged as crucial tools for organizing protests and other mass gatherings, such as concerts, parties, or political rallies, although, at times, some content may be aggressive. It is now "mandatory" for all parties to be adept at communicating via Facebook, Twitter, and other social media.

Some restrictions on internet content uncommon in other Western European countries remain in place in Italy. Drawing on a 1948 law against the "clandestine press," a regulation issued in 2001 holds that anyone providing a news service, including on the internet, must be a "chartered" journalist within the Communication Workers' Registry (ROC) and hold membership in the national journalists' association.[37] With the exception of one case from late 2000s, these rules have generally

34 Nctm, "Right to be forgotten, right to reputation and privacy: comment to the decision no. 23771/2015 of the civil court of Rome," April 2016, http://bit.ly/2dQZn8c.

35 The Supreme Court's ruling occurred outside the period of coverage of this report. See: Guido Scorza, "A ruling by the Italian Supreme Court: News do "expire." Online archives would need to be deleted," *L'Espresso*, July 1, 2016, http://bit.ly/29aeJ5c; See also: Athalie Matthews, "How Italian courts used the right to be forgotten to put an expiry date on news," *The Guardian,* September 20, 2016, http://bit.ly/2cPSINq.

36 European Commission, "E-Commerce Directive," 2000/31/EC, http://bit.ly/1iuT1su.

37 Diritto Tecnologia Informazione, Legge March 7, 2001, n. 62, "Nuove norme sull'editoria e sui prodotti editoriali," [New Rules on Publishing and Publishing Products] accessed August 21, 2012, http://www.interlex.it/testi/l01_62.htm.

not been applied to bloggers and, in practice, millions of blogs are published in Italy without repercussions. Nonetheless, many people who create websites on a range of issues (including scholarly research) still continue to collaborate with registered journalists to protect themselves from potential legal action.

Digital Activism

Starting with the 2013 general elections, social media and the web proved to be a major innovation in Italian politics. Online tools were central, not only as a communication medium, but also to measure political sympathies by measuring "likes," hashtags, and tweets for the many political players.[38] The Five Star Movement, a political party led by former comedian Beppe Grillo, based their political campaign almost exclusively on the internet and declined to take part in political talk-shows or television interviews. Beppe Grillo's blog and social media remain central platforms to convey the Movement's political goals and programs.[39]

Civil society organizations have also actively promoted and contributed to open data and freedom of information initiatives. Since 2014, a public campaign called "FOIA4Italy" has called for the adoption of a freedom of information act. After a fi st version was circulated in January 2016, an improved version was finally app oved by the Council of Ministers in May 2016.[40]

Violations of User Rights

Violations against users' rights are uncommon in Italy, although cases of legal intimidation and threats against online writers are occasionally reported. Criminal defamation laws remain a grave threat to online journalists and social media users, particularly in the ambiguous form they have been applied to the online sphere. A new antiterrorism law passed in April 2015 extended the period ISPs must keep users' metadata from 12 to 24 months, despite a ruling from Europe's high court striking down such requirements as an affront to human rights. On the other hand, Italy was the first European country to produce a "Declaration of Internet Rights" in July 2015, in a bid to increase awareness of digital rights and inspire legislative actions.

Legal Environment

As a signatory to the European Convention on Human Rights and other relevant international treaties, freedoms of speech and the press, as well as the confidentiality f correspondence, are constitutionally guaranteed in Italy.[41] Yet, given the country's civil law system, inconsistent judicial interpretations are not unusual. This has created some uncertainty when judges issue conflicting decisions on similar cases related to internet freedom, such as intermediary liability. For this reason, online free

38 Luca Annunziata, "Chi vince le elezioni su Internet?" *Punto Informatico*, February 8, 2013, http://bit.ly/1L887BP.

39 See http://www.beppegrillo.it

40 FOIA4Italy, "L'Italia ha un Freedom of Information Act," [Italy has a Freedom of Information Act], May 19, 2016, http://bit.ly/2d19ipS; See also: "Ecco il testo del decreto Foia, la trasparenza della PA parte da dicembre," *Reppublica,* May 19, 2016, http://bit.ly/2dTLOsZ.

41 An English copy of the constitution is available at, Constitution of the Italian Republic, http://bit.ly/1hARFPS; See especially art.15 and 21 Cost.

expression advocates have focused their efforts on proposing legal amendments to improve protections and prevent censorship rather than engaging in public interest litigation.[42]

Several laws present a threat to internet freedom in the country. Italy passed a new antiterrorism law in April 2015 that broadened language in the criminal code on terrorist recruitment as well as the endorsement or incitement of terrorism to include their action via online channels.[43] Critics worry that the law will be applied broadly and may sanction legitimate instances of free expression that fall within international norms for protected speech. On a positive note, the government withdrew provisions from the bill that would have authorized law enforcement agencies to remotely break into private computers. Prime Minister Renzi noted that the delicate issue needed further discussion.[44]

Defamation is a criminal offense in Italy: according to the criminal code, "aggravated defamation" is punishable by prison terms ranging from six months to three years and a minimum fine f EUR 516 (US$580). In cases of libel through the press, television, or other public means, there is no prescribed maximum fine [45] Though these provisions are rarely applied, civil libel suits against journalists, including by public officials and politicians, a e a common occurrence, and the financial bu den of lengthy legal proceedings may have chilling effects on journalists and their editors.

Although nonbinding, Italy was the fi st European country to adopt a "Declaration of Internet Rights" in July 2015.[46] The declaration includes provisions that promote net neutrality and establish internet access as a fundamental right. While generally seen as a positive development, the text has also raised some criticism for falling short on certain issues such as anonymity, encryption and data retention.[47]

Prosecutions and Detentions for Online Activities

Although no online activists have been detained or prosecuted by law enforcement agencies for disseminating or accessing information on the internet, legal threats against online journalists and bloggers were documented during the coverage period. According to the non-profit o ganization Ossigeno per l'Informazione, which tracks threats to journalists in Italy, 22 lawsuits with "clear intent of intimidation" were reported in June 2015 alone, many of them targeted against reporters of online news outlets.[48] It is likely that other cases are not publicly reported. Concerns also remained over the enforcement of criminal libel on platforms such as Facebook.[49]

In one case, journalist Antonio Brindisi was sued by residents of the island Gorgona because they felt

42 Andrea Monti (lawyer specialized on Internet freedom and activist), in a conversation with author, February 20, 2012.

43 Sghirinzetti, "Italy: Anti-terrorism decree to strengthen government surveillance."

44 "Tolto dal decreto antiterrorismo l'emendamento sui computer," *Internazionale*, March 26, 2015, http://bit.ly/1Lr1CeP.

45 Organization for Security and Cooperation in Europe Representative on Freedom of the Media, *Libel and Insult Laws: A matrix on where we stand and what we would like to achieve,* (Vienna: OSCE, 2005), 79, http://www.osce.org/fom/41958.

46 "Declaration of Internet Rights," http://bit.ly/2d0Sr6T.

47 Oreste Pollicino and Marco Bassini, "An Internet Bill of Rights? Pros and Cons of the Italian Way," LSE Media Policy Project Blog, August 5, 2015, http://blogs.lse.ac.uk/mediapolicyproject/2015/08/05/an-internet-bill-of-rights-pros-and-cons-of-the-italian-way/; See also: "Massimo Russo, "Ecco la bozza di Internet bill of rights, ora tocca ai cittadini migliorarla," *Wired*, October 13, 2014, http://bit.ly/1v6TKGU.

48 Ossigeno per l'Informazione, "The most dangerous news of June 2015 reported by Ossigeno," July 8, 2015, http://bit.ly/1KSPzG5; For a list of incidents reported by Ossigeno per l'Informazione to date, see: http://bit.ly/1j0mLC1.

49 See for example: Adriana Apicella "Diffamazione a mezzo stampa, è reato anche su Facebook," [Libel, also a crime on Facebook], Justicetv.it, January 17, 2013, http://bit.ly/2dYQ5rh; Mauro Vecchio,"Diffamazione, stampa e social pari sono?" *Punto Informatico,* January 15, 2013, http://bit.ly/1L88ZGK; "Cassazione: è diffamazione parlar male su Facebook anche senza fare nomi," *La Repubblica*, April 16, 2014, http://bit.ly/1PaZqKX.

offended by satirical remarks on the website "www.ilgorgon.eu." According to Ossigeno per l'Informazione, Brindisi was convicted of defamation by a court in Livorno in October 2015 and sentenced to pay a fine f 1,500 Euros, even though his blog had been taken down since 2012.[50]

Surveillance, Privacy, and Anonymity

Widespread technical surveillance is not a concern in Italy, and monitoring of personal communications is permissible only if a judicial warrant has been issued. Wiretapping is generally restricted to cases involving ongoing legal proceedings, except for terrorism investigations. In such instances, "pre-emptive wiretapping" may occur even if no formal prosecutorial investigation has been initiated. More lenient procedures are also in place for Mafia- elated investigations.[51] The country's authorities are widely perceived to be engaged in regular wiretapping,[52] and the news media regularly publicize wiretap information that is leaked to them.

In March 2008, Parliament approved a law (No. 48 of 2008) that ratified the Council f Europe's Convention on Cybercrime, which established how long internet-related communication data should be retained.[53] This matter was further refined with the inclusion in the Italian legislati e system of the 2006 EU Data Retention Directive.[54] Although the Court of Justice of the European Union struck down the directive in 2014, Italy passed an antiterrorism law in April 2015 that extended the period ISPs must keep users' traffic ecords (metadata), as opposed to the content of communications—from 12 to 24 months.[55] Providers must retain information such as broadband internet data, internet telephony, internet use via mobile phone, and email activity. The records can only be disclosed in response to a request from a public prosecutor (a judge) or a defendant's lawyer, and, like their counterparts elsewhere in Europe, Italy's law enforcement agencies may ask ISPs to make such information readily available so that they can respond to the needs of criminal investigations. Given the technical burden of this directive, most ISPs now use a third-party service that offers the necessary security guarantees for encryption and data storage.

As Italy moves towards greater e-governance, some concerns have been raised over the protection of user data in the hands of public agencies, as well as the security of digital data and the risk of identity theft.[56] As part of the Italy's digital agenda, the Digital Italy Agency (AgID) recently introduced an eID system called Public System of Digital Identity (SPID).[57] Launched in March 2016, SPID creates a "unique" PIN number that allows users to log into different public administration web services, including social security, pension, and tax agencies and municipalities. Only three providers are authorized to grant this "digital identity": Infocert, Tim (mobile telecom), and Poste (PosteID).

50 Ossigeno per l'Informazione, "Blog obscured for 3 years, managers condemned only now," October 15, 2015, http://bit.ly/1LuVD8I.

51 Privacy International, "Italy: Privacy Profile" in *European Privacy and Human Rights 2010* (London: Privacy International, 2010).

52 Although it is difficult o determine the real number of people affected by wiretaps (estimates range from 25,000 to over 130,000), many individuals who are caught up in wiretaps have no incriminating connection to the main target of the eavesdropping. The current law stipulates that such peripheral communications cannot be transcribed and any recordings should be destroyed right away, though this is not always carried out in practice. Thus it may happen that some exchanges are recorded and leaked to the media. This is the problem that the proposed bill on electronic surveillance was meant to address.

53 For a useful timetable of the required retention periods, see Gloria Marcoccio, "Convention on cybercrime: novità per la conservazione dei dati," [Convention on Cybercrime: News on Data Retention] Diritto Tecnologia Informazione, April 10, 2008, http://www.interlex.it/675/marcoccio7.htm.

54 D.L. 109/2008.

55 Sghirinzetti, "Italy: Anti-terrorism decree to strengthen government surveillance."

56 M. Calamari "Lo SPID è nato morto?", Punto Informatico April 21, 2016 , http://bit.ly/2fQLhso.

57 http://www.spid.gov.it/press-kit/SPID_8marzo_Presentazione.pdf.

In the past, the national postal service Poste Italiane's certified elect onic mail (PEC) service was named as the public agency most damaging to individual privacy at the "Annual Big Brother Awards," an event hosted by civil society privacy activists, for its gross mishandling of private information kept by the government's Registro delle Opposizioni, a register of people who wish to keep their contact information hidden from advertising companies.[58] Nevertheless, it is now mandatory for all businesses to use the PEC service in their communications with the public administration to cut costs and reduce paperwork.

Intimidation and Violence

Cases of intimidation or physical violence in response to online activity are reported sporadically, although individuals who expose the activities of organized crime in some parts of the country may especially be at risk of reprisals. In August 2015, the parliamentary anti-mafia commit ee voiced concerns about the high number of "acts of hostility" against investigative journalists by organized crime groups, recording 2,060 such incidents between 2006 and 2014. This included "traditional methods" of intimidation such as burning of cars, verbal threats and even sending bullets through the mail, but also increasing legal threats.[59] It is likely that many other cases are not publicly reported.[60]

As recorded by Ossigeno per L'Informazione, online journalists and bloggers have not been spared from abuse, with a number of threats or attacks reported during the coverage period. In a shocking case, anti-Mafia blogger and fo mer lawyer Mario Piccolino of Freevillage.it was shot dead in his office on May 29, 2015. Although immedia e speculation surrounding the cause of this attack pointed to Piccolino's anti-mafia writing [61] the murder appeared to be the result of a personal vendetta linked to a civil lawsuit.[62]

In July 2015, Mimmo Carrieri, an environmentalist who reports for the online outlet Viv@voce, was assaulted and stripped of his phone and camera while he was documenting camping abuses in a restricted area, even though he was already under police protection since 2012.[63] In September 2015, journalist Daniele Camilli of the online outlet *TusciaWeb* of Viterbo, who covers organized crime, received an anonymous letter that called for two organized crime families to use force against the journalist and his outlet.[64] In May 2016, Jacopo Norfo, journalist and chief editor of *Casteddu Online*, was insulted and intimidated on Facebook for publishing critical articles about hiring practices in Sardinia by the left-wing party SEL (Left, Ecology and Freedom).[65]

58 Cristina Sciannamblo "Big Brother Awards Italia: tutti i vincitori," *Punto Informatico*, June 6, 2011, http://bit.ly/1OubcQG.

59 Anti-Mafia arliamentary Committee, " Report on the State of Information and on the Condition of Journalists threatened by Organised Crime," August 5, 2015, http://bit.ly/2dAMvUN.

60 "How the Mafia Intimida es and Controls the Italian Media," *Vice,* March 15, 2016, http://bit.ly/21tm8zE.

61 "'Execution' of lawyer kills hope that residents can defeat Mafia" *The Independent*, June 6, 2015, http://ind.pn/2dyEFwa.

62 Ossigeno per L'Informazione, "Suspect murderer of Formia blogger arrested," June 23, 2015, http://bit.ly/1K84Cvm.

63 Ossigeno per l'Informazione, "Surrounded and threatened journalist calls for more protection," July 22, 2015, http://bit.ly/1Vvu8A1.

64 Ossigeno per L'Informazione, "Viterbo Anonymous Asks The Casamonicas to Punish Reporter and Website," September 16, 2015, http://bit.ly/2dQK7rN.

65 Ossigeno per L'Informazione, "Sardinia, Death Threats to Casteddu Online Reporter," June 3, 2016, http://bit.ly/1X3Dvcw.

Technical Attacks

The country's official cybe security strategy has been in place since December 2013.[66] The most common forms of technical attacks in Italy are the defacement or launching of denial-of-service (DoS) attacks against websites—mostly government-linked ones—as a form of political protest.[67] In February 2016, Ossigeno per l'Informazione reported that the news portal Immezcla.it, which covers immigration issues in the Mediterranean, was attacked and its contents were erased.[68] The online newspaper *La Voce di Venezia* also reported that its Facebook page was targeted by a hacking group called "Insane Army" on April 13 and 14, 2016.[69] Other cyberattacks—particularly against banks, government institutions, and business websites—remain a problem in Italy, as in other European Union member states. Nevertheless, Italy does not rank highly on the list of countries identified as points of origin for cybercrimes.[70]

In July 2015, the Milan-based private security fi m Hacking Team was hacked, leading to the release of several hundred gigabytes of emails and other data that was later posted to Wikileaks.[71] The company provides software applications to intelligence agencies around the world and had been criticized in the past for cooperating with nondemocratic regimes and lacking sufficient considerations of users' privacy.[72] In April 2016, however, the Italian government suspended its "global" authorization to export its software. While this would not affect countries within the European Union, the company would be required to seek approval from Italian authorities to request individual licenses for each country outside of the EU.[73] This decision came in the midst of growing scrutiny of surveillance software sales and followed the torture and death of the Italian PhD student Giulio Regeni in Egypt, which was also one of the countries on the list of Hacking Team customers.

66 Presidency of the Council of Ministers, *National Plan for Cyberspace Protection and ICT Security,*December 2013, http://bit.ly/1Lr3Gn4; and Presidency of the Council of Ministers, *National Strategic Framework for Cyberspace Security,* December 2013, http://bit.ly/1qVEWpW.

67 The Police and the judiciary are often targeted, see for example "Gli hacker colpiscono ancora:attaccato sito della polizia campana," *Corriere della Sera,* February 17, 2013, http://bit.ly/1L8atk1 .

68 Ossigeno per l'Informazione, "Reggio Calabria: hackers attack online newspaper and erase it," March 2, 2016, http://bit.ly/2dGXxra.

69 "Attacco hacker alla pagina Fb del sito "La voce di Venezia"" [Hacker attack to the Fb page of the website "Voice of Venice"], Nuova Venezia, April 15, 2016, http://bit.ly/2dCqxAJ.

70 An independent report by HostExploit shows Italy scoring quite well on a "badness" scale (France, Germany and the United Kingdom, all get a worse score). These results are graphically visible in here: Global Secuirty Map, "Italy," accessed 19 May 2015, http://globalsecuritymap.com/#it.

71 Wikileaks, "Hacking Team," https://wikileaks.org/hackingteam/emails/.

72 Alfonso Maruccia, "L'orgoglio ferito di Hacking Team," *Punto Informatico*, July 23, 2015, http://bit.ly/1LFkylL. See also the conclusions by CitizensLab here, "Tag Archives: Hacking Team," https://citizenlab.org/tag/hacking-team/; and by computer security expert Bruce Schneier here: Bruce Schneier, "Hacking Team Is Hacked," *Schneier on Seurity* (blog), July 6, 2015, http://bit.ly/1RD0iWY.

73 "Hacking Team Has Lost Its License to Export Spyware," April 6, 2016, Motherboard, http://bit.ly/1q9klUD.

Freedom House

Japan

	2015	2016
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	4	4
Limits on Content (0-35)	7	7
Violations of User Rights (0-40)	11	11
TOTAL* (0-100)	**22**	**22**

* 0=most free, 100=least free

Population:	**127 million**
Internet Penetration 2015 (ITU):	**93 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2016 Status:	**Free**

Key Developments: June 2015 – May 2016

- In December 2015, the Saitama District Court ordered Google to remove references to an individual's past arrest for child prostitution from public search results; the Tokyo High Court overturned the ruling in 2016 (see **Content Removal**).
- Abusive speech about foreign residents of Japan continued to circulate online, prompting the Osaka city government to pass Japan's fi st ordinance to combat hate speech in January 2016 (see **Media, Diversity, and Content Manipulation**).
- Millions were affected by cyberattacks exposing personal data in 2015 and 2016 (see **Technical Attacks**).

Introduction

Privacy concerns, data leaks, and cyberattacks were key issues for Japanese internet users during the coverage period, though internet freedom overall saw no change.

Japan's constitution protects all forms of speech and prohibits censorship, while the government, especially the Ministry of Internal Affairs and Communications, maintains a hands-off approach to online content, which is generally self-regulated by industry players. Internet penetration is over 90 percent. Despite strong access, however, some legislation disproportionately penalizes specific o - line activities.

As part of the Abe administration's strategy to boost national security, lawmakers passed the Act on the Protection of Specially Designated Secrets in 2013. The legislation, which criminalized both leaking and publishing broadly defined national sec ets regardless of intent or content, has repercussions for journalists, whistleblowers, and civil society watchdogs, particularly in the age of the internet. In a review of Japan's human rights practices in July 2014, the United Nations Human Rights Committee said the legislation laid out "a vague and broad definition f the matters that can be classified as sec et" and "high criminal penalties that could generate a chilling effect on the activities of journalists and human rights defenders."[1]

Security measures continued to be of particular concern for national and local government officials with the practical introduction of the "My Number" system of personal identification numbe s throughout the country in October 2015.[2] Amendments to the Act on the Protection of Personal Information were passed in the Diet in early September 2015,[3] in part to forestall fears of possible data leakages that were expected to heighten with the rollout of the system.[4] The amendments strengthened requirements for companies that process data to remove details that could be used to identify individuals when sharing personal information.

Obstacles to Access

In general, Japanese internet users experience few obstacles to access. Internet access remains high, and mobile phone companies are increasingly expanding their technological offerings. The availability of third-party SIM cards with mobile operators unlocking phones for a small fee, and the greater availability of SIM-free models of phones and tablets, have spurred increased competition in the mobile market.

1 United Nations International Covenant on Civil and Political Rights Human Rights Committee, "Concluding observations on the sixth periodic report of Japan," August 20, 2014, available at http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fJPN%2fCO%2f6&Lang=en.

2 "Gov't should give up use of 'My Number' system infringing on people's human rights," *Japan Press Weekly*, February 25, 2015, http://bit.ly/1jQN0eh; Ryo Asayama, "Japan's 'My Number' system offers IT boon, and risk," *Nikkei Asian Review*, March 17, 2015, http://s.nikkei.com/1Lorvrl.

3 "Revised personal information protection law enacted," *Mainichi Shimbun*, September 4, 2015.

4 "マイナンバー法案が審議入り　衆院本会議," [My Number Law proposal enters committee, Lower House plenary session] *Nikkei Asian Review,* April 23, 2015, http://s.nikkei.com/1L1MX8r; "マイナンバー法改正案が衆院可決　貯金口座にも適用,"[My Number Law amendments expected to pass in the Lower House, will be applied to savings accounts] ITmedia, May 21, 2015, http://bit.ly/1VH275Y ; "マイナンバー衆院通過　貯金口座にも適用　個人情報保護法改正案も," [My Number Law passes in the Lower House, to be applied to savings accounts, proposed amendments to Personal Privacy Law as well] *Sankei,* May 21, 2015, http://bit.ly/1c7UmFR.

Availability and Ease of Access

Internet penetration was at 93 percent in 2015, up from 89 in 2014.[5] Mobile phone penetration reached 125 percent in 2015, including personal handy-phone (PHS) handsets.[6] Official statistics report slightly over 155 million mobile phones (including PHS) in use in Japan in 2015, an increase of 4.9 percent over the previous year.[7] Access is high quality with competitive speeds averaging 15.2 Mbps in 2015.[8] Wi-Fi availability continued to increase in 2015 and 2016, including services provided by the private Wire and Wireless company, which offers free internet access in restaurants, coffee shops, and some train stations; registration requires an email address.[9]

Internet access costs most users around JPY 5,000 (US$50) per month.[10] According to the most recent government statistics, the average cost of internet access throughout Japan was JPY 6,505 (US$64) per month in 2014, 12 percent higher than the previous year.[11] The statistics show major disparities between regions, with connectivity costs in the heavily populated Kanto area nearly a third higher than the national average, and comparatively rural areas such as Hokkaido, Tohoku, Hokuriku, and Kyushu averaging close to a third lower.[12] Many providers bundle digital media subscriptions, including cable television, Voice over IP (VoIP), and email addresses, pushing costs higher. Spending on internet access is highest in the 40-49 age group, closely followed by the under-40 age group, with those over 70 years of age spending the least (although 24 percent more than in 2013).[13]

As these figu es suggest, access is well distributed across the population, though less common among the elderly. According to the latest available government Information Communications Statistics Database, internet penetration was 72 percent for children aged six to twelve in 2014, and over 95 percent in the age ranges of 13 to 49, compared to 21 percent for people over 80 years of age.[14] Mobile phone operators are expanding their market for handsets designed for children and the elderly, with easy-to-use, large-button phones.

Restrictions on Connectivity

There are few infrastructural limitations on internet access in Japan, though the vulnerability of Japan's communication network became apparent in 2011, when an earthquake and tsunami hit Japan's east coast, triggering a nuclear plant accident. Infrastructure was severely damaged, leaving

5 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

6 International Telecommunication Union, "Mobile-cellular Telephone Subscriptions, 2000-2015," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

7 Ministry of Internal Affairs and Communications, "Information and communications statistical database, basic data" [in Japanese], http://bit.ly/1ZgX2FO.

8 Akamai's *State of the Internet,* "Asia-Pacific Highlights (Q1, 2015)" June 24, 2015, https://www.stateoftheinternet.com/resources-connectivity-2015-q1-state-of-the-internet-report.html.

9 Starbucks, "at_STARBUCKS_Wi2," http://starbucks.wi2.co.jp/pc/index_en.html.

10 Informal Freedom House survey of providers' costs.

11 Statistics Japan, Katei shōhi jyōkyō chōsa nenpō (Heisei 26 nen) kekka-no gaikyō (Household Consumption Survey Annual Report 2014, Overview of Results) [in Japanese], http://www.stat.go.jp/data/joukyou/2014ar/gaikyou/index.htm.

12 Statistics Japan, Katei shōhi jyōkyō chōsa nenpō (Heisei 26 nen) kekka-no gaikyō (Household Consumption Survey Annual Report 2014, Overview of Results) [in Japanese], http://www.stat.go.jp/data/joukyou/2014ar/gaikyou/index.htm.

13 Statistics Japan, Katei shōhi jyōkyō chōsa nenpō (Heisei 26 nen) kekka-no gaikyō (Household Consumption Survey Annual Report 2014, Overview of Results) [in Japanese], http://www.stat.go.jp/data/joukyou/2014ar/gaikyou/index.htm.

14 Ministry of Internal Affairs and Communications, Information and Communications Statistics Database, *Heisei 26 nen chosa*, http://bit.ly/1mLIJEl.

many people without service for periods from a few days to one month and restricting relief efforts. Mobile phone usage dropped by almost half in the affected areas.[15]

Network congestion and server outages—the result of increasing smartphone traffic due in art to many applications sending automatic signals every minute—also frequently affect mobile use. KDDI, one of three major mobile carriers, has reported large scale disruptions in the past, particularly in 2012 and 2013. Fewer disturbances were reported during this year's coverage period.

Historically, Japan's internet connections were forged through cooperation among government agencies (including ministries and NTT, which was a government-owned monopoly until 1985), higher education institutions (mainly universities), and national research institutions. According to the Japan Network Information Center website, the fi st network operations (known as "N-1 Network," in operation from October 1974 to December 31, 1999) were a joint undertaking initially operated by the University of Tokyo, the University of Kyoto, and NTT that later expanded to link other national universities.[16] The network of connected institutions started to expand in the mid-1980s with the start of JUNET (Japan University Network), pioneered by Keio University professor Jun Murai. The fi st Japanese university to connect to an overseas university (the City University of New York) was the Tokyo University of Science in 1985.

Providers continue to diversify to meet consumers' needs by offering optical fiber se vices (mainly through NTT's backbone services to newer detached homes and condominiums), as well as mobile and ADSL services (the latter for older homes). In 2013, Nippon Telegraph and Telephone Corporation's (NTT) Docomo announced an expansion in LTE base stations to augment its Xi LTE and FOMA 3G services.[17] Providers such as Asahi-net offer WiMAX plans with mobile routers capable of accessing multiple networks throughout the country.[18]

ICT Market

Japan has three major mobile operators—au (KDDI), NTT's Docomo, and Softbank. All use the CDMA wireless network or a variant. NTT, formerly a state monopoly, was privatized in 1985 and reorganized in 1999 under a law promoting functional separation between the company's mobile, fi ed-line, and internet services.[19] Asymmetric regulation, which creates stricter rules for carriers with a higher market share, helped diversify the industry.[20] While the telecommunications market operates with hundreds of providers offering FTTH, DSL, CATV, FWA, and BWA services, the NTT group remains dominant in practice.[21] In 2015, NTT's Docomo annual report noted that the company held 43.6 percent of the Japanese market share, followed by au (KDDI) (28.5 percent), Softbank (24.7 per-

15 Izumi Aizu, "The Role of ICTs During the Disaster," *Global Information Society Watch Report 2011,* Association for Progressive Communications, 2011, http://bit.ly/1FZMXGU.

16 Japan Network Information Center, "The Internet Timeline," accessed September 1, 2015, https://www.nic.ad.jp/timeline/en/.

17 NTT DOCOMO, "DOCOMO Introduces Compact LTE Base Station – Downsized Equipment Will Facilitate Wider, Denser LTE Coverage," press release, June 20, 2013, http://bit.ly/1Oo6lyP.

18 AsahiNet, "Asahi Net WiMAX 2+," http://bit.ly/1N1Q6FQ.

19 Law Concerning Nippon Telegraph and Telephone Corporation, Etc., No. 85, December 25, 1984, as last amended by Law No. 87, July 26, 2005, http://bit.ly/1FZNyIG.

20 Toshiya Jitsuzumi, "An Analysis of Prerequisites for Japan's Approach to Network Neutrality," (paper, Proceedings of the Telecommunications Policy Research Conference, 2012) http://bit.ly/1dPQDcb.

21 Minoru Sugaya, "Regulation and Competition in the JP Broadband Market," (presentation, Pacific elecommunications Council, Tokyo, Japan, January 15, 2012) http://bit.ly/16U0HvB.

cent), and a fourth player, Y!mobile (3.2 percent).[22] Consolidation occurred in the mobile industry in the late 2015 fiscal ear, as Y!mobile, which was formed in August 2014 through a merger of Emobile (formerly a roaming mobile company) and Willcomm (a PHS carrier),[23] joined the Softbank group.[24]

No major foreign operators have successfully penetrated the telecommunications market independently; smartphone devices manufactured by Apple and Samsung are available to consumers through partnerships with the major mobile operators.

Increasing smartphone use has made the mobile market more competitive and resulted in improved pricing options: bundling mobile tablet plans with subsidies for second and third devices purchased by consumers; decreases in prices for data and family plans; and the introduction of benefits for long-term customers, such as such as those offered by Docomo to customers with 5- to 15-year histories of continuous service.

Third-party SIM card availability continued to increase during the coverage period. In 2014, the government announced plans to require cellphone carriers to unlock the SIM cards in mobile phones if requested by users, facilitating the use of third-party prepaid SIM cards.[25] In October 2014, the Ministry of Internal Affairs and Communications (MIC) issued new guidelines concerning SIM card unlocking.[26] Though the guidelines are still subject to criticism,[27] they helped address concerns that the cost of switching providers favored the dominant players and created a barrier for new entrants to the market. Besides benefitting apanese consumers,[28] the change is expected to serve the influx of tourists to Japan during the 2020 Tokyo Olympics.[29]

Regulatory Bodies

There is no independent regulatory commission in Japan, though observers believe that the industry has generally improved since the 2001 establishment of the Ministry of Internal Affairs and Communications (MIC), comprised of two former ministries (the Ministry of Home Affairs and the Ministry of Posts and Telecommunications) which were merged with the central government's Management and Coordination Agency. This "super ministry" regulates the telecommunications, internet, and broadcast sectors.[30] Nongovernmental, nonprofit o ganizations supported by the relevant companies in the sector have been formed to self-regulate the industry. These include television's Broadcasting Ethics and Program Improvement Organization, the Content Evaluation and Monitoring Association

22 NTT Docomo Inc., Annual Report 2015, p. 5. https://www.nttdocomo.co.jp/english/corporate/ir/library/annual/fy2014/index.html

23 "Ii mobairu to uirukomu ga "Y!mobile" ni – 8-gatsu ni burando o tōgō, sumaho 2 kishu nado shin tanmatsu o junji hatsubai," [E-Mobile and Willcomm merge their brands in August to become 'Y!mobile;' new handsets including two new smartphones to be launched successively] *ITmedia,* July 7, 2014, http://bit.ly/1Qb1Q9Q.

24 SoftBank Corp. "Notice of Merger," press release, January 23, 2015, http://bit.ly/1Qb21BY.

25 "Japanese cellular carriers to get ministry call to 'unlock' cellphones," *Asahi Shimbun*. June 29, 2014.

26 "New rule to OK unconditional switching of mobile carriers," *Japan Times*, October 1, 2014.

27 "Editorial: SIM lock removal requirement not enough for consumers," *Mainichi Daily News*, November 4, 2014.

28 "Phone users in Japan still paying for plenty of stuff they don't need," *Japan Times*, May 23, 2015.

29 "Narita airport to get SIM card vending machines," *Japan Times*, July 17, 2015.

30 Before 2001, regulation was managed by the now-defunct Ministry of Post and Telecommunications, and before that, the Diet.

for mobile platforms, and the internet's Content Safety Association, which manages blocking of child pornography online.[31]

Limits on Content

District courts ordered search engines to delink inaccurate or irrelevant material about specific individuals from public results, in a trend which could affect information in the public interest, although the Tokyo High Court overturned one such ruling on appeal. Media freedom observers reported increasing government pressure on traditional news outlets, and activists used digital tools to protest against laws which sought to redefine the role of Japan's Self-Defense Forces and reinterpret Article 9 of Japan's constitution, which embraces pacifism.

Blocking and Filtering

No direct political censorship has been documented in Japan. ISPs voluntarily fil er child pornography, and many offer parents the option to fil er other immoral content to protect young internet users.[32] Depictions of genitalia are pixelated to obscure them for internet users based on a common—though poorly-articulated—interpretation of Article 175 of the penal code, which governs obscenity.[33] Otherwise, individuals or police instruct ISPs to administratively delete contested or illegal content.

The threat of official con ent restrictions looms periodically during public debates about child safety, though carriers and content producers have successfully resisted intrusive regulation. In 2007, the MIC ordered mobile operators to install fil ering software enabling parents to control content seen by their children. A coalition of groups, including the Japan Internet Providers Association and the user rights organization Movement of Internet Active Users lobbied against the mandate and mobile users can now select voluntary fil ers.[34] Complaints to the official Consumer Affai s Agency about quasi-gambling functions in games played by children on mobile devices shot up in 2011, along with calls for government regulation.[35] Instead, in 2012, game developers Gree and DeNA Mobage voluntarily adopted caps on purchases of virtual items by minors.[36] Games integrated with social networks have also been criticized for their potential for abuse by sexual predators.

Private interests also pressure ISPs to restrict content. In 2012, a coalition of music rights advocates were reportedly offering to sell service providers a tool to detect whether material being uploaded

31 Broadcasting Ethics & Program Improvement Organization, "About BPO," http://bit.ly/1jevVLs; Content Evaluation and Monitoring Association, "About EMA," [in Japanese] http://bit.ly/1P0Mqrf; Internet Content Safety Association, "About the Organization," [in Japanese] http://bit.ly/1Mhsnmy.

32 Agence France-Presse, "Japan Internet Providers Block Child Porn," Benton Foundation, April 21, 2011, http://bit.ly/1jQS9Di; Electronic Network Consortium, "Development and Operation of the Next-Generation Rating/Filtering System on the Internet," press release, via New Media Development Association, April 30, 1999, http://www.nmda.or.jp/enc/rating2nd-en.html.

33 Amanda Dobbins, "Obscenity In Japan: Moral Guidance Without Legal Guidance," 2009, http://works.bepress.com/amanda_dobbins/1.

34 Izumi Aizu, "Japan," *Access to Online Information and Knowledge 2009,* Global Information Society Watch, http://bit.ly/16AioGr.

35 Ishaan, "Japanese Social Games Risk Seeing Crackdown," *Siliconera,* May 7, 2012, http://bit.ly/1Mht0fY.

36 Dr. Serkan Toto, "Self-Regulation: Dena Introduces Payment Caps For Minors On Mobage [Social Games]," Kantan Games, Inc (blog), April 24, 2012, http://bit.ly/1MhtfYn.

to the internet is subject to copyright, and sever connections of users violating Japan's strict copyright laws.[37] No follow-up was reported.

Content Removal

During the coverage period, courts continued to accept lawsuits from individuals requesting that search engines delink inaccurate or irrelevant material about them from public results. This "right to be forgotten" runs along similar lines to a 2014 decision by the Court of Justice of the European Union, which excluded public figu es to prevent abuse, but placed the onus of assessing whether requests merit that exception on the companies that operate search engines. In Japan, which lacks similar legal guidance, cases against search engine companies have been dealt with by the courts on an individual basis.

In November 2015, the Tokyo District Court issued a temporary injunction for Google to remove search results involving a dentist's prior arrest for malpractice fi e years before, on grounds that "search results should be deleted after a certain period."[38] The decision was the fi st in a Japanese court to involve content relevant to an individual's profession,[39] though news reports did not indicate if content was restricted as a result. In a separate case in December 2015, the Tokyo District Court issued an injunction against Yahoo Japan to delete 11 out of 47 search results concerning an individual who maintained his right to privacy. The presiding judge explained that "descriptions found in search results about the man's past 'significantly dis ort the (plaintiff's) current status.'[40] Details of the content affected were not publicly reported. Also in December 2015, the Saitama District Court upheld that "the right to be forgotten should be recognized with the passage of time."[41] Involving an individual who had been arrested for child prostitution and pornography in 2013, the original suit brought before the Saitama District Court in June 2015 ordered Google to remove search results, including media reports.[42] Google appealed the decision to the Tokyo High Court, and in July 2016, that court overturned the earlier judgment, rejecting the appeal on the grounds that "the right to be forgotten is not a privilege stated in law and its prerequisites or effects are not determined."[43]

The 2001 Provider Liability Limitation Act directed ISPs to establish a self-regulatory framework to govern takedown requests involving illegal or objectionable content, defamation, privacy violations and copyright infringement.[44] In 2002, industry associations produced guidelines designed to protect ISPs from legal liability within the jurisdiction of the Japanese courts. Under the guidelines, anyone can report material that infringes directly on their personal rights to the service provider, either to have it removed or to find out who pos ed it. No third party can do so. The provider notifies the individual who posted the content, and either fulfills the equest with their permission or removes the content without the authors' approval if they fail to respond. If the poster refuses permission, the service provider is authorized to assess the complaint for themselves, and comply if they believe it

37 Enigmax, "Jail For File-Sharing Not Enough, Labels Want ISP-Level Spying Regime," *TorrentFreak,* June 24, 2012, http://bit.ly/1L1QnIa.

38 "Google ordered to delete search results on dentist's arrest," *The Asahi Shimbun*, November 2, 2015.

39 "Google ordered to delete search results on dentist's arrest," *The Asahi Shimbun*, November 2, 2015.

40 "Tokyo court orders Yahoo Japan to remove search results on individual," *Japan Today*, December 8, 2015.

41 "Japanese court recognizes 'right to be forgotten' in suit against Google," *Japan Today*, February 28, 2016.

42 "Japanese court recognizes 'right to be forgotten' in suit against Google," *Japan Today*, February 28, 2016.

43 "Tokyo High Court overturns man's 'right to be forgotten'," *The Japan Times*, July 13, 2016.

44 Act on the Limitation of Liability for Damages of Specified elecommunications Service Providers and the Right to Demand Disclosure of Identification Info mation of the Senders, No. 137, November 30, 2001, available at UNESCO, http://bit.ly/1VH6zBu.

is legitimate. In this scenario, an ISP could give the complainant information to identify the poster—such as their name or IP address—without that person's consent, leading to privacy concerns. This process is voluntary, but by complying, service providers protect themselves from civil liability.[45]

In recent years, content removals have focused on obscene content, including child pornography and "revenge porn," explicit images shared without consent of the subject. After complying with a takedown order in 2014, Facebook was further ordered by a Tokyo court to "disclose the IP addresses used by fake accounts that were posting revenge porn."[46] A law to address online harassment by means of posting explicit images without the subject's consent passed in November 2014. Prior to this law's passage, upon receiving a complaint, providers were legally obligated to contact the original poster of the images to indicate that such objectionable content would be taken down within seven days. In the case where there was no response from the original poster, the content could be legally deleted by the provider. The new law passed in 2014 reduced the duration of time allowed to the providers to comply with takedown requests from seven days to two days (see Legal Environment).[47] Between November 27 and December 31, 2014, over 100 complaints of revenge porn were received by the National Policy Agency.[48]

The Internet Hotline Center, operated through the Internet Association Japan as part of a contract with the National Police Agency (NPA), cooperates with ISPs to solicit reports of illegal or harmful content from the public.[49] The center received a record high of 247,779 reports in 2015, an increase of close to 100,000 reports from the previous year and well above the former record high of 196,474 calls in 2012.[50] Nearly 140,000 reports were received between July and October 2015 alone.[51] A breakdown of reports by type reveals that 72,073 cases, or 29 percent of the total for 2015, featured information involving illegal activities, such as public display of obscene materials or "publicly inciting or soliciting others to abuse controlled substances." Among those, close to 50,000 were considered domestic cases, with the rest originating from overseas. A total 5,333 reports involved harmful information, which the center defines as "info mation that could invite illegal conduct, related to suicide, or which is 'difficult o judge as illegal but seems to be illegal.'" Of these, 63 percent were assessed as originating overseas. The center characterized the remaining reports as "beyond [the] scope of its operational guidelines, including defamation, slander, murder notices, intellectual property infringement, information inappropriate for children, and other cases."[52] After assessing the reports, the center referred 48,702 cases of illegal information to the NPA for handling, resulting in 32,534 content removal requests sent to ISPs, who complied with 93 percent;[53] for harmful information, 203 reports were forwarded to the NPA, who sent 1,719 content removal requests to ISPs, who complied in 81 percent of cases.[54] Providers are not obliged to comply with content removal requests submitted through the center.

45 Business Software Alliance, "Country Report: Japan," 2012, http://bit.ly/1VH7uHq.

46 "Court orders Facebook to reveal revenge porn IP addresses," *Japan Today*, October 22, 2014,

47 "*Ribenjiporuno ni chōeki 3 nen ika no bassoku jimin hōan teishutsu e*" ("LDP submit Bill to punish revenue porn with up to three years' imprisonment"), *Nihon Keizai Shimbun*, October 12, 2014. (http://www.nikkei.com/article/DGXLASFS11H03_S4A011C1PE8000/)

48 Takuro Yagi, "Police field 110 complaints f 'revenge porn' in fi st month of tough new law," *Asahi Shimbun*, April 3, 2015.

49 Internet Hotline Center Japan, "Annual Statistics 2013," May 1, 2014, http://www.internethotline.jp/statistics/2013e.pdf.

50 Internet Hotline Center Japan, "Annual Statistics 2014," June 8, 2016, http://www.internethotline.jp/statistics/index_en.html

51 Internet Hotline Center Japan, "Annual Statistics 2014," June 8, 2016, http://www.internethotline.jp/statistics/index_en.html

52 Internet Hotline Center Japan, "Annual Statistics 2014," June 8, 2016, http://www.internethotline.jp/statistics/index_en.html

53 Internet Hotline Center Japan, "Annual Statistics 2014," June 8, 2016, http://www.internethotline.jp/statistics/index_en.html

54 Internet Hotline Center Japan, "Annual Statistics 2014," June 8, 2016, http://www.internethotline.jp/statistics/index_en.html

Media, Diversity, and Content Manipulation

Japanese citizens exercise some self-censorship online, often on historical and social issues. The society at large prefers "harmony," and people avoid criticizing the role of Japan's Emperor, especially when connected with historic events like World War II. Individuals and public figu es who break this code risk censure and even attacks from right-wing fanatics, who notoriously tried to assassinate the Nagasaki mayor on these grounds in the 1990s. Though exceptional, incidents like this still exert a chilling effect on Japanese expression.

Although not explicitly affecting Japan's internet environment, commentators during the coverage period noted "alarming signs of deteriorating media freedoms in Japan."[55] In January 2016, the internal affairs minister, Sanae Takaichi, told members of the Diet that "broadcasters that repeatedly failed to show "fairness" in their political coverage, despite official wa nings, could be taken off the air."[56] In March, three television news anchors lost their jobs following reports of pressure from the current administration. Accounts of government interference in news gathering began escalating in 2014, when Tokyo-based television stations received a government document instructing that they "ensure fairness, neutrality and correctness," according to local news reports.[57] However, up to the end of the reporting period, there were no reports of content manipulation specifically focusing on digital content.

There are few known cases of the government or powerful groups proactively manipulating online news or other content. In a significant e ception, officials and the okyo Electric Power Company (TEPCO) withheld data about pollution after a nuclear power plant in Fukushima prefecture was severely damaged by the 2011 earthquake and tsunami, and citizens unwittingly exposed themselves to radiation. The MIC requested that four industry associations monitor false or unsubstantiated content circulating about the disaster online, including on social networks. Some observers said this was a measure to control public discourse, though deletions were not widespread. Service providers removed content, which included images of corpses, in at least 13 cases,[58] though the National Police Agency reported 41 items for review.[59] Others found an outlet to report on the aftermath of the disaster online.[60]

Media scrutiny of reportage involving the 2011 triple disaster continued during the coverage period. In mid-2016, articles appeared in major Japanese news outlets describing government officials p essuring TEPCO not to use the term "meltdown" at a news conference shortly after the events at the Fukushima Dai'ichi nuclear plant.[61]

55 Marvin Fackler, "The Silencing of Japan's Free Press," *Foreign Policy*, May 27, 2016, http://foreignpolicy.com/2016/05/27/the-silencing-of-japans-free-press-shinzo-abe-media/.

56 Justin McCurry, Japanese TV anchors lose their jobs amid claims of political pressure," *The Guardian*, February 17, 2016, https://www.theguardian.com/world/2016/feb/17/japanese-tv-anchors-lose-their-jobs-amid-claims-of-political-pressure.

57 "Self-censorship sensed as Japan's TV stations replace outspoken anchors," The Japan Times, January 26, 2016.

58 Madeline Earp, "Freelance, online reporting discouraged on nuclear threat," Committee to Protect Journalists (blog), April 14, 2011, https://cpj.org/x/42f5; Ministry of Internal Affairs and Communications, "Demand for Telecommunications Carriers Associations Regarding the Appropriate Response to False Rumors on the Internet Related to the Great East Japan Earthquake,"[in Japanese] press release, April 6, 2011, http://bit.ly/1PjW9It.

59 National Police Agency, "For Police Responding to False Rumors on the Internet," [in Japanese] June 21, 2011, http://bit.ly/1VH7lOT.

60 Keiko Tanaka,"20 Bitter Voices Rise From Fukushima After Japan's 2011 Nuclear Disaster," trans. Taylor Cazella, *Global Voices*, December 2, 2013, http://bit.ly/1L90n0j.

61 Kazuaki Nagata, "Tepco chief likely banned use of 'meltdown' under government pressure: report," *The Japan Times*, June 16, 2016.

In 2013 and 2014, some news reports expressed concern about nationalistic discourse by Japanese trolls, or *netōyo,* escalating into hate speech online, particularly targeting South Koreans and Chinese communities amid territorial disputes between Japan and their respective governments.[62] After an examination of "Japan's compliance with the international convention against racial discrimination" in August 2014, the UN Committee on the Elimination of Racial Discrimination recommended that hate speech be regulated.[63] As of August 2015, national-level legislation against hate speech remained elusive as major Japanese political parties were unable to agree on "a balance between restrictions on racial and ethnic slurs and freedom of expression guaranteed by the Constitution."[64]

Some countermeasures have been implemented. In 2015, a group of Korean residents and Japanese supporters established the Antiracism Information Center, which has a website and a physical location in Tokyo, to counteract hate speech online.[65] In May 2015, the Japanese website Niconico Dōga reported that it shut down a channel operated by the anti-Korean activist group *Zaitokukai*, citing violations of its terms of service.[66] In mid-December 2015, a viral online meme involving hate speech which purported to "debunk" the plight of refugees was circulated widely and subject to harsh criticism.[67] One month later, in January 2016, the Osaka city government passed Japan's fi st ordinance to combat hate speech. The ordinance authorized the public disclosure of groups who disseminate hate speech, defined as communication which defames and aims to exclude a particular group based on race or ethnicity" and including "online transmission," according to news reports.[68]

Blogs have a significant im act on public opinion, and several independent journalists are becoming influential th ough personal or commercial websites and social media accounts. Yet most online media remain small and community-based,[69] with no major national successes, and the mainstream media's habit of compliance and restraint may be standing in the way of the combative online news culture flourishing elsewhe e in Asia.[70] Kisha clubs, formal organizations only open to traditional media companies, and an advertising market that favors established players may be preventing digital media from gaining a foothold in the market. Kisha clubs provide essential access to officials in Japan, but have been accused of discriminating against new media practitioners in the past. In 2012, at least one online journalist was denied access to one of their Tokyo locations,[71] and the only two freelancers permitted to join an official g oup of 40 reporters on a tour of the Fukushima nuclear disaster site were forbidden from taking equipment.[72] Some online news outlets have struggled to sustain themselves financiall . *OhmyNews,* a South Korean platform, established a Japanese operation

62 Keiko Tanaka, "Countering Hate Speech in Tokyo's Koreatown," trans. Aparna Ray, *Global Voices*, March 6, 2014, http://bit.ly/1Rw5GLE.

63 "U.N. Panel urges Japan to regulate hate speech by law," *The Japan Times*, August 30, 2014.

64 "Party bickering shelves plan for law against 'hate speech'," *The Asahi Shimbun*, August 28, 2015.

65 Akira Nakano, "Antiracism website aids ethnic Korean victims of hate speech in Japan," *The Asahi Shimbun*, May 10, 2015.

66 "Video posting site shuts down anti-Korean Zaitokukai activists' channel," *The Japan Times*, May 20, 2015.

67 "As Japan Refuses to Accept More Refugees, a Hateful Meme Goes Viral," *Global Voices*, December 18, 2015. https://globalvoices.org/2015/12/18/as-japan-refuses-to-accept-more-refugees-a-hateful-meme-goes-viral/.

68 "Osaka assembly passes Japan's 1st ordinance to deter hate speech," *Japan Today*, January 16, 2016.

69 Keiko Tanaka, "Japan's Citizen Media Meet at Mikawa Medifes 2014," *Global Voices*, May 4, 2014, http://bit.ly/1hsF0OP.

70 Roger Pulvers, "Danger lurks when self-restraint segues into media self-censorship," *The Japan Times,* January 10, 2010, http://bit.ly/1Nq7dUR.

71 Keiko Tanaka, "Online Journalist Barred from Japan's Diet Press Hall," *Global Voices,* October 12, 2012, http://bit.ly/1L1S9t1.

72 Reporters Without Borders, "Freelance Journalists Face Discrimination On Fukushima Plant Visit," May 23, 2012, http://bit.ly/1Rw6qAu.

in 2006, but closed in 2008. The U.S.-based *Huffington Post* media website launched a Japanese-language version in 2013.[73]

YouTube, Twitter, Facebook, and international blog-hosting services are freely available, as are popular domestic platforms like Niconico Dōga, a video-sharing site, and LINE, a Korea-based chat application that was launched in Japan in 2011. Online campaigning continues to advance in Japan, as candidates and political parties used their websites and social media channels to share information and communicate with the electorate ahead of the July 2016 Upper House election. As only the third national-level election to be held in Japan since legislation allowing the use of websites and social networking services was passed in April 2013, candidates in particular made extensive use of platforms including Twitter, Facebook, YouTube, Niconico Dōga, and Ustream. However, even under revisions of the Public Offices Election La , although political parties and candidates may use email in their campaigns, general voters are not allowed to "call for votes" for a particular candidate via email (see Legal Environment).[74]

Digital Activism

Much digital activism in Japan has been effective at the local rather than national level. Grassroots online movements emerged in the mid-1980s when local community networks organized to protest deforestation in Zushi, Kanagawa prefecture.[75] Since then, some forms of digital activism have taken on social issues, such as one tracking racist graffiti in okyo.[76]

More initiatives sprang up in the "post-3.11" era (3.11 connotes the March 11, 2011 earthquake, tsunami, and nuclear plant accident). In the immediate aftermath of the triple disaster, maps sharing public information about disaster relief,[77] and Google's "Person Finder" web application were examples of the effective use of the internet to facilitate recovery.[78] Digital activists further spurred large demonstrations and protests against nuclear energy, many of which were organized through the internet and social media.

Free speech activists have also used the internet to campaign against the State Secrets law, which came into effect in 2014 (see Legal Environment). A Japanese internet activist and academic launched a whistleblower website to challenge the law.[79] The Students Against Secret Protection Law (SASPL), a Japanese activist group, actively used their website and social media channels to draw attention to and petition against the law's enactment. In May 2015, the group metamorphosed into the Students Emergency Action for Liberal Democracy (SEALDs) and continued to campaign via the internet against proposed laws which sought to redefine the ole of Japan's Self-Defense Forces and reinterpret Article 9 of Japan's Constitution, which renounces war.[80] The SEALDs actively protested

73 Arianna Huffing on, "Postcard From Japan: Talking Zen, Abenomics, Social Networking and the Constitution With Prime Minister Shinzo Abe," *Huffington Post,* May 9, 2013, http://huff.to/1MhvStk.

74 "公職選挙法—SNSでの選挙運動はOK,メールはNG" (Public Offices Election Law: Using SNS for cam aign activities is okay, using email is 'no good'). *President* (online), July 4, 2013 (July 15, 2013 print edition), http://president.jp/articles/-/9831.

75 Howard Rheingold, *The Virtual Community,* MIT Press, 1993.

76 Keiko Tanaka, "Countering Hate Speech in Tokyo's Koreatown," *Global Voices*, March 6, 2014, http://bit.ly/1Rw5GLE.

77 Keiko Tanaka, "Japan: OpenStreetMap Aggregates Typhoon Info," *Global Voices,* October 18, 2013, http://bit.ly/1jd6h9c; Keiko Tanaka, "Mapping Earthquake Reconstruction in Tohoku, Japan," *Global Voices*, October 7, 2013, http://bit.ly/1PjWKd0.

78 David Goldman, "Google gives '20%' to Japan crisis," CNN Money, March 17, 2011, http://money.cnn.com/2011/03/17/technology/google_person_finder_ja_an/.

79 "Japanese activist challenges secrets law with whistleblower website," *Japan Today*, December 22, 2014.

80 Jeff Kingston, "SEALDs: Students Slam Abe's Assault on Japan's Constitution," *The Asia-Pacific Journal: Japan Focus*, Volume 13, Issue 36, Number 1, August 31, 2015. http://apjjf.org/-Jeff-Kingston/4371.

the changes as undermining Japan's pacifist stance, although a bill einterpreting Article 9 to allow "collective self-defense" in support of Japan's allies passed into law in mid-September.[81] The SEALDs disbanded in August 2016, one month after the Upper House election in July.

Violations of User Rights

Significant amendments to the Act on the Protection of Personal Information (also referred to as the "Personal Privacy Law") were passed by the Diet in September 2015. While no security breaches affecting the new ID numbers allocated to residents of Japan under the "My Number" law have been reported since it went into operation in October 2015, official agencies reported that millions had been affected by record numbers of cyberattacks targeting personal data in 2015 and 2016.

Legal Environment

Article 21 of Japan's constitution prohibits censorship and protects freedom of "speech, press and all other forms of expression," as well as the "secrecy of any means of communication."[82] In general, individuals and the media can exercise this in practice, though social and legal constraints exist.

The Act on the Protection of Specially Designated Secrets came into force in December 2014, despite objections from the opposition, civil society, and protesters. The law gives a range of officials the discretion to indefini ely restrict public information pertaining to national security in any one of the categories of defense, foreign affairs, "prevention of designated harmful activities" (such as "counter-intelligence"), and prevention of terrorism.[83] Overseen by government officials rather than an independent body, it offers no protection for whistleblowers who reveal wrongdoing, leaving it open to misuse against Wikileaks-style whistleblowers and journalists.[84] For those people who handle such state-designated secrets, intentional leaks are punishable by up to 10 years' imprisonment, and unintentional leaks by up to 2 years. Individuals who knowingly receive such secrets from an administrative organ risk up to fi e years in prison for intentional disclosures and one year for disclosures made through negligence.[85] Subsequent guidelines outlined four main fields f state secrets (defense, diplomacy, anti-espionage, and antiterrorism measures), which are further divided into 55 categories.[86] Responding to criticism,[87] the government solicited public comments for a period of 30 days.[88] After receiving more than 20,000 public comments,[89] draft revisions were tabled. Yet even these drew concerns, particularly in terms of how the law would actually work in practice.[90] Protests continued throughout the country prior to the bill's coming into force in December 2014.

81 Matt Ford, "Japan Curtails Its Pacifist tance," *The Atlantic,* September 19, 2015, http://www.theatlantic.com/international/archive/2015/09/japan-pacifism-a ticle-nine/406318/.

82 The Constitution of Japan, November 3, 1946, http://bit.ly/1lLp7Tm.

83 Prime Minister of Japan, "Overview of the Act on the Protection of Specially Designated Secrets (SDS)," 2013, http://bit.ly/1OobNSj.

84 "Weak state secrets oversight," *The Japan Times*, July 28, 2014, http://bit.ly/1Mgu5QZ.

85 Cabinet Secretariat, "Overview of the Act on SDS Protection: 5. Penalty and Others," Preparatory Office for Enfo cement of the Act on the Protection of Specially Designated Secrets," http://www.kantei.go.jp/jp/topics/2013/headline/houritu_gaiyou_e.pdf#page=6&zoom=auto,-8,62.

86 "State secrets to be refined in o 55 fields" *The Japan News (Yomiuri Shimbun)*, July 18, 2014.

87 "Government revising guidelines on state secrets amid flur y of criticism," *The Japan Times*, September 20, 2014, http://bit.ly/1VHejsH.

88 "Government revising guidelines on state secrets amid flur y of criticism."

89 "Gov't sets guidelines on state secrets as concerns remain over arbitrary designation," *Mainichi Shimbun*, October 15, 2014.

90 "Kansai's fears of new law no state secret," *Japan Times*, October 26, 2014.

Other laws include potentially disproportionate penalties for online activity, including a 2012 legal revision targeting copyright violators—including any internet user downloading content they know has been illegally copied, as opposed to just those engaged in piracy for commercial gain.[91] While both uploading and downloading pirated material was already illegal under the copyright law, with uploaders subject to 10 years' imprisonment or fines up o JPY 10 million (US$102,000), the version in effect since October 1, 2012 added two years in jail or fines up o JPY two million (US$20,500) for downloading a single pirated file [92] The Japanese Bar Association said that downloading, as an essentially insignificant pe sonal act, should be regulated by civil instead of criminal laws.[93] In November 2015, fi e people were arrested for posting a chapter of *One Piece* online, a popular manga comic that is serialized monthly. The fi e people uploaded a chapter (translated into English) onto a website "host[ing] unauthorized uploads of Japanese comics."[94]

A 2013 revision of the Public Offices Election Act undid long-standing estrictions on the use of the internet for election campaigns. Limits remain on paid online advertising and campaign emails, which could only be sent directly by a party or candidate—not a supporter—in a measure designed to prevent fraud, though members of the electorate can freely solicit support on social media.[95] While these provisions were contested and revisions are still planned,[96] news reports said politicians violating these restrictions face a potential JPY 300,000 (US$3,060) fine or one ear in prison; imprisonment would strip them of political rights to vote or run for office. oters found improperly soliciting support for a candidate via email could be fined JPY 500,000 en (US$5,100) or jailed for two years, which would also deprive them of political rights.[97]

Article 175 of the Japanese penal code bans the sale or distribution of broader categories of obscene material, and while it dates from over 100 years ago, it is considered to apply online. [98] However, it does not define what constitu es obscenity, leading to concerns that it may infringe on artistic expression and LGBTI (lesbian, gay, bisexual, transgender, and intersex) rights.[99] In June 2014, a law passed punishing possession of images of child sexual abuse, with a possible penalty of one year imprisonment.[100] In August 2015, police in the Kansai area of Japan issued an arrest warrant for the founder of FC2 (a video-sharing website), under suspicion of uploading obscene "electromagnetic recordings" and making them available to an "unspecified number f people."[101] The suspect and the corporation that operates FC2 are both based in the U.S.[102]

91 Daniel Feit, "Japan Passes Jail-for-Downloaders Anti-Piracy Law," *Wired,* June 21, 2012, http://wrd.cm/1hsGKaV.

92 Maira Sutton, "Japan's Copyright Problems: National Policies, ACTA, and TPP in the Horizon," *Deeplinks Blog,* Electronic Frontier Foundation, August 21, 2012, https://www.eff.org/deeplinks/2012/08/copyright-japan.

93 "Japan Introduces Piracy Penalties for Illegal Downloads," BBC, September 30, 2012, http://bbc.in/1g7S3gn.

94 Casey Baseel, "Police arrest 5 men over illegal upload of 'One Piece' manga and translation," Rocket News, November 21, 2015. http://en.rocketnews24.com/2015/11/21/police-in-japan-arrest-fi e-men-connected-with-illegal-upload-of-one-piece-manga-and-translation/.

95 "Editorial: Internet election campaigns can change Japan's politics," *Asahi Shimbun,* April 20, 2013, http://bit.ly/1cOFsVZ.

96 Ida Torres, "Japan's Internet election campaigning ban one step closer to being lifted," *Japan Daily Press,* April 4, 2013, http://bit.ly/1R1hVPk.

97 Ayako Mie, "Election campaigning takes to Net," *The Japan Times, April 11, 2013, http://bit.ly/1GyqxaQ;* "Japanese parliament permit use of Internet campaigning during elections," *TJC Global* (blog), April 20, 2013, http://bit.ly/1LBPvNV.

98 James R. Alexander, "Obscenity, Pornography, and the Law in Japan: Reconsidering Oshima's *In the Realm of the Senses,*" *Asian-Pacific Law and Policy Journal* 4, no.1 (2003): 148-168, http://bit.ly/1OodGhM; Keiho [Penal Code] Act No. 45 of April 24, 1907, [in Japanese] http://bit.ly/1JVbWGD.

99 Keiko Tanaka, "Japan's Porn Law is Strangling Artists," February 18, 2013, http://bit.ly/1VHbkLA.

100 "Japan bans child pornography possession," *BBC,* June 18, 2014, http://bbc.in/1qc3U5j.

101 "Arrest warrant issued for founder of FC2 video-sharing website on obscenity charges," *Mainichi Japan,* August 20, 2015.

102 "FC2 founder placed on intl wanted list," *Japan News by The Yomiuri Shimbun,* August 20, 2015.

Heightened awareness of revenge porn and online harassment culminated in the ruling Liberal Democratic Party (LDP) passing a bill criminalizing revenge porn in November 2014. The law stipulates that "offenders who distribute such images could face up to three years in prison or a fine f up to JPY 500,000 yen (US$5,100), with third-party distribution also leading to up to one year in prison or a fine f JPY 300,000 yen (US$3,060).[103]

Prosecutions and Detentions for Online Activities

No citizens faced politically-motivated arrest or prosecution for legitimate digital activity during the coverage period of this report.

Surveillance, Privacy, and Anonymity

Japan's Supreme Court protects privacy through its interpretation of Article 13 of the constitution, which provides for the right to life and liberty.[104] "Secrecy of communication" is also protected under telecommunications laws,[105] though some digital activities require registration. Major mobile carriers require customers to present identification documents in o der to subscribe. Internet cafe users are required to produce formal ID such as a driver's license and register their name and address. Police can request these details, along with usage logs, if they detect illegal online activity.

Under voluntary guidelines drafted by four ISPs in 2005, service providers automatically inform police of internet users identified on p o-suicide websites, and comply with law enforcement requests for information related to acts of self-harm.[106] A law enacted in 2003 and revised in 2008 prohibits electronic communications from encouraging sexual activity with minors.[107] Under the law, all online dating services must register with the police, verify their customers' ages with a driver's license or credit card, and delete or block content that appears to involve someone under 18; most services voluntarily monitor messages in real-time to ensure compliance.

Under a wiretap law enacted in 1999, law enforcement agents may seek a court order to conduct electronic surveillance in criminal investigations involving drugs, fi earms, human trafficking, or o - ganized murders, in an exception to articles of other laws that explicitly forbid wiretapping.[108] The law obliges agents to notify targets of wiretaps after investigations are concluded and inform the Diet about the number they implement annually. While the law was extremely controversial when it passed, in part due to the authorities' politicized abuse of surveillance in the past,[109] lawmakers were seeking to expand it in 2012.[110] Critics say the law does not prevent the systematic storage of inter-

103 "Release of explicit images without consent to be criminalized," *Japan Times*, November 18, 2014.

104 Privacy International, "Chapter i: Legal Framework," in *Japan*, December 12, 2006, https://www.privacyinternational.org/reports/japan/i-legal-framework.

105 Ministry of Internal Affairs and Communications, Telecommunications Business Act, Act No. 86 of December 25, 1984, http://bit.ly/1ZhfM8n.

106 Carolina A. Klein, "Live Deaths Online: Internet Suicide and Lethality," *American Academy of Psychiatry and the Law* 40, no. 4 (December 2012): 530-536, http://www.jaapl.org/content/40/4/530.full.

107 Akira Saka, "Regulation for Online Dating in Japan,"(presentation Keio University, Japan, 2008) http://bit.ly/1GyrZtI.

108 Privacy International, "Chapter ii: Surveillance," in *Japan*, December 12, 2006, https://www.privacyinternational.org/reports/japan/ii-surveillance-policy.

109 In 1997, a court ordered the government to pay a senior member of the Japanese Communist Party 4 million yen [US$35,500] in damages for illegally wiretapping his residence in the 1980s. See, "Tokyo, Kanagawa Bow to Wiretap Ruling," *The Japan Times,* July 7, 1997, http://bit.ly/1P0TRhW.

110 Tsuyoshi Tamura, "Legal panel to discuss wiretapping for wider range of crimes," *Asahi Shimbun,* December 25, 2012, http://bit.ly/1L95TjI.

cepted communications or protect innocent parties.[111] Security agents and the military have been accused of implementing illegal surveillance in cases involving national security in 2003 and 2004.[112]

A law to protect personal information dating from 2003 protects individuals' data collected electronically by private and public sector organizations, where the data involves more than 5,000 records.[113] Law enforcement requests for this data should be supported by a warrant.[114] In response to technological developments, the growing use of big data, and the introduction of the "My Number" national resident system the following month, significant amendments o the Act on the Protection of Personal Information (also referred to as the "Personal Privacy Law") were passed by the Diet in September 2015. In the amended Act, "personal information" is defined in mo e specific erms as "biometric information" and "numeric data that is capable of identifying a specific individual (such as mobile phone numbers and passport numbers)."[115] Anonymization provisions allow for personal data to be transferred to a third party without the consent of the subject if specific equirements are met.[116] The amendment banned the collection of sensitive information such as "race, medical history, and criminal history."[117] Criminal sanctions for misusing personal data and restrictions on the transfer of personal data to overseas jurisdictions lacking equivalent data protection frameworks were also strengthened.[118] Finally, the amendment established the Personal Information Protection Committee as an "independent authority under the Cabinet Office" as a eplacement for the Consumer Affairs Agency, which previously oversaw personal data utilization.[119]

The "My Number" law, which was passed in the Diet in May 2013, came into effect during the coverage period of this report. From October 2015, all long-term residents of Japan were assigned a unique 12-digit number to be used for unified social elfare services, including taxation, pension benefits, and healthca e. Municipal governments also offered photo ID cards with "My Number" information that contain electronic data chips. A public opinion survey conducted by the Cabinet Office in anuary 2015 found that while only 28 percent of respondents were aware of the "My Number" system, nearly a third of those were concerned that "My Number" information could be used for unauthorized purposes.[120]

Data storage for an individual's "My Number" occurs mainly on the municipal government level, which is the basis for administration of the national resident register, municipal taxation, healthcare, and social services. In addition to collecting "My Number" identification numbe s from their own employees, public and private employers also require employees to submit their dependents' "My

111 Privacy International, "Chapter ii: Surveillance."

112 Reuters, "Japan's Military Watched Citizens: Communist Party," *bdnews24*, June 6, 2007, http://bit.ly/1PjY3ss.

113 Business Software Alliance, "Country Report: Japan."

114 Privacy International, "Chapter iii: Privacy Issues," in Japan, December 12, 2006, https://www.privacyinternational.org/reports/japan/iii-privacy-issues.

115 "New amendments to data protection law in Japan," Simmons & Simmons elexica, September 11, 2015, http://www.elexica.com/en/legal-topics/data-protection-and-privacy/11-new-amendments-to-data-protection-law-in-japan.

116 "New amendments to data protection law in Japan," Simmons & Simmons elexica, September 11, 2015, http://www.elexica.com/en/legal-topics/data-protection-and-privacy/11-new-amendments-to-data-protection-law-in-japan.

117 Joe Jones, "Japan's Amends its Data Privacy Law: 'Big Data' Comes with New Regulations," Global IP & Privacy Blog, September 16, 2015. http://www.iptechblog.com/2015/09/japan-amends-its-data-privacy-law-big-data-comes-with-new-regulations/.

118 Daisuke Tatsuno and Kensaku Takase, "Introduction of significant amendments o Japan's Privacy Law, Global Compliance News, September 4, 2015. https://globalcompliancenews.com/introduction-of-significan -amendments-to-japans-privacy-law/.

119 "New amendments to data protection law in Japan," Simmons & Simmons elexica. September 11, 2015. http://www.elexica.com/en/legal-topics/data-protection-and-privacy/11-new-amendments-to-data-protection-law-in-japan.

120 "Editorial: Gov't must explain purpose of 'My Number' identification sys em," *The Mainichi,* March 31, 2015, http://bit.ly/1FUXUd4.

Number" identification numbe s to confi m dependent status. Upon such requests, employers must confi m beforehand that they are using dependents' "My Number" identification numbe s only for such purposes and that they have systems in place to safeguard personal information. Despite initial fears,[121] no official eports of fraudulent use of personal data have been made since the system's implementation.

The government has announced that starting in 2018, "My Number" identification numbe s may be linked voluntarily with individuals' bank accounts to ensure accurate reporting of annual income, benefits, and taxation, with this p ovision becoming mandatory from 2021.[122]

The "My Number" system is the most recent in a series of attempts to nationally unify Japan's Basic Resident Registry procedures to facilitate information sharing among local governments in the case of residents who move, register births and deaths, and apply for social services.[123] The issue of a nationally available registry service has been contested based on privacy issues and fears of personal information leakages. Politicians and bureaucrats have maintained that personal identification nu - bers would streamline social benefits and maintain accuracy and fai ness in the provision of government services,[124] as well as assist in identifying individuals in the case of natural disasters.[125]

Intimidation and Violence

No physical violence has been reported against bloggers or internet users in relation to their online activity.

Technical Attacks

While distributed denial-of-service (DDoS) attacks were part of the arsenal used by nationalists in Japan, China, and South Korea to target perceived opponents in other countries, and cyberattacks have been reported against commercial and government targets,[126] they are not known to have been used to systematically target individuals or civil society groups. However, media and individual attention to cybersecurity threats has increased since mid-2015 when 1.25 million citizens were affected by the release of personal information obtained by illegally accessing Japan's pension system using an email virus.[127]

In January 2016, a Kyodo News survey reported that "at least 2.07 million sets of personal data were [either] stolen or feared leaked from 140 companies and organizations in Japan [that] were hit by cyberattacks in 2015."[128] Nearly half of the targets, including private companies, government agencies, and universities, indicated that they noticed such attacks only after being alerted by third parties,

121 "'My number' is dangerous," *The Japan Times*.

122 "My Number system raises red flags in apan ahead of notice release," Asia Times, October 3, 2015. http://atimes.com/2015/10/my-number-system-raises-red-flags-in-ja an-ahead-of-notice-release/

123 Rebecca Bowe, "In Japan, National ID Proposal Spurs Privacy Concerns," *Deeplinks Blog*, Electronic Frontier Foundation, June 13, 2012, http://bit.ly/1OofXJQ.

124 "EDITORIAL: ID number system should be a tool to build a fair society," *The Asahi Shimbun*.

125 "Lower House passes 'my number' bill," *The Japan Times,* May 10, 2013, http://bit.ly/1L1We0n.

126 "Over 1,000 targeted cyber-attacks hit Japanese entities in 2012," *The Japan Times,* March 1, 2013, http://bit.ly/1LBUFtq.

127 William Mallard and Linda Sieg, "Japan pension system hacked, 1.25 million cases of personal data leaked," eds. Robert Birsel and Clarence Fernandez, *Reuters,* June 1, 2015, http://reut.rs/1QkFnWy.

128 "At least 2 million sets of personal data feared stolen in 2015 cyberattacks," *The Japan Times*, January 4, 2016.

including the Japan Computer Emergency Response Team Coordinator Center and the police.[129] In February 2016, the National Institute of Information and Communications Technology reported "a record 54.51 billion cyberattacks detected in Japan" throughout 2015, and said that many originated from computers in China and the United States.[130]

Cyberattacks focusing on animal rights issues garnered media attention during the coverage period. Early 2016 news articles reported DDoS attacks targeted the prime minister's official ebsite to protest Japanese whaling activities throughout 2015.[131] Websites associated with the Taiji dolphin hunt, the location featured in the 2009 documentary "The Cove," were also subject to repeated cyberattacks during October and early November.[132] The Anonymous hacker network reportedly claimed responsibility for at least 37 such attacks; the Taiji municipal website was a major target.[133] Anonymous hackers used Twitter to warn of further attacks on the Taiji municipal website as well as aquariums throughout Japan.[134] This activity continued into 2016, with Japanese car manufacturer Nissan, and Narita Airport reporting cyberattacks in January 2016.[135] In February 2016, Anonymous claimed responsibility for cyberattacks causing outages on the Japan External Trade Organization (JETRO), National Tax Agency, and Japan Securities Finance Company websites.[136]

129 "At least 2 million sets of personal data feared stolen in 2015 cyberattacks," *The Japan Times*, January 4, 2016.

130 "Record 54.5 bil cyberattacks detected in Japan in 2015," *Japan Today*, February 21, 2016.

131 "At least 2 million sets of personal data feared stolen in 2015 cyberattacks," *The Japan Times*, January 4, 2016.

132 "Cyber-attacks spread across Japan from Taiji dolphin hunt town," *The Asahi Shimbun*, November 13, 2015.

133 "Cyber-attacks spread across Japan from Taiji dolphin hunt town," *The Asahi Shimbun*, November 13, 2015.

134 "Cyber-attacks spread across Japan from Taiji dolphin hunt town," *The Asahi Shimbun*, November 13, 2015.

135 "Narita airport website inaccessible after huge number of accesses," *Japan Today*, January 24, 2016. "Nissan shuts down websites after anti-whaling cyberattacks," *The Japan Times*, January 14, 2016.

136 "Anonymous hackers harpoon Japanese websites in whaling protest," *The Japan Times*, February 10, 2016.

Freedom House

Jordan

	2015	2016
Internet Freedom Status	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	12	13
Limits on Content (0-35)	16	16
Violations of User Rights (0-40)	22	22
TOTAL* (0-100)	**50**	**51**

* 0=most free, 100=least free

Population:	**7.6 million**
Internet Penetration 2015 (ITU):	**53 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- In an attempt to curb cheating by high school students on their final- ear exams, the government blocked WhatsApp, Instagram, and Viber for several hours across the country in June 2015 (see **Restrictions on Connectivity**).
- After Jordan's telecommunications regulator rejected mobile providers' attempt to charge for VoIP servicers, providers blocked calling features on communication apps (see **Restrictions on Connectivity**).
- In June 2015, amendments to the Cybercrime Law came into effect in June 2015 which set out prison sentences for online defamation. Authorities later ruled that the law supersedes a provision in the press law that forbids journalists from being jailed (see **Legal Environment**).
- Journalists like Jamal Ayoub, Osama Ramini, Hassan Safirah, tef al-Joulani, Dhaigham Khreisat, Diyaa Khraisat, and Ramez Abo Yousef were detained, prosecuted, and in some cases sentenced to prison terms of three to four months for news articles that were deemed defamatory to public officials or ha mful to Jordan's foreign relations (see **Prosecutions and Detentions for Online Activities**).

Introduction

Internet freedom declined in Jordan over the past year due to restrictions on communication apps and arrests of journalists under the newly amended Cybercrime Law.

In June 2015, amendments to the Cybercrime Law came into effect, including a provision that undermines journalists' immunity from imprisonment under the Press and Publication Law (PPL). Human rights groups have called on parliament to repeal Article 11 of the Cybercrime Law, which penalizes online defamation with a fine and prison sen ence of at least three months.[1] The Law Interpretation Bureau later ruled that the law could also be applied to journalists for articles that appeared on outlets' websites, thereby contravening protections in the PPL. At least seven journalists were arrested for news articles that appeared online over the coverage period, while several others were detained for Facebook posts.

Observers see the new clampdown as sending mixed signals about the state's stance on reform. After the regional uprisings of 2011, constitutional amendments were passed to calm public discontent, improving protections on freedom of expression and strengthening the independence of the judiciary, while parliamentary elections took place under a slightly improved electoral framework in January 2013. However, when amendments to the PPL came into force that June, nearly 300 websites were blocked for failing to register with the Media Commission. Although most of the sites eventually received licenses and were unblocked, the government continued to block unlicensed news websites during the coverage period. Amendments to the antiterrorism law passed in 2014 broadened the definition f terrorism to include acts that "could threaten the country's relations to foreign states or expose the country or its citizens to retaliatory acts on them or their money." Several Jordanian journalists and activists have been tried under this provision, in some cases leading to prison sentences.

While internet access has grown, certain social media platforms and communication apps have recently experienced restrictions in the country. In June 2015 (and again in 2016), authorities blocked Instagram, Viber, and WhatsApp in an effort to prevent students from cheating on secondary school exams. While the restrictions were temporary, lasting several hours at a time, they were nonetheless unnecessary and disproportionate. Millions of Jordanians who rely on the services to do business and communicate with one another were unable to access them. Furthermore, mobile providers permanently blocked Voice over Internet Protocol (VoIP) services offered by the likes of Viber, WhatsApp, and Skype during the coverage period, after the providers failed in their bid to charge customers more for making calls over the internet.

Obstacles to Access

Mobile broadband has soared in the country, boosted by the introduction of 4G LTE and new packages with more affordable pricing. However, the ICT market continues to be largely controlled by the influence of Jordan's existing providers.

1 "Jordan: Talking is Not a Crime.. A Campaign to Repeal Article 11 of Cybercrime Law," Al Araby Al Jadeed [in Arabic], March 5, 2016 http://bit.ly/1T4jjTR.

Availability and Ease of Access

According to the International Telecommunication Union (ITU), a total of 53 percent of the Jordanian population had access to the internet by the end of 2015, up from 27 percent fi e years earlier.[2] On the other hand, national figu es from the Telecommunications Regulation Commission (TRC) estimated 7.9 million Jordanians had access to the internet, resulting in a penetration rate of 83 percent by the end of 2015. Similarly, the TRC estimated the number of mobile broadband subscriptions at 2.736 million by the end of 2015, while fi ed-line ADSL subscriptions numbered far less at 219,752. Mobile phone usage has also expanded, as the number of subscriptions was slightly over 13.7 million by the end of 2015, representing a penetration rate of 145 percent.[3]

According to Pew Research Center, there is a "real and pervasive" demographic digital divide among internet users in Jordan. While 75 percent of individuals from the ages of 18-34 were internet users, the percentage dropped to 57 percent among those aged 35 years and above. The contrast was even starker when looking at education levels. Ninety-six percent of people with "more education" used the internet, compared to only 41 percent of Jordanians with "less education." The report also shed light on economic differences, as 80 percent of people with high incomes were internet users compared to 50 percent in low-income groups.[4]

For several years, internet connection fees were considered high relative to neighboring countries and the cost of living. Prices have dropped, but complaints about the quality of service persist. Monthly fi ed-line subscription prices currently range from JOD 19.9 (US$28) for speeds of 1 Mbps and an allowance of 10 Gigabytes (GB), to JOD 34.9 (US$59) for speeds of up to 24 Mbps and unlimited downloads. Orange Jordan also began offering a fibe -optic connection with speeds up to 80 Mbps and unlimited download allowance for JOD 74.9 per month (US$105.5). Postpaid monthly plans for Evolved High-Speed Packet Access (HSPA+) range from JOD 10 (US$14) to JOD 20 (US$28) per month, depending on speeds and data allowances.[5] By comparison, gross national income per capita is US$4,950, or US$413 per month.[6] Meanwhile, internet access in many of the country's governorates and remote areas remains poor, as almost all companies concentrate their operations and promotions in major cities, particularly the capital Amman.

Restrictions on Connectivity

In June 2015, the Jordanian government ordered internet service providers to block access to WhatsApp, Instagram, and Viber for a couple of hours on days that secondary school students sat for their national exam (Tawhiji).[7] An estimated six million Jordanians use WhatsApp. Observers criticized the move, intended to prevent cheating, as unnecessary and disproportionate. [8]

In March 2016, Jordanian mobile operators attempted to impose fees on the use of VoIP services in

2 International Telecommunication Union, "Percentage of individuals using the Internet," 2015, http://bit.ly/1cblxxY.

3 TRC, "Telecommunications Indicators (Q1/2015-Q4/2015)," http://bit.ly/1MucXhd.

4 Jacob Poushter, "Internet Access Growing Worldwide but Remains Higher in Advanced Economies," Pew Research Center, February 22, 2016, http://pewrsr.ch/1TwX4H2.

5 Zain, "Voice Plans & Benefits" 2015, http://www.jo.zain.com/english/consumer/voice/Pages/default.aspx.

6 World Bank Databank, "GNI per capita, Atlas method (current US$)," 2009-2014, , http://bit.ly/1Diyy0Q.

7 Ibrahim Mbaydeen, "The government blocks Tawjihi classrooms' access to three applications", [in Arabic] Al-Ghad, June 20, 2015 http://bit.ly/260JtOi.

8 Reem Al-Masri, "Cheating in Tawjihi: Do not blame Whatsapp", [in Arabic] 7iber, June 22, 2015, http://bit.ly/1NozUgL.

order to increase profits, but ere later stopped by the TRC. [9] However, the providers later blocked users from making free or cheap phone calls over services like WhatsApp and Viber. In a statement to news site *7iber*, Yousef Mutawe, Chief Technology Officer (C O) at Zain, admitted that "these services are not available" on 3G and 4G networks. Mutawe justified the mo e by stating that these applications reaped profits without incurring any licensing fees for using the in ernet network, which was built by the operators.[10]

While no other restrictions on connectivity were seen in Jordan over the past year, the centralization of the internet backbone infrastructure in government hands remains a concern. The formerly state-owned Jordan Telecom controls the fi ed-line network and provides access to all other ISPs, thereby centralizing most of the connection to the international internet. The government retains a degree of control over the country's internet backbone, and all traffic within the count y must flow th ough a government-controlled telecommunications hub.

ICT Market

The ICT sector is regulated under Law No. 13 of 1995 and its amendment, Law No. 8 of 2002. The law endorses free-market policies and governs licensing and quality assurance.[11] Citizens and businesses can obtain internet access through privately owned service providers without state approval or registration. The market is dominated by Umniah (a subsidiary of Batelco Bahrain), Zain, and Jordan Telecom, in which France Telecom owns 51 percent of shares, with the remaining shares divided between Jordan's Social Security Corporation, armed forces, and others.

3G services were fi st launched by Zain and Jordan Telecom (Orange) in mid-2010 and increased upon implementation of a tax exemption for the purchase of smartphones and the launch of mobile broadband by another provider, Umniah.[12] A call from the TRC to introduce a fourth mobile operator in December 2012, however, was rejected by Zain and Jordan Telecom.[13] No new providers have been introduced since then and the three companies have a similar share of the market.[14] After rejecting two international operators, the Jordanian government awarded Zain Jordan the rights to introduce 4G/Long Term Evolution (LTE) services to the market, which it launched on February 14, 2014. In January 2015, Orange Jordan was awarded the second 4G license for US$100 million and launched LTE services in Amman in May 2015, with plans to expand the services nationwide.[15]

Regulatory Bodies

The TRC is the independent agency responsible for regulating the ICT sector. It is governed by the

9 ""No Charges on Online Calling Apps- Telecom Commission," Jordan Times, March 16, 2016. http://bit.ly/2bywrkk.

10 Reem al Masri, "Blocking Internet Calls: When Telecommunications Companies Sieve out Content". 7iber, August 15, 2016, http://bit.ly/2b04m3O.

11 "Jordan," in One Social Network With A Rebellious Message, Arabic Network for Human Rights Information, 2009, http://bit.ly/1V0uqvC.

12 International Telecommunication Union, "Smartphone tax exemption drives 3G growth (Jordan)," news release, January 19, 2012, http://bit.ly/1JBLEtS.

13 Ghazzal, Mohammad, "Orange Jordan Opposes TRC Plan," Jordan Times, December 15, 2012, accessed April 30, 2013 http://bit.ly/1ECBaO5.

14 Mai Barakat, "Jordan will be challenging, but a fourth operator might find elbow oom as a mobile broadband provider," Ovum, February 21, 2013, http://bit.ly/1JBMhUg.

15 Mohammad Ghazal, "Orange launches 4G in Amman, to expand nationwide by Q3," Jordan Times, May 26, 2015, http://bit.ly/1eCIvRh.

Telecommunications Law and defined as a "financially and administrat ely independent juridical personality."[16] Nonetheless, it is accountable to the Ministry of Information and Communication Technology (MoICT), which was created in April 2002 to drive the country's ICT development.[17] The TRC's Board of Commissioners and its chairman, currently Ghazi Salem Al-Jobor (appointed in June 2015),[18] are appointed by a resolution from the Council of Ministers based on a nomination from the prime minister.[19] Although one of the TRC's responsibilities is to monitor quality of service, it relies on self-evaluation reports submitted by the ISPs themselves, in which, for example, Orange Jordan claims that 99.9 percent of complaints are solved within 10 days of receipt. In March 2015, French telecoms company Orange brought a case before the International Centre for Settlement of Investment Disputes against Jordan for a lack of transparency in the procedure for renewing a 2G license.[20]

Limits on Content

Jordan's online media sphere has become increasingly censored since the amended Press and Publication Law came into force in 2013. Authorities have become more proactive in issuing and enforcing gag orders to news sites, often blocking them for failing to adhere to strict editorial guidelines. Self-censorship remains pervasive, particularly around the royal family and Islam, although digital activism has made many concrete gains over the past year.

Blocking and Filtering

Authorities block unlicensed local new sites and, occasionally, sites that fail to adhere to strict editorial guidelines or gag orders. On January 28, 2015, Jordanian authorities blocked the licensed local news website *Saraya News* after it published a report stating that an imprisoned Iraqi militant would be freed in a hostage negotiation deal with the "Islamic State" (IS) militant group.[21] The website was unavailable for 40 days, during which two staff were detained (see "Prosecutions and Detentions for Online Activities").

Amjad Al-Qadi, the head of the Media Commission, sent a memo on April 6, 2015 to all owners and editors of licensed news websites instructing them not to publish any news or information related to the military without a "clear and direct request to the authorized military sources." The request was delivered through an email sent to website owners and editors.[22]

During the period in question, several gag orders were issued on a variety of topics. For example:

- Amman's prosecutor general issued a gag order in September, 2015 banning information concerning the case of a program on the local Roya TV channel, which contained explicit sexual content and led to controversy among Jordanians.[23]

16 The Telecommunications Regulatory Commission of Jordan, Chapter III, http://bit.ly/1Mwi5QE.

17 Information & Communication Technology Association-Jordan, "Jordan ICT Sector Profile" Slide 10, accessed July 5, 2013, http://bit.ly/1V0uKKZ.

18 TRC, "Board of Commissioners Profile" http://bit.ly/1LD3DRd.

19 TRC, Telecommunication Law No. (13) of 1995, January 10, 1995, pg 18, accessed June 26,2013, http://bit.ly/1KWfNtT.

20 "Orange Sues Government Over 2G," [in Arabic] Al-Ghad, March 22, 2015, http://bit.ly/1Jl3Fjl.

21 Committee to Protect Journalists, "Jordan Arrests Two Journalists on Aiding Terrorism Charges," January 29, 2015, http://cpj.org/x/5ecf.

22 The report author received a copy of the email.

23 "Gag Order Bans Publication on Roya's Case," Al Rai, September 10, 2015. http://bit.ly/2bmWH3C.

- In March 2016, Jordan Media Commission Director General Amjad Qadi ordered a ban on information related to a raid on a terrorist cell in Irbid, Jordan.[24]

Blocking of websites is currently carried out with respect to the Press and Publications Law (PPL), amended in 2012, which stipulated that news websites need to obtain a license from the Media Commission or face blocking. The law also requires any electronic publication that publishes domestic or international news, press releases, or comments to register with the Ministry of Commerce and Industry. One of the requirements for a general news website to obtain a license is to have an editor-in-chief who has been a member of the Jordan Press Association (JPA) for at least four years. The problematic situation eased in July 2014, when the JPA law was amended to enable journalists in online media to become members. Prior to that, journalists could only become members if they underwent a period of "training" in an "official" media o ganization. According to the Center to Defend Freedom of Journalists (CDFJ), around 500 journalists in Jordan are not members of the JPA.

For many observers, the law's broad definition f a news website includes almost all Jordanian and international websites, blogs, portals, and social networks. According the amended PPL, an electronic publication is defined as "[a]ny ebsite with a specific eb address on the internet which provides publishing services, including news, reports, investigations, articles, and comments, and chooses to be listed in a special register maintained at the Department, pursuant to instructions issued by the Minister for this purpose."[25] Articles 48 and 49 enable the head of the Media Commission to block any website for failing to obtain a license or, more broadly, for violating Jordanian law.

Consequently, 291 news websites were blocked in June 2013 on instructions from the head of the Media Commission (then-named the Press and Publications Department) after a nine-month grace period. Most have since applied for a license to get unblocked. By June 2014, there were 160 licensed general news sites and 100 specialized websites. To obtain licenses, most general news websites hired new chief editors who were already JPA members, a concerning development for independent media given that 64 percent of JPA members work in government or government-related media outlets.[26] Out of 160 licensed websites, 68 hired new editors-in-chief who have full time jobs at other media outlets, a violation of Article (23-A) of the PPL.[27] As of October 2014, 112 websites were blocked, but only 15 of those were operational—the remaining had shut down.

Some unlicensed websites have resorted to using alternative domains in order to remain accessible in Jordan, such as JordaniansVoice.net and 7iber.com. But in June 2014, the newly appointed head of the Media Commission sent a request to the TRC to block the alternative domains, which in turn sent a decree to ISPs to implement the blocking. In addition, the head of the Media Commission pressed charges against *7iber* two months later for operating an unlicensed media organization in violation of Article 48(B) of the PPL.

The Jordanian government claimed that the amendments were introduced "to regulate the work of news websites and in order to increase transparency and accountability." Officials sta ed that the law was called for by professionals within the industry in order to preserve professionalism and protect the media from those "who have practiced embezzlement, defamation and blackmailing to a de-

24 "Gag Order Bans Coverage of Irbid Terror Cell News," Jordan Times, March 6, 2016. http://bit.ly/2b9VfRy.
25 Jordanian Media Monitor, Amended Press & Publications Law No. 32 of 2012, August 2013, http://bit.ly/1zqh8ig.
26 Sawsan Zaideh, "The Jordan Press Association: A Monopoly by Law", 7iber, February 16, 2015, http://bit.ly/1zhSXSw.
27 Sawsan Zaideh, "Licensing News Websites: Legal Restrictions and Structural Deformities," 7iber, November 3, 2014, http://bit.ly/1bWgbba.

gree that threatened social peace."[28] On the other hand, local journalists, international human rights groups,[29] and a former Jordanian minister of media affairs and communication criticized the decision as a serious affront to freedom of the press[30] and a decisive move to censor the internet in Jordan.[31]

Content Removal

The 2012 amendments of the PPL increased the liability of intermediaries for content posted on their sites, placing readers' comments under the same restrictions as normal news content. Clause 3 of Article 49 states that both the editors-in-chief and owners of online publications are legally responsible for all content posted to the site, including user comments.[32] Moreover, websites must keep a record of all comments for six months after initial publication and refrain from publishing any "untruthful" or "irrelevant" comments.[33] As a result, some news websites, such as JO24, stopped, for a limited period of time, allowing comments altogether as an expression of protest.[34]

Media, Diversity, and Content Manipulation

The overwhelming majority of journalists continue to practice self-censorship, as the annual survey on media freedoms conducted by the Amman-based Center for Defending the Freedom of Journalists showed. According to the center's surveys, a staggering 95.2 percent of journalists said they practiced self-censorship in 2014, compared to 91 percent and 85.8 percent, respectively, in 2013 and 2012.[35] When asked about taboo topics, 93.3 percent said they avoided criticizing the armed forces, and 90.4 percent stated they feared criticizing the king, the royal court and members of the royal family. In previous years, more than three-quarters of journalists indicated they avoid publishing any material critical of the military, the judicial system, tribal leaders, and religion.[36] In one incident, prominent journalist and writer Rana Sabbagh wrote on her Facebook profile that her bi- eekly column in *Al-Ghad* newspaper was banned by the editor, and that she would publish the column on Facebook and in another media outlet.[37]

The online information landscape was also limited by direct bans on reporting on certain topics. For instance, after Jordanian security forces foiled a terror plot and arrested members of a terrorist cell in the northern city of Irbid in March 2016, the State Security Court issued a statement that banned

28 UN General Assembly, Human Rights Council, Report of the Working Group on the Universal Periodic Review, January 6, 2014, http://bit.ly/1FlG39f.

29 Article 19, "Jordan: Websites Blocking Order Must be Revoked Immediately," June 6, 2013, accessed February 3, 2014,http://bit.ly/1JQyooW.

30 Amman Net "Udwan: Blocking the Websites is against the Democratic Empowerment," Jordan News Agency, June 3, 2013, accessed February, 3 2014. http://bit.ly/1xXFNhe.

31 Reporters Without Borders, "International Free Expression Groups Call For An End To Internet Censorship In Jordan," October 8, 2013, accessed February 3, 2014, http://bit.ly/1KrbWyx.

32 Jordanian Media Monitor, Amended Press & Publications Law No. 32 of 2012, August 2013, http://bit.ly/1zqh8ig.

33 Jordanian Media Monitor, Amended Press & Publications Law No. 32 of 2012, August 2013, http://bit.ly/1zqh8ig.

34 In a discussion about the impact of website licensing and the PPL, publisher of news website JO24 Basel Okour said that they stopped allowing comments on their website in protest of the law and to protect the privacy of their readers. See "An Open Meeting at 7iber to Discuss the State of Online Journalism After the Website Registration Requirement," [in Arabic], YouTube video, 1:43:44, posted by Jordan Days, December 8, 2014, https://www.youtube.com/watch?v=MjUkvuRcBlI.

35 Center for Defending Freedom of Journalists, "Dead End: Media Freedom Status in Jordan", May 17, 2015, http://bit.ly/20DOvwc.

36 "DPP Brings Down Media Freedom in Jordan," Al Araby Al-Jadeed, May 3, 2014, http://bit.ly/1Nd4opP.

37 Rana Sabbagh, Facebook post, August 20, 2014, https://www.facebook.com/rana.sabbagh.777/posts/10152655581815903?pnref=story

all media from publishing information on the incident.[38]

On April 6, 2015, the head of the Media Commission sent a memo to all news websites stating that "websites should refrain from publishing or broadcasting any articles or military information without getting this news or information from official sou ces in the Armed Forces."[39] Months earlier, on November 26, 2015, the Armed Forces appointed for the fi st time an official spo esperson, following increased media coverage of Jordan's participation in the U.S.-led coalition against IS militants.[40] However, this did not result in increased transparency or access to information from the armed forces, as the number of comments and statements made by this spokesperson regarding the war on IS was only four, and he did not make any statements regarding Jordan's participation in the Saudi-led coalition against Yemen.[41]

Spotlight on Marginalized Communities

Freedom on the Net 2016 **asked researchers from India, Indonesia, Kenya, Kyrgyzstan, Jordan, Mexico, Nigeria, and Tunisia to examine threats marginalized groups face online in their countries. Based on their expertise, each researcher highlighted one community suffering discrimination, whether as a result of their religion, gender, sexuality, or disability, that prevents them using the internet freely.**

In Jordan, Khalid Abdel-Hadi highlighted discrimination the LGBT community face online.[1] The study found:

- Homosexuality is legal in Jordan, but the LGBT community remains subject to discrimination and prejudice. LGBT Jordanians are therefore often torn between their sexualities and their identities as Muslim Arabs. Although there are no official legal measures taken against LGBT bloggers or journalists who cover LGBT issues objectively, they face the same discrimination.
- Portrayals of LGBT people in the media often reflect misinfo mation, stereotypes, and sensationalism. Headlines can be particularly provocative online, since many websites deliberately use LGBT themes as clickbait to attract viewers and advertising revenue. Other online news portals will pick up the story, sharing inaccurate information and harmful stereotypes with thousands of people, and ultimately putting many LGBT individuals at risk.
- Jordanian officials will not incentivize local media o create LGBT positive content due to the prevailing anti-LGBT sentiment among their constituents. Changes in content will have to come from small, independent media that can be distributed online, like blog posts, comics, and short videos. Internet freedom is therefore central to the future of LGBT rights in Jordan.

1 Khalid Abdel-Hadi, research paper, October 2016, on file with F eedom House.

Facebook and YouTube are still among the top fi e visited websites in Jordan.[42] As of April 2016, 89 percent of all social media users in Jordan used Facebook, while 71 percent used WhatsApp.[43] State officials, including the oyal Hashemite Court,[44] the Queen, the Crown Prince,[45] and Prince Hassan,[46]

38 "Gag Order Bans Coverage of Irbid Terror Cell News", Assabeel, March 6, 2016, http://bit.ly/22wn8n3

39 The researcher obtained a copy of the official memo

40 "Colonel Mamdouh Al-Ameri Appointed Official Spo esperson of the Army", Al-Ghad, November 26, 2014 http://bit.ly/1Hlhzwv.

41 Omar, Mohammad, "Media and Propaganda: The Triumph of Propaganda and the Demise of the Press," 7iber, May 28. 2015 http://bit.ly/1ezV8x9.

42 Alexa, "Top Sites in Jordan," accessed on August 17, 2016, http://www.alexa.com/topsites/countries/JO.

43 "Facebook, Whatsapp Overshadow Twitter in Jordan's Social Media Sphere," Jordan Times, April 13, 2016, http://bit.ly/2bBODMQ.

44 Royal Hashemite Court Instagram Page, http://instagram.com/rhcjo.

45 King Abudullah II Bin Al Hussein Instagram Page, http://instagram.com/alhusseinbinabdullahii .

46 Prince Majlis El Hassan Twitter Page, https://twitter.com/majliselhassan.

have established social media accounts to communicate with the public. Queen Rania is by far the most popular of these accounts, with more than 5.3 million followers on Twitter and over 600,000 on Instagram.[47] She was, in fact, referred by *Forbes* Middle East magazine as "The Queen of Social Media."[48] Among government officials, Fo eign Minister Nasser Judeh has 124,000 Twitter followers. [49]

Digital Activism

In the past year, activists have used social media to advocate for a host of political, economic and social issues.

In late February 2016, students of the University of Jordan staged a sit-in against a decision to raise tuition fees at Jordan's oldest university.[50] Students used social media to mobilize their colleagues, share updates, and draw media attention to their cause. With the popular hashtag "Open Sit-In" (Al I'tesam Al Maftouh in Arabic), news of the protests went viral and thousands of Jordanians expressed their support.

Throughout 2015, a campaign titled "*Ma'an Nasel*" (which literally translates into "Together We Arrive") sought to advocate for better public transportation services. In addition to the campaign's organized action on the ground, commuters were asked to send videos that captured their experiences with public transportation, which were later uploaded and shared on social media during peak hours. According to the organizers, these videos were part of a wider "electronic demonstration" that brought together voices from a diverse base of users and called for change.[51]

On May 2, 2015, activist Reem Al-Jazi wrote an op-ed to protest the fact that hospitals require the approval of the father or a male guardian before admitting a child, even for emergency procedures, and do not acknowledge the mother.[52] Her article went viral and sparked a social media campaign petitioning parliament to amend Article 123 of the Civil Law that only grants guardianship to the father or the paternal grandfather or uncle.[53]

Violations of User Rights

The passage of a new cybercrime law led to a significant uptick in detentions and prosecutions of journalists. Generally, free speech is not protected online, with journalists, political activists, and ordinary users facing arrest and possible prosecution if they overstep the boundaries of acceptable speech. Strict penalties for criminal defamation against public authorities, both foreign and domestic, remain a prominent concern.

47 Queen Rania Al Abdullah Twitter Page, https://twitter.com/QueenRania; Queen Rania Al Abdullah Instagram, http://bit.ly/1iVLx62.

48 Abderrahim Etouil, "Queen of Social Media," Forbes Middle East, July 1, 2011, http://bit.ly/1KMPUv0.

49 Nasser Judeh Twitter Page. https://twitter.com/nasserjudeh?lang=en

50 "UJ protesters end protest after board slashes fees", Jordan Times, April 7, 2016 http://bit.ly/1V1fkKY.

51 Phone Interview with the author in April, 2016.

52 Reem Al Jazi, "Women: Full Responsibilities and Stolen Rights," [in Arabic] Khaberni, May 2, 2015 http://bit.ly/1SVFrNV.

53 Reem Al Jazi, "Petition my son's life is my responsibility," May 2015, http://chn.ge/1SBn85R.

Legal Environment

In June 2015, the amended Cybercrime Law No 27 came into effect with at least one provision that poses a serious threat to online freedom. According to Article 11 of the law, internet users can face a jail term of no less than three months and a maximum fine f JOD 2,000 (US$ 2,800), if they are found guilty of defamation on social media or online media outlets. In practical terms, this means journalists face harsher penalties online than in print media, since the Press and Publications Law prohibits the jailing of journalists. In 2015, the Law Interpretation Bureau issued a ruling that Article 11 supersedes other legislation, rendering journalists' immunity that is safeguarded by the Press and Publications Law irrelevant.[54] Thus, journalists may now be tried for print articles if those articles appear online.[55]

In March 2016, a group of journalists and activists launched a campaign to repeal Article 11, titled "Talking Is Not a Crime," which they perceive as "unconstitutional" as it undermines the freedom of expression safeguarded by the Jordanian constitution.[56] According to the Center for Defending Freedom of Journalists, seven journalists and activists have been detained since the passage of the amendment.[57]

In September 2011, responding to public discontent, constitutional amendments were introduced to strengthen checks and balances and ensure greater protections for human rights.[58] Several constitutional amendments touched directly or indirectly on internet freedom. Specificall , terms such as "mass media" and "other means of communication," which likely encompass online media, were added to provisions that protect freedom of expression and concomitantly allow for its limitation during states of emergency (Article 15). With regard to the right to privacy, judicial approval was added as a precondition for censorship or confiscation f private communications (Article 18).[59] Despite the passage of an Access to Information Law in 2007, a number of restrictions remain on requesting sensitive social and religious content.[60]

Beyond these constitutional protections, several laws that hinder freedom of expression and access to information remain on the books. These include the 1959 Contempt of Court Law, the 1960 penal code, the 1971 Protection of State Secrets and Classified Documents La , the 1992 Defense Law, the 1998 Jordan Press Association Law, and the 1999 Press and Publications Law. Defamation remains a criminal offense under the penal code. Amendments to the press law enacted in 2010 abolished prison sentences for libel against private citizens (as opposed to public officials). Ho ever, the same bill increased fines and jail sen ences for defaming government officials o up to JOD 10,000 (US$14,000) and 3 to 12 months imprisonment.[61]

54 International Press Institute, "Jordan's Online Media at stake", 2015, http://bit.ly/1SCa4qQ.

55 Daoud Kuttab, "Losing the Arab Spring accomplishments?," Jordan Times, March 9, 2016, http://bit.ly/1oXWIgS.

56 "Jordan: Talking is Not a Crime.. A Campaign to Repeal Article 11 of Cybercrime Law", Al Araby Al Jadeed [in Arabic], March 5, 2016 http://bit.ly/1T4jjTR.

57 Maher Shwabkeh, "a Campaign in Jordan to Protect Freedoms", [in Arabic], Al Hayat, April 3, 2016, http://bit.ly/1WrZ5GI.

58 The Law Library of Congress, "Jordan: Constitutional Law Court Newly Established in Jordan," news release, December 3, 2012, accessed June 26, 2013, http://1.usa.gov/1V0VPTH.

59 Constitution of Jordan, January 1, 1952, http://www.kinghussein.gov.jo/constitution_jo.html.

60 For example, the law bars public requests for information involving religious, racial, ethnic, or gender discrimination (Article 10), and allows officials o withhold all types of classified info mation, a very broad category (Article 13) see, Arab Archives Institute, "Summary of the Study on Access to Information Law in Jordan," June 2005, http://www.alarcheef.com/reports/englishFiles/accessToInformation.pdf.

61 Jordan Media Strengthening Program, Introduction to News Media Law and Policy in Jordan, May 2011, pg 38, http://bit.ly/1F79kKt.

The Press and Publication Law, amended in 2012, bans the publication of "material that is inconsistent with the principles of freedom, national obligation, human rights, and Arab-Islamic values."[62] Article 38 of the PPL also prohibits any "contempt, slander, or defamation of or abuse of" religions or prophets. The same article prohibits the publication of any material that is defamatory or slanderous of individuals who are also protected by the same law against "rumors" and "anything that hinders their personal freedom."[63] Journalists, website owners, and editors-in-chief face a fine f JOD 5,000 (US$7,500) if found to violate the law. In addition, civil defamation suits against private individuals can result in fines f between JOD 500 to 1,000 (US$700 to 1,400).[64]

In early 2014, a law was passed to limit the powers of the quasi-military State Security Court, before which citizens and journalists could be tried for crimes related to freedom of expression, to only terrorism, espionage, drug felonies, treason, and currency counterfeiting.[65] Worryingly, amendments to the antiterrorism law passed in mid-2014 essentially reversed many of the advances made in the above-mentioned law by expanding the definition f "terrorism" to include broader offenses.[66] In addition to more legitimate offenses such as attacking members of the royal court or provoking an "armed rebellion," the definition f terrorist activities now includes any acts that "threaten the country's relations to foreign states or expose the country or its citizens to retaliatory acts on them or their money," an offense that had already been listed in the penal code.[67] The law also explicitly penalizes the use of information and communication technologies (ICTs) to promote, support, or fund terrorist acts, or to subject "Jordanians or their property to danger of hostile acts or acts of revenge."[68]

Prosecutions and Detentions for Online Activities

Several journalists and activists have been detained because of their online activities. On April 22, 2015, journalist Jamal Ayoub, chief website editor Osama Ramini, and general manager Hassan Safirah f *Al Balad* were all arrested and charged with "disturbing relations with a foreign state" under the anti-terrorism law, among other charges. Ayoub had written an article criticizing Saudi Arabia's intervention in Yemen.[69] Charges were later changed to "insulting a foreign state and its army" and Ayoub was sentenced to four months in prison, while Ramini and Safirah ere both sentenced to three months.[70] Ramini was again detained in October 2015 after publishing news about a public school located in al-Tafileh go ernorate in which all students failed to pass the Tawjihi (national exam in Jordan).[71]

62 The Press and Publications Law 1998 amended by Law No. 32.

63 Law number (32) 2012. Amendments to The Press and Publications law for the Year 1998 (8), Article 38, clauses A, B, C & D.

64 The Press and Publications Law 1998 amended by Law No. 32.

65 Human Rights Watch, "Jordan: End Trials of Persecutors Undermining Regime," October 29, 2013, http://bit.ly/1hEq94a.

66 Human Rights Watch "Jordan: Terrorism Amendments Threaten Rights," May, 17, 2014, http://bit.ly/Rhgpzz, and "Royal Endorsement of Anti-Terrorism Law,"[in Arabic] Gerasa News, June 1, 2014, http://bit.ly/1N5YSnh.

67 Anti-Terrorism law –No 18 2014 Article 3 (b), http://bit.ly/1trDOKp.

68 Reporters Without Borders, "King urged to repeal draconian changes to anti-terrorism law," June 16, 2014,http://bit.ly/1UvoACc.

69 Human Rights Watch, "Jordan: Events in 2015", http://bit.ly/1Sg2tUT.

70 "State Security Court Rules in Al Balad's Case". Al Balad News Website. October 29, 2015: http://bit.ly/2bvDviL.

71 Mohammad Ghazal, "Al Balad website's chief editor detained over violating e-crimes law," Jordan Times, October 20, 2015, http://www.jordantimes.com/news/local/al-balad-website%E2%80%99s-chief-editor-detained-violating-e-crimes-law%E2%80%99, and "Ramini detained for 14 days", Assabeel, October 21, 2015, http://bit.ly/1qRVINk.

On June 30, 2015, Jordanian authorities arrested activist Ali Malkawi,[72] who in a Facebook post criticized the stance of Arab and Muslim leaders towards the plight of Muslims in Burma. Acquitted from "disturbing relations with a friendly state," Malkawi was instead convicted of "lengthening the tongue" and sentenced to three months in prison, but was later released after paying a fine [73]

In July 2015, columnist Jihad Muhaisen was detained over a Facebook post in which he said he criticized the democratic process in Jordan and joked he would become a Shiite. Muhaisen's contract with *Al-Ghad* daily newspaper and the Ministry of Political Development were both terminated after the incident. He faced charges of undermining the regime and lèse majesté. In October 2015, the State Security Court acquitted Muhaisen from the fi st charge, but found him guilty of lèse majesté and sentenced him to three months in prison. [74]

On August 18, 2015, Atef al-Joulani, editor-in-chief of *Assabeel* newspaper, was detained over an article titled "Gas cylinders… Are we more careful than the Italians?" The article criticized Jordan's Standards and Metrology Organization for rejecting a shipment of gas cylinders from India. Director General of the Organization, Haider Al-Zabin, filed a complaint against Joulani, who was detained over his opinion in accordance with the amended Cybercrime Law.[75] Joulani was later released on bail, but the court had not ruled on his case.

In September 2015, satirist Omar Zorba, who is very popular on Jordanian social media, was detained over a Facebook post that criticized the lavish wedding of a former prime minister's son.[76] He was sued again in early 2016 for mocking a Jordanian TV presenter online under the Cybercrime Law.[77] Zorba claimed that both the ex-premier and the TV presenter dropped the cases.

Shortly after this incident, television presenter Tareq Abu Al Ragheb was detained over a Facebook post in which he was accused of offending another religion and "threatening the peaceful co-existence in the Kingdom," although according to him, the charge was for a post seen as "non-objective and full of libel and slander."[78] He was released from jail after a week.

Dhaigham Khreisat, Diyaa Khraisat, and Ramez Abo Yousef from *Al Hayat* weekly newspaper were detained in November 2015, after allegedly insulting the director of the Legislation and Opinion Bureau, Nufan Ajarmeh, in an article published on their website.[79] Ajarmeh had caused controversy earlier when the Bureau ruled that the amended Cybercrime Law could be applied to online journalists. Ajarmeh was later accused of slander and defamation by Tareq Abu Al Ragheb (see above case) for a Facebook post in which Ajarmeh criticized those who opposed government moves to raise gas

72 The Arabic Network for Human Rights Information, "Jordan: ANHRI Demands Release of Blogger "Ali Mohamed Al-Malkawi," July 30, 2015, http://bit.ly/1RUrwuN.

73 "Young Man Given a Prison Sentence Over a Facebook Post," Ya-Media, March 13, 2016, http://bit.ly/2bkFkRd.

74 "Court Rules in Jihad Muhaisen's Case," Jadal News, October 25, 2015, http://bit.ly/2bxdEWR.

75 The Arabic Network for Human Rights Information, "Jordan: Curb on Freedom of Expression… Journalist Atef Al-Joulani Detained for a Critical Article," August 19, 2015, http://bit.ly/1RVJhd0.

76 Omar Obeidat, "Former premier drops case against web-based satirist charged with defamation," Jordan Times, September 16, 2015, http://bit.ly/1p0A8nZ.

77 Suzanna Goussous, "Social media activist sued for 'mocking' Jordan TV presenter over census song," Jordan Times, January 4, 2016, http://bit.ly/1ShwOCq.

78 "TV presenter detained over "a Facebook post," Jordan Times, November 3, 2015, http://bit.ly/1WsbnP8.

79 "Three journalists released on bail after detention over alleged slander," Jordan Times, November 19, 2015, http://bit.ly/1SCea2h.

cylinder prices and car licensing fees as "animals and their waste" without mentioning names.[80]

In December 2015, the State Security Court sentenced Iyad Qunaibi, a prominent Islamist activist, to two years in prison for several nonviolent Facebook posts. Qunaibi, a key figu e in the Salafism movement in Jordan, criticized several acts that he deemed "un-Islamic" in Jordan, including a gathering of homosexuals attended by the American ambassador in Amman. The sentence was later reduced to one year.[81]

In June 2016, Muslim scholar Amjad Qourshah, who is a prominent and controversial figu e in Jordan, was arrested over a YouTube video in which he questioned Jordan's role in the war against the Islamic State (IS) militant group. Published in 2014, the video showed Qourshah in his private car criticizing Jordan's policy and participation in the war against IS, claiming that Jordan should instead target drug dealers, who outnumbered terrorists in his opinion.[82] Although many Jordanians strongly oppose Qourshah's views, including his anti-Christian and anti-Shiite comments, many expressed disagreement over his detention.

Political tensions have also resulted in the prosecution of Jordanians affilia ed with the Muslim Brotherhood. In February 2015, the deputy leader of the Muslim Brotherhood in Jordan, Zaki Bani Irshaid, was sentenced by the State Security Court to 1.5 years in prison with hard labor.[83] The Court of Cessation upheld the ruling in April 2015.[84] He had been charged with "harming Jordan's ties with a friendly state" under the amended antiterrorism law after he published a post on his Facebook profile criticizing the AE government and accusing it of sponsoring terrorism and supporting the "Zionist agenda."[85]

Members of parliament (MPs) have also faced criticism for their online activities. In September, 2015, MP Raed Hjazin had to delete a post a few minutes after sharing it, which was deemed offensive to Khalid Bin Waleed, one of Prophet Muhammad's companions. Consequently, lawyer Abdul Jabar Abu Qulah filed a lawsuit against him for "inciting sectarianism"[86]

Surveillance, Privacy, and Anonymity

Since the passage of amendments to the antiterrorism law in 2014, a number of people have been arrested and put on trial at the State Security Court for private messages they posted on WhatsApp. While there is no concrete evidence that the government systematically monitors and intercepts private communications, defense lawyers say that material obtained from mobile phones or laptops is often obtained without a court order, which cannot be legally used as evidence.[87] In October 2013, Ayman al-Bahrawi was accused of "lengthening the tongue" and "insulting" foreign heads of state in private WhatsApp messages found on his mobile phone.

80 "Legislation and Opinion Bureau Director Sued Over Facebook Post," Jordan Times, December 7, 2015, http://bit.ly/2b0Jg8N.

81 "Jordan Reduces Sentence Against Salafi P eacher," Al Jazeera, May 16, 2016, http://bit.ly/2bil0wy.

82 "Muslim scholar detained 'over comments on Jordan's role in anti-Daesh war'," Jordan Times, June 15, 2016, http://bit.ly/2bkHKPP.

83 "Muslim Brotherhood leader sentenced to 1.5 years in jail", Jordan Times, February 15, 2015, http://bit.ly/1EbfNMS.

84 "Cessation Court Overturns Bani Irshaid's Appeal of State Security Court Ruling,"[in Arabic] Al-Ghad, April 15, 2015 http://bit.ly/1Fk7y6l

85 Rana F. Sweis, "Jordan Arrests Muslim Brotherhood Official O er Criticism of United Arab Emirates", The New York Times, November 21, 2014, http://nyti.ms/1B3k9FC.

86 "MP to be tried over Facebook post on prophet's companion," Jordan Times, October 22, 2015, http://bit.ly/2bHPrRy.

87 Al-Masri, "Anti-Terrorism Law: Between Prosecuting Terrorist Ideology and Dissident Opinion."

A recent report titled "Digital Privacy in Jordan: Perceptions and Implications among Human Rights Actors",[88] showed individuals still feared being blackmailed, using personal information that is available publicly or privately. In addition, the majority of participants in the research mentioned that the Intelligence Department was the entity most likely to threaten access to their private communications. Although participants seemed aware of surveillance, very few of them reported using technical tools to protect their data. Instead, they chose not to make their data public or share it electronically, and preferred to have face-to-face interaction with their sources if the information is sensitive or erased all traces of their names on their devices.[89] Jordanians have a long-standing belief that "someone is listening in" when it comes to their phone calls. Expectedly, this attitude has passed naturally to the internet, where it is believed that security services closely monitor online comments, cataloging them by date, internet protocol (IP) address, and location.

Furthermore, clauses within mobile phone contracts give Jordanian companies the right to terminate services should customers use it in any way "threatening to public moral or national security."[90] Cybercafes, where users might otherwise write with relative anonymity, have been subjected to a growing set of regulations in recent years. Since mid-2010, operators have been obliged to install security cameras to monitor customers, who must supply personal identification info mation before they use the internet. Cafe owners are required to retain the browsing history of users for at least six months.[91] Authorities claim these restrictions are necessary for security reasons. Although enforcement is somewhat lax, the once-thriving cybercafe business is now in decline due in part to the restrictions, as well as increased access to personal internet connections.

Intimidation and Violence

There were no reported instances of physical violence against internet users for their online activities during the coverage period. A climate of fear and intimidation remains, however, for those working in online media. The last reported incident occurred on July 17, 2012, when unknown perpetrators raided the offices f the online news site *Watan*, stealing documents and damaging equipment.[92]

On September 25, 2016, Jordanian writer Nahed Hattar was shot dead outside of a courthouse in Amman, where he was due to face trial for publishing a satirical cartoon deemed "offensive to Islam" on his Facebook page. The caricature depicted a bearded man in heaven, sleeping with women and giving orders to God to bring him wine and cashews.[93] Hattar, a Christian who had expressed his support for the Syrian president Bashar al-Assad, explained the cartoon "mocks terrorists and their concept of God and heaven."[94] Thousands of Jordanians expressed their solidarity with Hattar's family,

88 Information and Research Center at King Hussein Foundation & 7iber, "Digital Privacy in Jordan: Perceptions and Implications among Human Rights Actors", 2015 http://bit.ly/1WrGA51.

89 Information and Research Center at King Hussein Foundation & 7iber, "Digital Privacy in Jordan: Perceptions and Implications among Human Rights Actors", 2015 http://bit.ly/1WrGA51.

90 Eye on Media, "Declining Freedom, Restrictions on the Internet and a Financial Crisis," December 25, 2013, http://bit.ly/1KN2GcQ.

91 International Freedom of Expression Exchange, "Cyber crime law attacks free expression; Internet cafés monitored," news release, August 18, 2010, http://www.ifex.org/jordan/2010/08/18/cyber_cafe/; "Interior requires internet cafes to install surveillance cameras and keep internet visits for months" [in Arabic], Saraya News, June 3, 2010, http://www.sarayanews.com/object-article/view/id/23211.

92 "Report: increasing attacks on journalists in Jordan, mostly from the security," [in Arabic] Satel News, July 8, 2012, http://bit.ly/15WAUGB.

93 "Writer turns himself in after cartoon sparks outrage". Jordantimes. August 13, 2016. http://bit.ly/2bfjr2d.

94 "Jordan: Nahed Hattar shot dead ahead of cartoon trial," Al Jazeera, September 26, 2016, http://www.aljazeera.com/news/2016/09/jordan-nahed-hattar-shot-dead-cartoon-trial-160925080745317.html.

demanding an end to hate speech and incitement online.

Technical Attacks

Over the past year, incidents of cyberattacks against bloggers and staff of online news websites decreased in severity compared to previous years. In 2012, the webpages of the news sites *Khaberni* and *Al Ain* were hacked; the site of the Jordanian rap group Ahat was also hacked on September 15, 2012.[95] In February 2011, one of the country's most popular news websites, *Ammon News,* was hacked and temporarily disabled after its editors refused to comply with security agents' demands to remove a statement by 36 prominent Jordanian tribesmen, in which they called for democratic and economic reforms. Among other actions, the hackers deleted the joint statement, which were politically sensitive given the groups' historic support for the monarchy.[96]

95 Skeyes Center for Media and Cultural Freedom, Press and Cultural Freedom in Lebanon, Syria, Jordan and Palestine – Annual Report 2012, 2013, http://foundationforfuture.org/en/Portals/0/Grantees%20Publications/SKeyes%202012%20Annual%20Report%20EN.pdf.

96 Committee to Protect Journalists, "In Jordan, website hacked after running sensitive statement," February 9, 2011, http://cpj.org/x/416b.

Freedom House

Kazakhstan

	2015	2016
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	14	14
Limits on Content (0-35)	23	23
Violations of User Rights (0-40)	24	26
TOTAL* (0-100)	**61**	**63**

* 0=most free, 100=least free

Population:	**17.5 million**
Internet Penetration 2015 (ITU):	**73 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- Users reported difficulties in accessing social media and communication apps during widespread land reform protests (see **Restrictions on Connectivity**).
- Authorities blocked access to entire content hosting platforms, including Tumblr and Sound Cloud, in an effort to block extremist content (see **Blocking and Filtering**)
- The regulator adopted a new internet monitoring technology, the Automated System of Monitoring the National Information Space (see **Content Removal**).
- A National Security Certifica e was introduced, technology which will potentially allow authorities greater access to user data (see **Surveillance, Privacy, and Anonymity**).

Introduction

Internet freedom declined in Kazakhstan in 2015-2016 with lengthy prison sentences handed out to social media users and the introduction of an invasive "National Security Certifica e," which may allow greater surveillance online.

Regulation of the internet in Kazakhstan is heavily influenced by the authoritarian go ernment, which blocks websites, uses the legal system to stifle f ee speech online, and is developing a complex infrastructure to control internet traffic. Despi e increases in the numbers of people accessing the internet, with improved affordability and speed, internet freedom is deteriorating.

Within the past year, social media and communications apps have been cut off on several occasions, including during the widespread land reform protests in May 2016. Numerous blockings were recorded, affecting entire international content-sharing platforms and critical domestic news sites. The list of agencies authorized to issue orders for ISPs to block certain resources without a court decision has been expanded to include the regulator, and access providers themselves have been made responsible for monitoring and fil ering illegal content.

Kazakhstani authorities use criminal charges against social media users in an effort to silence dissident expression and punish online mobilization, issuing prison sentences of up to fi e years. Meanwhile, the government introduced a "National Security Certifica e," software which must be installed on all devices, and is likely to increase the government's capacity to intercept user communications and data.

Obstacles to Access

The government of Kazakhstan continued to work on improving ICT infrastructure through direct investment in the national operator, Kazakhtelecom, and by facilitating market competition and private ownership in the telecommunications industry. However, authorities restricted access to social media platforms on numerous occasions throughout the coverage period, as well as initiating temporary localized internet outages.

Availability and Ease of Access

Internet access has grown significantly in Kazakhstan o er the past few years, increasing from a penetration rate of 18 percent in 2009 to almost 73 percent in 2015, according to the International Telecommunication Union (ITU).[1] Official fig es showed some variation. In September 2014, officials claimed that internet penetration had exceeded 75 percent,[2] though in early 2016 the government's estimate stood at 72.9 per cent.[3] The Ministry of Investments and Development reported that 82.2 percent of households had an internet connection as of January 2016. The number of mobile and fi ed-line broadband connections reached 10.2 million and 2.1 million users respectively.[4]

1 International Telecommunication Union, "Percentage of Individuals Using the Internet," 2000-2015, http://bit.ly/1cblxxY.

2 "The number of Internet users has reached 12 million," [in Russian] *Kazinform*, September 19, 2014, http://bit.ly/1Zlc3Xf.

3 Official esponse an electronic information request on submitted to the eGov.kz portal, [in Russian] http://bit.ly/29lIPI5, accessed on July 9, 2016.

4 Statistical data of the Ministry of Investments and Development [in Russian], posted on February 5, 2016, accessed on July 9, 2016, http://bit.ly/29xF7tX.

The mobile phone penetration rate grew to 187 percent in 2015, according to the ITU.[5] According to Budde, a telecommunications research and consultancy site, overall mobile subscriber growth rates have declined due to market consolidation, reaching around 31 million subscribers in 2016. Mobile broadband penetration rates reached 61 percent in the same period.[6]

Official statistics do not p ovide data on the number of urban versus rural connections, but access is more limited in rural areas, where 45 percent of the population resides. Almaty—the most populous city and the business and cultural center of Kazakhstan—accounts for more than 35 percent of internet users, and for more than 55 percent of the ICT industry's revenue.[7] A study by TNS Central Asia showed that 67.5 percent of active internet users reside in big cities.[8] Most people access the internet from their mobile devices and at home. Free access is available in various public places.

Access is distributed relatively evenly across Kazakhstan's multiethnic communities. The competition between the Kazakh language and Russian, still widely used by many urban residents as a part of the Soviet legacy, has an impact on access. All public institutions are required to provide at least two language versions on their website, and many private sector actors follow this example. However, there is much more domestic content available in Russian than in Kazakh, especially in alternative news coverage online; social media discussions are also held primarily in Russian.

Kazakhtelecom introduced a record 120 Mbps connection speed in 2015.[9] Its principal rival in the retail sector, Beeline-Kazakhstan, offers speeds up to 100 Mbps.[10] The average connection speed, estimated by the Akamai "State of the Internet" Report, was 5.9 Mbps in the third quarter of 2015.[11]

Both state and private ISPs have reduced their tariffs in the coverage period. Kazakhtelecom's popular broadband (50- 120 Mbps) subscriptions currently cost between US $11 and US $18 per month; Beeline offers 20-100 Mbps contracts for between US$5 and US $12 per month. The advertised "maximum speed" refers to foreign traffic. Major ISPs ha e also removed traffic caps f om some of their packages. Mobile phone service prices have been dropping, with new competition between operators leading to more generous data packages. However, high inflation coupled with significan currency devaluation in 2015 caused average monthly incomes to shrink to US$345 in 2016, and access to the internet remains prohibitively expensive for many in Kazakhstan.[12]

Restrictions on Connectivity

The government imposes no restrictions on the bandwidth of access offered by ISPs, but it centralizes the infrastructure in a way that facilitates control of content and surveillance. Kazakhtelecom, through its operations and a number of subsidiaries, holds a *de facto* monopoly on backbone infrastructure; Beeline is the only independent backbone provider. The internet exchange point —a peering center, established by Kazakhtelecom in 2008—is meant to facilitate service among fi st-tier providers, but in 2010, it turned down Beeline's application to join the pool without giving any rea-

5 International Telecommunication Union, "Mobile-cellular telephone subscriptions, 2000-2015," http://bit.ly/1cblxxY.

6 "Kazakhstan - Telecoms, Mobile and Broadband," *Budde*, December 09, 2015, bit.ly/1Qic4TS.

7 "Revenue of enterprises providing internet access by regions as of January 2015," [in Russian] *Ranking*, February 24, 2015, http://bit.ly/1DNjp8a.

8 "Internet audience of Kazakhstan: User portrait and preferences," [in Russian] *Forbes.kz*, July 28, 2015, bit.ly/1RFwrzM.

9 Kazakhtelecom, "Results of activity in 2015," Press release, February 02, 2016, bit.ly/1PXAFli.

10 Beeline, Press Release, [in Russian] November 02, 2015, bit.ly/1TmtPYT.

11 Akamai, "Average connection speed," map visualization, *State of the Internet*, 2015, http://bit.ly/1WRjumM.

12 Mojazarplata, "Average Monthly Wages," [in Russian] accessed March 5, 2015,

son.[13] However, plans to create a new internet exchange point were announced in April 2016. The consortium behind the project, which was initiated by the regulator, includes both Beeline and Kazakhtelecom along with other major ISPs and mobile operators, and the State Technical Service.[14]

In 2012, amendments to the Law on National Security allowed the government to forcibly suspend telecommunications during anti-terrorist operations or the suppression of mass riots.[15] Further legislation was passed to compel private actors—websites, ISPs or mobile operators—to block or disconnect service at the government's request. Laws passed in 2014 authorize the state to shut down communication services at the discretion of the prosecutor general's office without a cou t order if "networks are used for felonious aims to damage the interests of individuals, society or state," including the dissemination of illegal information, calls for extremism, terrorism, mass riots, or participation in unauthorized public gatherings. This regulation could cover telephony, text messages, and instant messaging applications. The law makes either telecom operators or the State Technical Service responsible for the implementation of the prosecutor's order. In February 2015, the law was implemented to temporarily shut down internet and mobile phone services in South Kazakhstan province following the break out of ethnic violence in the region.[16]

Internet connections were subject to disruption within the coverage period. In August 2015, users in Aktau (Western Kazakhstan) were shortly disconnected form the internet on both Kazakhtelecom and mobile networks because of a cable breakage.[17] Access to certain social media platforms was reported at times during the coverage period, and a general slowdown of internet connectivity was reported during widespread land reform protests in May 2016, possibly indicating intentional throttling.

Additionally, an internet outage was reported in Aktobe, a city in Kazakhstan's North West, during a period of violence after the end of the coverage period, with the authorities cutting the town from the internet on June 5-6.[18] This hindered communications among residents and with the outside world during the unrest, in which 19 people were killed.[19]

ICT Market

The state owns 52 percent of Kazakhtelecom, the largest ISP in Kazakhstan through the sovereign wealth fund Samruk-Kazyna. Kazakhtelecom has an 85 percent share in the fi ed broadband internet market,[20] and fully or partly owns a number of other backbone and downstream ISPs. Beeline, by its own estimates, accounted for 13.1 percent of the broadband internet market in early 2015.[21] In

13 "Comment by Mr. Kemelbek Oishybaev, Beeline's executive, to the online Q&A session," [in Russian] *Yvision* (blog), accessed January 13, 2014, http://bit.ly/1jhBXKA.

14 **"**Peering center to be set up in Kazakhstan," [in Russian] *Profit.kz*, April, 2016, http://bit.ly/1TB3B2D.

15 "Республики Казахстан О национальной безопасности Республики Казахстан," [The Law on National Security] *Zakon*, July 10, 2012, http://bit.ly/1jfspR0.

16 Joanna Lillis, "Local Ethnic Conflict Exposes National ault Lines," *Eurasianet*, February 11, 2015, http://bit.ly/1AXDP1Z.

17 "Internet acts up in Aktau because of cable breakage," [in Russian], *Lada.kz*, August 10, 2015, bit.ly/1XHX6MP.

18 "Kazakhstan: Aktobe violence wrongfoots authorities," *Eurasianet*, June 6, 2016, http://www.eurasianet.org/node/79096.

19 "Death toll from Aktobe attack reaches 19: Kazakh police," *Reuters,* June 7, 2016, http://www.reuters.com/article/us-kazakhstan-shooting-toll-idUSKCN0YT0M3.

20 ""Kazakhtelecom secured its prevalence," [in Russian] *Forbes.kz*, October 20, 2015, bit.ly/1U5opRn.

21 Email interview with a Beeline representative, March 2015.

February 2016, regional business associations criticized the state's apparent tendency to favor Kazakhtelecom for government telecommunications contracts[22]

In late 2015 and early 2016, Kazakhtelecom sold its subsidiary Altel to Tele2-Kazakhstan, a private operator. This was a positive development in Kazakhstan's ICT market, increasing competition between service providers through privatization.[23] Altel previously held a monopoly over the 4G LTE network,[24] and had been receiving state funding as well as special treatment from the regulator.[25] During the coverage period, the regulator has introduced mobile number portability, which, as of January 2016, operators must provide to their clients free of charge.[26] The regulator also ended Altel's monopoly on 4G/LTE technology by offering additional frequencies to all other market players. [27]

In early 2016, there were four mobile telephone service providers, three of which use the GSM 3G standard (Kcell, Beeline, and Tele2). All the GSM operators are privately operated with foreign shareholders. In September 2015, TeliaSonera, the European telecommunications company that operates Kcell, announced that it would retreat from a number of post-Soviet markets, including Kazakhstan.[28] Its shares are expected to be taken back by Turkcell, which previously owned them.

Regulatory Bodies

The Committee for Communication, Informatization, and Information is the official body designa ed to hold regulatory, operational, and controlling functions over the internet, but it is not independent, since it operates under the Ministry of Investments and Development. The past year saw some reshuffling f various ministries and government bodies. In early May 2016, president Nazarbayev ordered the creation of the Ministry of Information and Communication to "monitor public opinion and all types of media, including internet and social media, in order to quickly identify and react to the most pressing problems."[29] Meanwhile, the Committee for Communication, Informatization and Information was reorganized into the Committee of State Control over Communications, Information and Mass Media, and will work on updates to Kazakhstan's law on mass media, including the internet. [30]

The Internet Association of Kazakhstan (IAK), established in 2009 in the form of a union of legal entities, claims to unite the country's internet community,[31] yet some of its former members question the group's independence, transparency, and non-profit status [32] IAK participates in discussions on

22 Yelena Ulyankina, "Entrepreneurs say authorities are lobbying for Kazakhtelecom's interests," [in Russian] *NV.kz*, February 22, 2016, http://bit.ly/1NZB5U6.

23 "Kazakhstan's second-tier mobile operators merge to enter the premier league," [in Russian], *Digital.Report*, November 05, 2015, bit.ly/216k5U1.

24 "Full-scale introduction of 4G in Kazakhstan is delayed," [in Russian], *Tengri News*, June 24, 2014, http://bit.ly/1GYUL83.

25 Prime Minister of Kazakhstan Karim Massimov: Official ebsite, "DBK to finance the 4G net ork expansion project in Kazakhstan," press release, December 24, 2014, http://bit.ly/1jfsYKD.

26 "Operators are ready to introduce MNP..." [in Russian], *Digital.Report*, December 29, 2015, bit.ly/1PCibFs.

27 "Kazakhstan lifts state monopoly on 4G," [in Russian], *Digital.Report*, January 13, 2016, bit.ly/1okzQIr.

28 "TeliaSonera to retreat from Central Asia," *Reuters*, September 17, 2015, reut.rs/20Baa6B.

29 "Nazarbayev ordered creation of the ministry of information and communication," [in Russian], *Vlast.kz*, May 5, 2016, http://bit.ly/1STpRCH.

30 "Committee for state control over communications, information and mass media established in Kazakhstan," [in Russian], *Tengrinews.kz*, http://bit.ly/29n3lSi.

31 Email interview with IAK president, Shavkat Sabirov, February 2016.

32 "Konstantin Gorozhankin talks Kaznet business and impotent state programs," [in Russian], *VoxPopuli.kz*, interview, May 21, 2015, bit.ly/1F1u3bJ.

draft laws concerning ICT use and, since 2014, has worked with the office f the prosecutor general on fighting child abuse online, com atting hate speech, trolling, content promoting suicide among teenagers, extremism, terrorism, and cyberfraud.

Since 2005, the government has required that any website in the top-level ".kz" domain zone be hosted on servers within Kazakhstan. The ".kz" domain is managed by the Kazakhstani Network Information Center (KazNIC) registry. The Kazakhstani Association of IT Companies administers domain names and regulates KazNIC tariffs. In January 2015, the Association doubled the minimum price of a .kz domain name. [33] In 2015, a law was passed granting the government the power to appoint both the registrar and the domain name administrator. Though the government has not made changes to the current appointments, some experts are concerned that this power may be subject to abuse.[34]

Limits on Content

The authorities have continued restricting content online, including during protests throughout the coverage period. Entire platforms hosting user-generated content have also been subject to periodic blocking, often without any public justification. The most frequent reason used to justify restrictions to online content is extremism; however, the courts review those applications in bulk and the proceedings are not transparent. The regulator has introduced an automated monitoring system to identify banned content. New legislative amendments force ISPs to monitor the online space for supposedly illegal content, with penalties if they fail to remove it.

Blocking and Filtering

The government possesses extensive legal powers to block online content. Websites and entire content hosting platforms were newly blocked during the coverage period. The authorities also restricted social media and communication apps, particularly during periods of unrest like the land reform protests of May 2016, hindering communication among citizens and distorting the flow f information.

According to the Mass Media Law, all internet resources, including websites and pages on social networks, are considered media outlets. Under 2014 amendments to the law, the public prosecutor is authorized to order service providers to block content without a court order. ISPs must conform to such requests until the website owner deletes the content in question and the law provides no space for an ISP to reject the order or for the website owner to appeal.[35] However, in January 2016, new amendments to the Mass Media Law were passed requiring authorities to seek a court decision before content can be blocked, but only for websites that have undergone voluntary registration with the regulator. Unregistered websites can be blocked based on the regulator's decision alone. In February 2016, the regulator said it was adopting an "Automated System of Monitoring the National Information Space" to uncover illegal content online (see Content Removal).

Three justices of the Saryarka District Court of Astana are designated to deal with cases related to

33 NazNIC, "About page" accessed on February 16, 2016, bit.ly/1mFfj04.

34 "Kazakh regulator to determine the registry of .kz zone," [in Russian] *Digital.Report*, March 7, 2016, http://bit.ly/24LccG7.

35 Diana Okremova "Online publications in Kazakhstan: Voluntary or Obligatory?" [in Russian], *Digital.Report*, January 21, 2016, http://bit.ly/1QLa3QC.

blocking online content.[36] Judges and prosecutors repeatedly display a lack of technical expertise, banning URLs of irrelevant websites like search engines. Websites can be blocked even in the absence of the defendant's representative; no further notification— o the public or the website owner—about why the website is blocked is required. The court issues frequent decisions to block websites, banning dozens at a time, mostly on the grounds of religious extremism.

Monitoring of online content is reportedly conducted by numerous authorities, including the National Security Committee, the Presidential administration, and even local administrations. The Committee for Religious Affairs under the Ministry of Culture and Sports evaluates websites for extremism. In January-November 2015, 900 cases of websites were submitted for the body's consideration. Of the 700 it reviewed, half were recommended for blocking.[37] This is nearly fi e times more than in 2014.[38]

In January 2016, users reported temporary difficulties accessing social media platfo ms for a number of hours. No official explanation was p ovided for these disruptions, though some speculate that the authorities were testing their capacity to shut down online communications.[39] Later in the year, authorities specifically estricted internet access and communication apps during periods of unrest and violence, hindering communication among citizens and distorting the flow f information. Significant blocking occur ed in May 2016, after unsanctioned rallies against land reform were organized through social networks. On the eve of the scheduled date, the authorities blocked major social networking sites and messengers. Users reported difficulties access social media apps, inclu - ing Facebook, Twitter, VKontakte, WhatsApp, Viber, and YouTube, between May 19 and May 23 2016.[40] A number of local independent online publications were blocked as well, including the Kazakh Service of RFE/RL and Uralskweek (West Kazakhstan).[41] Websites run by international media outlets reporting on the detention of protesters were also blocked, including Reuters. Users experienced difficulties accessing sea ch engines around this time.

Other platforms were temporarily disrupted based on court orders to limit access to extremist content:

- In early May 2015, SoundCloud, an international platform for sharing music and podcasts, was blocked because of one account that allegedly contained extremist materials by the Hizb-ut-Tahrir Islamist group. It was restored in late June.
- Vimeo, a global platform extensively used by professional videographers, was blocked in September and October 2015. A district court in Astana had authorized the blocking of Vimeo, along with a dozen other sites which were deemed to have been hosting extremist materials.[42] Dailymotion, another video-hosting platform, was also blocked, although it was not listed among the violators. Many people in Kazakhstan use sites like SoundCloud and Dailymotion in their professional lives.

36 Shavkat Sabirov, president of the Internet Association of Kazakhstan, said at the Roundtable "How to make internet safe for children" in Almaty, April 14, 2014.

37 "Users to be held liable for videos of executions," [in Russian] *Vlast.kz*, November 27, 2015, bit.ly/24cZv6I.

38 "55 websites were blocked in Kazakhstan…," [in Russian] *Zakon*, August 27, 2014, http://bit.ly/1AohB3j.

39 "Successful test of shutting down internet held in Kazakhstan," [in Russian] LiveJournal user *Ibrashkz*, January 16, 2016, bit.ly/1QiBIOC.

40 "Largest social networks and messengers temporarily shut down in Kazakhstan," [in Russian], *Tjournal.ru*, May 20, 2016, http://bit.ly/29mv1aw.

41 "Arrests and blocks," *Radio Azattyk*, May 21, 2016, http://bit.ly/29BfRnd.

42 "Vimeo.com blocked in Kazakhstan," [in Russian], *Tengrinews.kz*, September 22, 2015, bit.ly/1PI2E73.

- Tumblr.com was blocked by a court decision in October 2015, following the regulator's complaint about "extremist and pornographic blogs" hosted on the platform.[43]

The blocks came amid heightened official rhe oric against social media. In June 2015, President Nazarbayev publicly slammed social networking websites as a reason for the deterioration of spiritual and moral values among the youth in Kazakhstan.[44] In September 2015, a representative of the regulator claimed that most illegal information, including recruitment by terrorist groups, is disseminated in Kazakhstan via Facebook and YouTube.[45]

Other content was restricted without a clear explanation. Blogging platforms WordPress and Blogspot were reported to be inaccessible in December 2015 and January 2016. In January 2016, users reported temporary difficulties accessing social media platfo ms for a number of hours. No official explanation was provided for these disruptions, though some speculate that the authorities were testing their capacity to shut down online communications.[46] The authorities have repeatedly threatened to block access to social media ahead of elections, including ahead of the January 2016 parliamentary elections.[47]

On April 15 and from April 29 to May 1 2016, users reported disruptions in accessing Google services, including Search, YouTube, and PlayMarket.[48] Some observers speculated that the disruptions to Google's PlayMarket may have been related to attempts to restrict access to Meduza.io, an independent online Russian news outlet which is banned in Kazakhstan but had made its content available through an app on PlayMarket. Since late 2015, users have separately reported problems with downloading attachments in Gmail.

Other websites were also intermittently or permanently unavailable during the coverage period without clear reason. These include the Open Society Foundation website, online resource centers for journalists IJNET.org and IFCJ.org, Archive.org, Pinterest, movie database iMBD.com, cloud storage Mega.nz, photo hosting service Flickr.com, UrbanDictionary.com, Wikia.com, online library lib.ru, online petition website Avaaz.org, Snapchat, and international media, including the British *Daily Mail*, Russian Meduza.io, Ferghananews.com, and Echo Moskvy. Kazakhstan blocks adult pornography, and other content about sexuality. In summer 2015, users reported that the LGBTI dating website BlueSystem had been blocked.

The lack of transparency surrounding website blocking was notable in two cases. ISPs blocked prominent independent online publications Ratel.kz and Zonakz.net between September 2015 and February 2016, though both service providers and the relevant authorities denied initiating the block. Access was restored without explanation after the two websites, together with major media NGOs, urged the general prosecutor to initiate a criminal case for violating their constitutional right to freedom of information. The Organization on Security and Co-operation in Europe (OSCE) criticized the blocking in a special address to Kazakhstan's Foreign Ministry.[49]

43 "Tumblr is blocked for propaganda of extremism and pornography," [in Russian] *Tengrinews.kz*, April 11, 2016, http://bit.ly/1NFz8RT.

44 "Nazarbayev slams social networks, Internet, pseudo-culture," *Tengrinews.kz*, June 10, 2015, bit.ly/1WuAtKw.

45 "Social media used by terrorists to recruit Kazakhstani citizens," [in Russian] *Khabar.kz*, September 28, 2015, http://bit.ly/23ckXWf.

46 "Successful test of shutting down internet held in Kazakhstan," [in Russian] Livejournal user *Ibrashkz*, January 16, 2016, bit.ly/1QiBIOC.

47 "Social media can be blocked during the campaign," [in Russian], *Otyrar.kz*, February 20, 2016, bit.ly/1oXxvUu.

48 "Why Youtube is not working in Kazakhstan" [in Russian] *Yvision* (blog), May 1, 2016, http://bit.ly/1THVEZy.

49 "OSCE asks Astana to unblock websites," [in Russian], *Azattyq.org*, October 01, 2015, bit.ly/1OhUaPV.

Separately, in April 2016, the regulator banned InDriver, a popular application that directly connects drivers and potential passengers. The authorities claimed the app violated legislation that governs taxi services, and ordered service providers to block its website. Notably, four days after the problem was fi st reported, Asset Issekeshev, the minister of investments and development, met representatives of Uber, which is expected to launch in Kazakhstan in 2016. [50] The blocking took place without a proper court decision, sparking concerns over possible preferential treatment being given to other businesses offering similar services.[51]

Users wishing to circumvent censorship are increasingly using virtual private networks (VPNs).[52] Since early 2011, some anonymizing sites and proxy servers have been blocked. In the past, cybercafes were forced to delete or block circumvention tools. In June 2015, media reports said that the authorities were blocking such tools with renewed intensity, citing a court decision dated September 10, 2014 that banned "the functioning of networks and/or means of communication that can be used to circumvent the technical blocking by ISPs."[53] The Tor Project's official ebsite is intermittently inaccessible from Kazakhstan.[54] It is difficult o verify how far the Tor network itself is affected by blocking, but according to the public records of its use, the number of connections to the service's "relay" nodes from Kazakhstan dropped by about 40 percent in October 2016. The number of users connecting via "bridge relays," which are not listed publically and are more difficult o block, increased by about 800 percent. This pattern often indicates a censorship event.

Content Removal

The authorities used varied means to enforce the removal of content online in the coverage period, including pressure on critical online outlets to take down specific con ent and requests to international social media platforms.

The legal framework supporting content removal underwent some changes. By equating all internet resources with media outlets, the country's media law makes web publishers—including bloggers and users on social media websites—equally liable for the content they post online, but it does not further specify if online platforms are responsible for content posted by third parties. In October 2015, the regulator stated that social media users could be held liable for extremist comments posted on their pages by third parties as they could be regarded as permitting the publication of extremist materials in a mass media outlet, an offence under the criminal code punishable by up to 90 days in prison. Users who themselves post or share such content may be fined for its "p oduction, storage, import, transportation and dissemination", and in some cases, jailed for up to 20 years.[55]

The January 2016 amendments to the Communications Law oblige ISPs to monitor content themselves and make their own decisions on whether to restrict content.[56] The new Administrative Code, in force since 2016, imposes penalties on ISPs for not complying with censorship orders, with a fine

50 "Uber to launch officially in Kazkahstan " [in Russian] *Profit.kz*, April 27, 2016, http://bit.ly/23eQ1ob.

51 "InDriver ready to appeal the blocking in Kazakhstani court," [in Russian], *Forbes.kz*, May 3, 2016, http://bit.ly/29mY2nt.

52 "Internet clubs will demand IDs " [in Russian] *Zakon*, January 25, 2012, http://bit.ly/1QBFqCV.

53 Askar Muminov, "Anonymizers outlawed," [in Russian] *Kursiv*, June 8, 2015, http://bit.ly/1KWiYzw.

54 Tweet by @TorProject, December 03, 2015, bit.ly/1KYitaJ.

55 "Kazkahstani citizens can be arrested for someone else's comments in social media," [in Russian] *Tengrinews.kz*, October 21, 2015, bit.ly/1PAdqy5.

56 "ЗАКОН РЕСПУБЛИКИ КАЗАХСТАН," [Law of the Republic of Kazakhstan].

of up to US$2,000.[57] The same legislation imposes penalties on ISPs of up to US $20,000 for not storing users' personal data.

In order to avoid having a website or webpage blocked, individuals must remove content that is deemed extremist or is otherwise banned (see Blocking and Filtering).[58] In February 2016, the regulator adopted new rules for the monitoring of media, including online media, using a new technology called the "Automated System of Monitoring the National Information Space." No information on how this system will operate is publicly available, though once illegal content has been identified, the regulator will notify the website owner to remove the content. The owner will have three hours to comply, after which the hosting provider will be required to block the website, and legal charges will be brought against the website.[59]

Examples of content reported removed during the coverage period include the following:

- In October 2015, a court ordered ADAM Magazine, an opposition publication critical of the government, to close its Facebook page. The print magazine had been suspended in September 2015 after a series of libel cases, extremism charges, and technical violations.[60] The prosecutors successfully argued that the magazine and its Facebook page must be deemed a single outlet.[61]

- In November 2015, the crowdsourcing website Proizvolkz.net, run by the country's leading human rights watchdog, removed a video of self-immolation protesting of police behavior in Southern Kazakhstan. The regulator had ordered the removal, on grounds that the video violated children's rights legislation.[62]

- In February 2016, a court in Aktau (Western Kazakhstan) ordered the Society to Assist Drivers, a movement against corruption in traffic police, o remove a video from its YouTube account. The ruling said the video, which depicted a police officer who was ap arently abusing his power, had violated the police office 's honor and dignity.[63]

- In April 2016, Radiotochka.kz, a news site, published a report about the financial assets f MP Gulzhana Karagusova and her family members. The article was republished by many other online media outlets. However, almost all of them subsequently took the article down, some saying that they were pressured to do so.[64]

The authorities also approached international companies to remove content. In November 2015, the government announced that it had struck a deal with LiveJournal Russia in which LiveJournal agreed to comply with Kazakhstan's requests to remove pages containing terrorist, religious extremist, and

57 Article 637.9.5 of the Administrative Code of the Republic of Kazakhstan, accessed February 17, 2016, bit.ly/1Ts8IEl.

58 "ЗАКОН РЕСПУБЛИКИ КАЗАХСТАН," [Law of the Republic of Kazakhstan].

59 "Kazakhstan adopts rules for state monitoring of internet," [in Russian] *Digital.Report*, February 29, 2016, http://bit.ly/1SegFwe.

60 "Kazakhstan: Muzzling of magazine raises press freedom concerns," *Eurasianet,* September 2, 2015, http://www.eurasianet.org/node/74921.

61 "ADAM magazine banned at the prosecutor's request," [in Russian], *Adil Soz*, October 22, 2015, bit.ly/1QLyZHK.

62 "Authorities want a human rights website to protect children," [in Russian] *Digital.Report*, November 23, 2015, bit.ly/1KYlQhS.

63 "Aktau court made driver delete video of police officer f om internet," [in Russian] *Informburo.kz*, February 15, 2016, bit.ly/1QthQSG.

64 Anna Kalashnikova, "Radiotochka puts back the Karagusova piece," [in Russian] *Ratel.kz*, April 20, 2016, http://bit.ly/1WwaHrC.

violent content, as well as instructions on how to make explosives. In return, LiveJournal was offered the possibility of expansion in Kazakhstan within the framework of local laws, including potentially opening an office in Kazakhstan."[65]

From July to December 2015, Google received 19 requests for content removal, primarily for national security reasons, complying with 5 percent of requests.[66] Twitter reported four content removal requests, and zero compliance in the same period.[67] Facebook reported restricting access to 25 posts based on requests from the authorities in the second half of 2015. The stated reasons included violations of counterterrorism legislation.[68]

The government of Kazakhstan has also pursued legal suits abroad in attempt to have content removed. In early 2015, Kazakhstani authorities sought a U.S. Federal court order against Respublika-kz.info to compel the outlet, now hosted in the USA, to shut down. They also tried to make the court compel Facebook to disclose information about users associated with Respublika's account.[69] However, the court ultimately rejected both demands.[70]

Media, Diversity, and Content Manipulation

In addition to blocking and removing content, the online media landscape in Kazakhstan is also subject to less overt forms of restrictions on the free flow f information, such as progovernment propaganda and pressure to self-censor. Self-censorship in both traditional and online media outlets is pervasive. Social media remains the most liberal environment for the public exchange of news and opinions, but discourse there is considered to be very prone to manipulation and propaganda, including by commentators paid by the government. Although the authorities impose no restrictions on advertising with critical websites, the atmosphere of self-censorship extends to businesses too, and disruptions to the sites due to blocking or DDoS attacks make it difficult for them o attract sponsorship.

Central government procurement contracts in the media sphere reached KZT 43 billion (US$120 million) in 2015, not counting funds that are distributed by local administrations. Many progovernment online media outlets are frequent recipients of such contracts, including local privately owned blogging platforms.

The government has been subtly funding and recruiting popular bloggers and social media personalities to report on state matters since 2013.[71] In October 2014, a group of Facebook users registered the Bloggers Alliance of Kazakhstan to "make the country's information space healthier."[72] The office f the Alliance is located in the government's headquarters, furthering speculation that it was created to mislead the public by claiming to represent all Kazakhstani bloggers. These suspicions were reinforced by a statement the alliance released in February 2015 calling to replace the early presidential elections orchestrated by the authorities with a referendum to extend the incumbent

65 "Experts discuss unblocking of LiveJournal in Kazakhstan" [in Russian], *Digital.Report*, November 11, 2015, bit.ly/1TosgZ2.
66 Google Transparency Report page, accessed on February 17, 2016, bit.ly/1Qp26QF.
67 Twitter Transparency Report page, accessed on February 17, 2016, bit.ly/1KVxdRy.
68 Facebook Transparency Report page, accessed on February 17, 2016, bit.ly/21bXZzw.
69 Casey Michel, "US Judge Rejects Kazakhstan's Facebook Demands," *The Diplomat*, March 08, 2016, http://bit.ly/1U8bo9l.
70 "American court to let Kazakh website publish leaked emails," [in Russian] *Digital.Report*, November 06, 2015, bit.ly/1QbM3df.
71 Makpal Mukankyzy, "Bloggers invented the term – 'Tazhin's list,'" *Azattyq*, February 27, 2013, http://bit.ly/1LDKnZL.
72 "Bloggers unite in alliance," [in Russian] *BNews*, October 8, 2014, http://bnews.kz/ru/news/post/232657/.

president's powers until 2022, because, according to the statement, "everyone knows that President Nazarbayev's historical role makes him uncontested."[73]

LGBTI people in Kazakhstan are routinely stigmatized and discriminated against, and the situation worsened with a proposed law that would have banned "propaganda of homosexuality to protect children" and was initially passed in parliament. In May 2015, the Constitutional Council rejected the draft law, citing the "lack of clarity and discrepancies in terminology in Russian and Kazakh versions of the draft law, which left room for the possibility of violation of some constitutional norms."[74] Some observers characterized the decision as a compromise to appease the international community as part of Kazakhstan's unsuccessful bid to host the 2022 Winter Olympics. In October 2015, lawmaker Almas Turtayev asked the prime minister to "adopt a law restricting social media in Kazakhstan" because of "illegal, frightening and immoral content" that is disseminated there, including "open propaganda of sexual relations and acts, such as pedophilia".[75]

Civil servants, public officials, and emplo ees of state-owned companies are obliged to follow a set of guidelines, published in 2014, in their use of the internet. The guidelines urge employees not to post or repost material critical of the government, and not to "friend" authors of such posts in order to prevent possible threats to the image of the civil service, as well as preventing the dissemination of false information or leaks.[76]

Digital Activism

Though users continue to actively share content on various matters, including corruption, controversies in the judicial system, blatant cases of injustice, and others, the use of social media and other digital tools to organize for social and political campaigns is limited. In February 2014, an unexpected 20 percent devaluation of the national currency prompted frustrated citizens to use social media to organize a series of small rallies. However, a 100 percent currency devaluation in 2015 produced no protests. Nevertheless, a number of online campaigns drew attention in the coverage period.

A campaign to preserve a historic building in Almaty was launched on Facebook in summer 2015. Although the building in question was ultimately demolished, the campaign advocated for public participation in the decision-making process and managed to raise awareness. The new mayor, who assumed office in Sep ember, turned civic involvement and use of technology for feedback and problem-solving purposes into his selling point.

In September and October 2015, a fundraising campaign was launched to support online news site ratel.kz after it was blocked in unclear circumstances (see Blocking and Filtering). The initiative gained visibility in social media, where the website shared banners to solicit donations.

In April 2016, a rally against land reform allowing the sale of land to foreigners was held in Atyaru

73 "Bloggers' Alliance suggests holding a referendum instead of elections," [in Russian] *Novosti-Kazakhstan*, February 18, 2015, http://bit.ly/1AsWCMM.

74 Sayazhan Kaukenova, "Law on protection of children from information threatening their health is declared unconstitutional," [in Russian] *Vlast*, May 26, 2015, http://bit.ly/1Fd0yEG.

75 "A new call to regulate social media in Kazakhstan – now because of morale," [in Russian] *Digital.Report*, October 21, 2015, bit.ly/1ovbn3T.

76 Victor Burdin, "State officials not allo ed to criticize the power," [in Russian] *Forbes Kazakhstan*, January 12, 2015, http://bit.ly/1FexLTt.

(Western Kazakhstan) and was organized largely on Facebook.[77] Following a wave of protests and promises by activists to stage more rallies against land reform, the authorities suspended the law and convened the Public commission for land reform, inviting politicians, experts, and public figu es, including prominent critics and human rights activists, to develop new approaches to its implementation. The Atyaru rally sparked nationwide protests against land reform in May 2016.

Violations of User Rights

A new law introduced a National Security Certificate, software which must be installed on all user devices in Kazakhstan, potentially allowing the government to monitor encrypted traffic and conduct man in the middle attacks. Criminal prosecution of social media users and internet journalists on charges of extremism, insulting national dignity, or trumped up allegations of drug possession continued within the coverage period. Additionally, authorities cracked down on activists organizing land reform rallies on social media, arresting dozens of people. Online commentators continued to face pressure from the authorities, including the apparent interception of their electronic correspondence. There was at least once case of physical violence against a blogger during the coverage period.

Legal Environment

The constitution of Kazakhstan guarantees freedom of expression, but this right is qualified by many other legislative acts and in practice is severely restricted. The criminal code penalizes the dissemination of rumors, or "patently false information, fraught with the risk of breach of public order or imposition of serious damage," punishable by a fine f up to US$70,000 and up to 10 years in jail. Libel is a criminal offence that may result in up to US$20,000 in fines and up o two years of imprisonment. The criminal code provides stricter punishment for libel or insult of the president and other state officials, judges, and membe s of parliament, and Kazakhstani officials ha e a track record of using defamation charges to punish critical reporting.

The judiciary is not independent from the executive, and the president appoints all judges. The constitutional court was abolished in 1995 and replaced with the constitutional council, to which citizens and public associations are not eligible to submit complaints.

In March 2016, the Prime Minister's office eleased an order prohibiting all officials and visi ors of state bodies from using mobile devices with cameras and internet connection – smartphones, tablet PCs and smart watches. The move, which affected also the Judiciary and Legislature, is aimed at preventing the leakage of sensitive information.[78] In April 2016, the Ministry of Public Service revealed plans to ban state officials f om using social networking sites in the workplace, citing the need to "increase discipline".[79]

Prosecutions and Detentions for Online Activities

The government of Kazakhstan continues to arrest and prosecute individuals for posting critical po-

77 "Max Bokaev: People are ready for democracy," [in Russian] *Exclusive.kz*, April 28, 2016, http://bit.ly/1UmAimD; "Max Bokaev: Not a single lantern was broken," [in Russian] *Azh.kz*, April 24, 2016, http://bit.ly/1SzMC1P.

78 "Kazakhstan bans smartphones in government buildings," *BBC*, March 18, 2016, http://bbc.in/1rokp3P.

79 "State officials in Kazakhstan o be disconnected from social media," [in Russian] *Digital.Report*, April 27, 2016, http://bit.ly/1SOKIMJ.

litical or social commentary online, particularly involving Russia. Charges are usually brought under laws banning "extremism," specificall , the incitement of interethnic hatred.

- Bolatbek Blyalov, an activist and critic of the government, was arrested in November 2015 for incitement of interethnic hatred for online video interviews slamming the "imperial policy of Russia". He was held in custody in the run-up to the trial, and the case drew the attention of international rights organizations. In January 2016, shortly before the trial's end, Blyalov admitted his guilt, announced the cessation of his activism, and asked the public "not to politicize his case." He was convicted to 3 years of restricted freedom and released.[80] [81]

- In July 2015, a 22-year-old man in Petropavl (Northern Kazakhstan), was sentenced to three years in jail for "posting provocative materials of interethnic and interreligious hatred," and insulting the "national dignity of other ethnicities," after publishing material online relating to the Russian-speaking population of Kazakhstan and in relation to Muslims.[82]

- In July 2015, a court in Uralsk (Western Kazakhstan) sentenced a person to three years of restricted freedom for using Facebook to call for the "elimination of Russia" and a shutdown of Russian TV channels in Kazakhstan.[83]

- In December 2015, Yermek Taichibekov, a well-known pro-Kremlin blogger, was sentenced to four years in prison for incitement of interethnic hatred after calling for the unification of Kazakhstan and Russia on his Facebook page. Taichibekov denied that his actions were criminal and insisted that the trial was politically motivated. The case against Taichibekov was initiated by a complaint from a group of nationalist activists calling themselves the National Patriots.[84]

- Igor Sychev, administrator of a group called "Overheard in Ridder" on Russian-language social network VK.com, was sentenced to fi e years in prison in November 2015 for inciting separatism after posting a poll asking if the group if Ridder, northeastern Kazakhstan, should become a part of Russia.[85]

The government has also continued to arrest and detain individuals for posting content on social media which is deemed to be threatening or critical of the ruling regime.

- Two outspoken critics of the government, Serikzhan Mambetalin and Ermek Narymbayev, were sentenced in March 2016 to two and three years restricted freedom and prohibition of public activity, respectively, for inciting hatred and insulting national dignity after they reposted an article ridiculing the "vices" of Kazakhs on social media,[86] though they had

80

81 "Blyalov released in court," [in Russian] *RFE/RL Kazakh service*, January 21, 2016, bit.ly/1WDk3Qb.

82 "A North Kazakhstan resident sentenced for incitement of inter-ethnic strife in social media," [in Russian] *Novosti-Kazakhstan*, July 31, 2015, bit.ly/1QwiLZ4.

83 "An Uralsk resident sentenced for incitement of inter-ethnic strife on Facebook," *Uralskweek.kz*, July 16, 2015, bit.ly/1KDpeyN.

84 "Taichibekov sentenced to 4 years in jail," [in Russian] *RFE/RL Kazakh service*, December 11, 2015, bit.ly/1Tv3mao.

85 "Blogger Sychev sentenced to 5 years in prison," [in Russian], *RFE/RL Kazakh service*, November 15, 2015, bit.ly/1L5jXQF.

86 "Activists got restrction of freedom instead of imprisonment," [in Russian] *RFE/RL Kazakh service*, March 30, 2016, http://bit.ly/1NFtGyn.

accompanied their posts with critical comments about the article's contents.[87] Mambetalin and Narymbayev were arrested in October 2015 and remained in custody until a hearing in January 2016. The case was marred by numerous procedural violations and viewed by many as a politically motivated show trial.

- In August 2015, three Facebook users were charged under the criminal code for spreading rumors after they published posts on Facebook stating that riots which occurred at the Artem market in Astana in June 2015 were ethnically motivated, resulted in deaths, and that police used rubber bullets to disperse the crowd. At least one of the accused was sentenced in August 2015 to two-and-a-half years of restriction of freedom.[88]

- A criminal investigation has was launched in early 2016 against Facebook user Kyril Kovyazin after he posted negative comments on his Facebook page regarding Kazakhstan's revered historical-cultural figu e Abay Qunanbaiuli. Kovyazin is being investigated for the dissemination of radical ideas. [89]

- In April 2016, an Almaty resident was detained, interrogated and put into pre-trial custody for sharing a photo of a person allegedly killed in Kyzyl-Orda (South Kazakhstan) during a protest which transpired to be a photo taken in China in February 2015. The detained is accused of disseminating knowingly false and provocative material (Article 274.2.3. of the Criminal Code).[90]

- In May 2016, dozens of activists in different cities of Kazakhstan were detained and sentenced to up to 15 days of administrative arrest after they shared their intention to take part in the land reform rallies through their accounts in social media. The authorities said the posts were calls to attend unsanctioned gatherings.[91] Dozens of journalists, including many from online publications, were also briefly detained while eporting on the land reform protests.[92]

The authorities have also targeted individuals working for independent online news outlets. In May 2016, editor of opposition news site Nakanune.kz, Guzyal Baydalinova, was sentenced to 18 months prison on criminal charges of spreading false information under Article 274 of the criminal code after the website published articles alleging Kazakhstan's largest bank, Kazkommertzbank, was involved in misconduct and corruption in the country's construction industry. Baydalinova was already found to have damaged the state-owned bank's reputation in a civil libel suit in June 2015 in which she was ordered to pay US $107,000. [93] Observers suspect the government, which has close ties to Kazkommertzbank, of initiating the prosecution as part of an attempt to silence dissenting journalism

87 "Mambetalin and Narymbaev arrested for 2 months for incitement of national hatred," [in Russian] *Tengrinews.kz*, October 15, 2015, http://bit.ly/1r1hI7O.

88 "A person sentenced for dissemination of rumors about Artem riots," [in Russian], *Informburo.kz*, August 04, 2015, bit.ly/1SMGpR5.

89 "Police investigates a case of insulting the Abai Studies on Facebook," [in Russian] *Fergananews*, February 15, 2016, bit.ly/1WDcn0k.

90 "Almaty resident detained for sharing fake Kyzyl-Orda photo," [in Russian] *Informburo.kz*, May 6, 2016, http://bit.ly/1Nlvpca.

91 "More than 20 people arrested for 'calls for rallying,' " [in Russian], *RFE/RL's Kazakh Service*, May 19, 2016, http://bit.ly/29na3bg.

92 "55 journalists detained in Kazakhstan," [in Russian], *AdilSoz.kz*, May 26, 2016, http://bit.ly/29mEVZM.

93 Joanna Lillis,"Kazakhstan: Libel Trial Rekindles Fears of Media Muzzling", *Eurasianet.org*, July 01, 2015, bit.ly/1RS8hht.

online.[94] Furthermore, in January 2016, Yulia Kozlova, another journalist at Nakanune.kz, had her apartment searched and faced drug possession charges that her supporters said were in retaliation for her work. In February 2016, Kozlova was acquitted of those charges by a court.[95]

Surveillance, Privacy, and Anonymity

It is difficult to estimate the scope and depth of government surveillance of online communications in Kazakhstan. The "system for operational investigative measures" (SORM) system of surveillance implemented by the government is similar to that of other former Soviet republics and allows for deep packet inspection (DPI) of data transmissions. The general public, as well as civil society activists, often underestimate the potential threat of government surveillance and do not always take steps to protect their privacy or use encryption software. Some anonymizing tools are subject to blocking (see Blocking and Filtering).

In December 2015, Kazakhtelecom issued a press release stating that internet users would be required to install a national security certificate on their devices by January 1, 2016, in order to comply with recent amendments to the Law on Communications. The statement said the certificate would be issued by the State Technical Service (STS) and its installment enforced by ISPs. Kazakh authorities maintain that the certificate will be used to increase security online by fighting cybercrime and restricting the dissemination of illegal information.[96]

The announcement raised several privacy and security concerns. The certificate is designed to intercept traffic to and from foreign sources, and allow government officials to gain access to encrypted mobile and web communications. It could empower authorities to conduct man-in-the-middle attacks on encrypted traffic between Kazakh users and foreign servers, though authorities deny that the certificate will be used for this purpose.[97] The certificate may also restrict users from accessing much of the internet, as browsers and websites may decline to trust devices using the certificate. The government was reportedly attempting to secure a WebTrust audit of the certificate to prevent this from happening, but the status of that audit was unclear in mid-2016.

Little information was available regarding the rollout of the certificate, though it appeared to be in progress at the beginning of the year. One ISP had reportedly received the certificate for installation in March 2016.[98] Additionally, users can download the certificate onto their devices from the website of telecoms operator KazTransCom.

Various authorities already monitor internet traffic. A professional from a private-sector telecom company who spoke on the condition of anonymity stated that the president's administration, the prosecutor general's office, and the National Security Committee have been planning to launch three different content monitoring systems, including software to monitor social networking sites. In

94 Human Rights Foundation, "HRF to Kazakhstan: Drop criminal defamation charges against news editor," June 6, 2016, https://humanrightsfoundation.org/news/hrf-to-kazakhstan-drop-criminal-defamation-charges-against-news-editor-00502.

95 Vyacheslav Polovinko, "Almaty court acquitted journalist Yulia Kozlova," [in Russian] *RFE/RL Kazakh service,* February 29, 2016, http://bit.ly/1SyeL9w.

96 "National security certificate of Kazakhstan: protection of users or of the state," [in Russian], *Digital.Report*, December 04, 2015, bit.ly/1LC6732.

97 "Experts: Kazakh authorities want to monitor protected user traffic" [in Russian], *Digital.Report*, December 04, 2015, bit.ly/1XHHb1g.

98 "TeliaSonera in Kazakhstan received the national security certificate," [in Russian] *Digital.Report*, March 14, 2016, http://bit.ly/1QRV8Zb.

the past, the Almaty city administration acknowledged that it monitors popular social networking sites.[99] Activists using social media are occasionally intercepted or punished, sometimes preemptively, by authorities who have prior knowledge of their planned activities. Most recently, dozens activists were subject to arrests and administrative imprisonments after calling for land reform rallies on social media (see Prosecutions and Detentions for Online Activities).

Kazakhtelecom maintains that its DPI system is used for traffic management and p ovides no access to users' personal data.[100] According to Shavkat Sabirov, president of the Internet Association of Kazakhstan (IAK), the DPI system was installed on the backbone infrastructure in 2010 by the Israeli company Check Point Software Technologies. In July 2015, WikiLeaks published an exchange of emails between an alleged official f the Kazakh special services and Hacking Team, the Italian spyware fi m. The exchange of emails appears to suggest that the government might have obtained software to monitor and interfere with online traffic, including enc ypted communications, as well as to perform targeted attacks against certain users and devices.[101]

SIM card registration is required for mobile phone users. Legislation obliges both ISPs and mobile operators to retain records of users' online activities, including phone numbers, billing details, IP addresses, browsing history, protocols of data transmission, and other data, via the installation of special software and hardware when necessary.[102] Providers must store user data for two years and grant access within 24 hours to "operative-investigatory bodies," including the National Security Committee, secret services, and military intelligence, when sanctioned by a prosecutor, or in some cases "by coordination with prosecutor general's office."[103]

Additionally, the 2013 law on countering terrorism granted extra powers to the security bodies and obliged mass media (including internet resources) to assist the state bodies involved in counterterrorism.[104] However, the exact mechanisms of assistance are not specified.

In March 2016, the regulator issued new rules for public access points, which removed all previous requirements, including the requirement to document customer IDs. Instead, a single technical method of user authentication was introduced with a one-time SMS code. However, SIM cards in Kazakhstan remain subject to obligatory registration, which may enable authorities to monitor online activities of users accessing internet from public hotspots.[105]

Intimidation and Violence

One case of physical violence was reported in the coverage period. Bota Zhumanova, a prominent economic blogger who had been sporadically criticizing the fiscal authorities and local anks, was

99 Asemgul Kasenova, "Repentant terrorists' testimonies to be used in fighti g extremism," [in Russian] *Tengri News*, October 1, 2013, http://bit.ly/1NuVlRF.

100 Community Information Security, "Here we received official confirmation from the use of DPI Kaztel," *Yvision* (blog), accessed August 2014, http://bit.ly/1G2HzTp.

101 WikiLeaks, "Hacking Team," accessed on February 22, 2016, bit.ly/1XI2DmK.

102 Ksenia Bondal, "Следи за базаром - нас слушают" [Watch out, we are watched] *Respublika*, republished by *Zakon*, November 5, 2009, http://bit.ly/1WRqj8b.

103 "Rules of rendering internet access services," adopted by the governmental decree #1718 on December 30, 2011, http://bit.ly/1R2vtdw

104 "Law of the Republic of Kazakhstan on amendments and addenda into several legislative acts of the Republic of Kazakhstan regarding counteraction to terrorism," [In Russian] *Zakon*, January 8, 2013, http://bit.ly/1jfvsIV.

105 "Kazakhstan introduced new rules for public points of internet access," [in Russian] *Digital.Report*, March 16, 2016, http://bit.ly/1S3t3Nw.

brutally beaten near her house in October 2015. A CCTV camera captured the attacker, who did not attempt to take any of Zhumanova's belongings. Police investigated the case, which they characterized as hooliganism or a robbery, and arrested a suspect two weeks later.[106] Zhumanova said the attack was in retaliation for her work.[107]

Technical Attacks

Technical attacks against online news media and government websites were observed during the coverage period. According to Olzhas Satiev, president of the Center for Analysis and Investigation of Cyber-attacks, more than 90 percent of Kazkahstani websites have vulnerabilities.[108] Satiev's organization has exposed several such vulnerabilities on the websites of e-government services, the Ministry of Foreign Affairs, and others. In June 2015, a governmental website, Invest.gov.kz, was hacked and defaced with ISIS-related images and slogans.[109] In February 2016, the official ebsite of EXPO-2017, an international exhibition hosted by the government, was disabled following a phishing alert and possible damage to its visitors.[110]

Kazakhstani activists and dissidents were also subject to technical attacks within the coverage period, and some suspect the government's involvement. In February 2016, Seitkazy Matayev, president of the National Press Club, and Asset Matayev, director general of the KazTAG news agency, said that their Gmail accounts had been accessed without permission from computers in other cities in Kazakhstan.[111] Separately, in August 2016 reports emerged that Kazakh opposition figu es and dissidents living abroad, including Irina Petrushova and Alexander Petrushov of the critical publication *Respublika*, were targeted in 2015 with malware attacks. The Electronic Frontier Foundation reported that the attacks were conducted by agents of the government via the Indian security company Appin Security Group.[112]

106 "Court sanctioned arrest of the man who attacked Zhumanova," [in Russian] *Tengrinews.kz*, October 29, 2015, bit.ly/1oxhpAk.

107 "Bota Zhumanova talks details of the attack," [in Russian] *Current Time*, November 04, 2015, bit.ly/1oXimTg.

108 "Olzhas Satiev: More than 90 percent..." [in Russian], interview, *Profit.kz*, February 10, 2016, bit.ly/1T1mbmZ.

109 Facebook, post by Kaisar Zhumabai-uly, accessed on February 22, 2016 https://www.facebook.com/kaissar.zhumabayuly/posts/7081180192997846.

110 Facebook, post by Denis Sulhachev, accessed on February 22, 2016, on.fb.me/1oXvg3v.

111 "Statement on situation around National Press Club and KazTAG news agency," *Adil Soz*, February 22, 2016, bit.ly/1oXyyUp.

112 Electronic Frontier Foundation, "I got a Letter from the Government," August 3, 2016, https://www.eff.org/files/2016/08/03/i-go -a-letter-from-the-government.pdf.

Freedom House

Kenya

	2015	2016
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	9	8
Limits on Content (0-35)	7	7
Violations of User Rights (0-40)	13	14
TOTAL* (0-100)	**29**	**29**

* 0=most free, 100=least free

Population:	**46 million**
Internet Penetration 2015 (ITU):	**46 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Partly Free**

Key Developments: June 2015 – May 2016

- Average broadband connection speeds surpassed the global average in 2016, enabling greater and higher quality access to the internet for Kenyans (see **Availability and Ease of Access**).
- A music video promoting gay relationships was unsuccessfully targeted for removal, and netizens suspected government interference with a website satirizing the president (see **Content Removal**).
- The Kenyan Film and Classification B ard expressed intent to regulate online video content, sparking concerns of potential censorship (see **Content Removal**).
- Arrests and prosecutions under KICA Section 29 for criticizing government officials or their associates during the coverage period numbered in the dozens, continuing a problematic trend of silencing ordinary netizens that began in 2014 (see **Prosecutions and Detentions for Online Activities**).
- In a positive step, Section 29 was declared unconstitutional in April 2016 (see **Legal Environment**).
- Research revealed that Kenya's National Intelligence Service was a registered customer of FinFisher's sophisticated surveillance technology (see **Surveillance, Privacy, and Anonymity**).

Introduction

Internet freedom in Kenya declined slightly in the past year due to increasing arrests and prosecutions for "misusing" online tools to criticize the authorities.

Kenya is one of the most wired countries in sub-Saharan Africa, boasting a number of undersea fiber optic cable landings in the coastal city of Mombasa and serving as a gateway for several others countries in the region.[1] Continued investments in information and communication technology (ICT) infrastructure has paid off, with Kenya's average broadband connection speeds reaching 7.2 Mbps, surpassing the global average of 6.3 Mbps in 2016. As a result, user growth has been profound; government data touted an 80 percent internet penetration rate in mid-2016, a figu e that incorporates the expanding mobile phone user population.

While the internet is still relatively free, the government has increased attempts to restrict it in the past couple of years, driven by sensitivities around hate speech since the tumultuous 2008 elections, growing terrorist threats, and the upcoming general election in 2017. During the coverage period, an unprecedented number of Kenyan bloggers and social media users were arrested or summoned for questioning, mainly for their online commentary criticizing government officials. This continued a trend of silencing ordinary netizens—in addition to journalists—that began in 2014. Most arrests were made under Section 29(a) of the 2013 Kenya Information and Communications Act (KICA), which penalized the "misuse of licensed telecommunications equipment" before it was ruled unconstitutional by the Supreme Court in April 2016. Arrests and prosecutions dropped significantly following the ruling.

No websites, social media platforms, or communication apps are blocked in Kenya, though unsuccessful efforts to take down ostensibly objectionable content was reported in the past year. In one incident, the Kenyan Film and Classification B ard (KFCB) ordered Google's Kenya office o pull down a YouTube music video that the agency deemed inappropriate for promoting homosexual relationships. Google declined, pointing to its lack of jurisdictional authority over flagged ouTube content.

In keeping with the KFCB's growing interest in policing Kenya's internet for "morally corrupt" content, the body signaled intentions to restrict online videos in January, particularly on the newly launched streaming service, Netflix, out f concerns that some content may be unsuitable for minors. In October, the KFCB followed up with the draft Film, Stage Plays and Publication Act 2016, which if enacted, would require ISPs to police their networks for illegal content such as pornography and hate speech, and potentially facilitate censorship.

Meanwhile, Kenyans grew increasingly concerned about government surveillance efforts in the past year, especially following October 2015 revelations that the National Intelligence Service was a registered customer of FinFisher surveillance technology.

Obstacles to Access

Steadily increasing access to the internet was fueled in large part by relatively low-priced mobile services and expanding mobile broadband networks. Average broadband connection speeds surpassed the

1 David E. Weeklys, "The Internet in Kenya" June 2015, http://techsahara.com/the-internet-in-kenya-according-to-david-e-weekly-of-google/#sthash.E9fl T1T.dpuf

global average in 2016. The telecommunication regulator's independence was questioned after irregularities in the members' appointment process led to it being disbanded in February 2016.

Availability and Ease of Access

The Kenyan government's commitment to developing the country's information and communication technologies (ICT) sector as a tool for economic growth has led to a tremendous increase in the number of users, notably on mobile devices. Much of this growth has been driven by growing recognition of the necessity of internet services and the decreasing costs of internet enabled devices.

Internet users numbered 37.7 million, according to government data from June 2016, a 27 percent increase over the previous year,[2] representing 80 percent penetration of the country's estimated 47 million population.[3] Data from the International Telecommunications Union (ITU) from 2015, which may not account for mobile internet access, estimated a lower penetration rate of 46 percent, a modest increase from 43 percent in 2014.[4] Fixed-line broadband penetration remained very low, however, at less than one percent in 2015.[5]

The government reported nearly 40 million mobile phone subscriptions in June 2016,[6] a penetration rate of 90 percent, up from 80 percent the previous year. The ITU reported 81 percent penetration in 2015.[7] However, many people have more than one subscription to take advantage of incentives offered by different providers or to expand their geographic coverage, putting the actual number of users much lower. The mobile sector is the predominant provider of data and internet services to Kenyan users, mostly through 3G and Long-term Evolution (LTE) networks, which account for 99 percent of total internet subscriptions.[8] Broadband connection speeds are fast, documented at 7.2 Mbps by Akamai's *State of the Internet* report, above the global average of 6.3 Mbps.[9]

Kenya has comparatively low-priced mobile services for Africa, with calling rates around KES 4 (US$ 0.04) per minute.[10] Data bundles are available for prepaid mobile customers, while mobile broadband subscriptions on GPRS/EDGE and 3G/4G networks continue to increase. This growth can be attributed to competitive mobile internet tariffs, promotions, competition between providers, and the rise in social media use, particularly among young people. In 2015, the Alliance for Affordable Internet ranked Kenya 25 out of 52 countries assessed that met the UN Broadband Commission's target for affordable mobile broadband, set at a maximum of 5 percent of a country's gross national

2 Communications Authority of Kenya, Quarterly Sector Statistics Report: Q4 2015/2016 (April-June 2016), http://www.ca.go.ke/images/downloads/STATISTICS/SECTOR%20STATISTICS%20REPORT%20Q4%202015-2016.pdf

3 Worldometers. http://www.worldometers.info/world-population/kenya-population/

4 International Telecommunication Union, "Percentage of Individuals Using the Internet,"2000-2014, http://bit.ly/1cblxxY.

5 Kenya - Fixed Broadband, Digital Economy and Digital Media - Statistics and Analyses. http://www.budde.com.au/Research/Kenya-Fixed-Broadband-Digital-Economy-and-Digital-Media-Statistics-and-Analyses.html?r=51

6 Communications Authority of Kenya, Quarterly Sector Statistics Report: Q4 2015/2016 (April-June 2016).

7 International Telecommunication Union, "Mobile-cellular Telephone Subscriptions," 2000-2014, http://bit.ly/1cblxxY.

8 Communications Authority of Kenya, Quarterly Sector Statistics Report: First Quarter of the Financial Year 2015/2016 (July-September 2015).

9 Akamai, "Average Connection Speed," map visualization, *The State of the Internet*, Q1 2016, accessed August 1, 2016, http://akamai.me/1LiS6KD

10 Safaricom rates, accessed August 1, 2016, http://www.safaricom.co.ke/personal/calls-sms/prepay/prepay-calls-and-sms-rates

income (GNI) per capita.[11] But while internet penetration continues to increase across the country, there is still a large urban-rural divide in access, with internet use mainly concentrated in Nairobi.[12]

Large rural areas of the country have not been able to benefit f om Kenya's high-capacity bandwidth in part due to market disparities and weaknesses in last mile connectivity, which is expensive and requires basic infrastructure such as electricity and roads that are often poorly developed in rural areas. This prompted the government to establish the Universal Service Fund (USF) in 2013 to raise KES 1 billion from the industry each year in order to expand mobile and internet services.[13] The National Optic Fibre Backbone Infrastructure (NOFBI) also aims to expand rural access; to date, it has been implemented in 27 rural towns. The NOFBI project aims to improve communication across the country's newly devolved governance structures and increase delivery of e-government services, such as applications for national identity cards or passports and registration of births and deaths.[14]

Restrictions on Connectivity

During the year under review, there were no reports of the government controlling the internet infrastructure to limit connectivity. Kenya connects to the international internet via four undersea cables—Seacom, the East Africa Marine System (TEAMS), EASSY, and Lower Indian Ocean Network (LION2)—which increased the broadband availability and improved internet speeds over the past several years. License provision for access to the international gateway was liberalized in 2004.[15]

ICT Market

Kenya's ICT sector is competitive, comprised of over ten internet service providers (ISPs) and three mobile phone providers. As of June 2016, Safaricom continued to dominate the market for mobile phone services with a market share of 64 percent for internet and mobile data subscriptions, 78 percent for voice services, and 94 percent for SMS.[16] This high market share prompted the ICT cabinet secretary and regulator to propose regulations in July 2015 to reign in Safaricom's monopoly of the sector.[17] The Attorney General subsequently asked Parliament to withdraw the proposed regulations, accusing the ICT ministry of overstepping its mandate.

Meanwhile, two other mobile operators—Airtel Networks and Telkom Kenya (Orange)—served the remaining share of the mobile market. There are no limitations on the number of operators permit-

11 A4AI, The Affordability Report, 2014, http://a4ai.org/affordability-report/report/2015/.

12 The need for digital inclusion can be inferred when one considers Facebook active usage statistics as a reflection f internet connectivity patterns in Kenyan towns. It is estimated that over 60 percent of Kenyans (2.5-3 million) who log onto Facebook at least once a month are based in Nairobi, followed by Mombasa with 8 percent and Eldoret 4 percent. The rest of the towns have 3 percent and below of those active on Facebook on a monthly basis. See, John Kieti, "Kenya's top 20 towns on Facebook" June 2015, http://www.gmeltdown.com/2015/06/kenyas-top-20-towns-on-facebook.html

13 Muthoki Mumo, "Sh74 billion needed to bridge Kenya's yawning digital divide," Daily Nation, May 28, 2013. http://bit.ly/1lPvXUo.

14 ICT Authority, "National Fibre Optic to cover all 47 counties by December 2015" http://www.icta.go.ke/nofbi-update/.

15 David Souter and Monica Kerretts-Makau, "Internet Governance in Kenya – An Assessment for the Internet Society," Internet Society, September 2012, http://bit.ly/1M0d9xv.

16 Communications Authority of Kenya, Quarterly Sector Statistics Report: Q4 2015/2016 (April-June 2016).

17 Lynet Igadwah, "Safaricom CEO says dominant player tag to slow its growth into global brand," Business Daily Africa, July 30, 2015, http://bit.ly/2fkdLqL

ted to launch and operate telecommunications infrastructure, with both data carriers and cellular licenses allowed to run domestic fiber net orks.[18]

Regulatory Bodies

Kenya's telecommunications sector is regulated under the Kenya Information and Communication Amendment Act (KICA) 2013, which established the Communications Authority of Kenya (CA) as the regulator for both broadcast and online media.[19] While KICA explicitly enshrines the independence of the CA, the act was widely criticized for the power it granted to the cabinet secretary of the ICT ministry to appoint the now authority's board without stakeholder input as well as the presidential appointment of the board's chairperson.

The regulator's murky independence was highlighted in May 2015 when the High Court disbanded the CA's board after what it determined were irregularities in the appointment process,[20] such as the appointment of board members outside statutory timelines. The ICT ministry appealed the decision.[21] However, the new ICT cabinet secretary who assumed office in December 2015 [22] withdrew the appeal at the advice of the Attorney General in 2016, on the basis that it would not be successful,[23] effectively declaring the board null and void. A new board was inaugurated in May 2016.[24]

Limits on Content

No websites were blocked during the coverage period, though a YouTube music video promoting gay relationships was unsuccessfully flagged for removal, while the owner of a website satirizing the president accused the government of interfering to briefly take it offline. The Kenyan Film and Classification Board expressed intent to regulate online video content, sparking concerns of potential censorship.

Blocking and Filtering

Internet content is not blocked or fil ered in Kenya, and internet users have unrestricted access to social networking platforms and communication applications such as Facebook, Twitter, YouTube, and Linkedin, all of which rank among the 20 most popular websites in the country.[25]

Online censorship may be on the horizon. In January 2016, the Kenya Film Classification B ard

18 Robert Schuman and Michael Kende, Lifting barriers to Internet development in Africa: suggestions for improving connectivity, Internet Society, May 2013, 35, http://bit.ly/1sIsL10.

19 Republic of Kenya, "The Kenya Information and Communication (Amendment) Bill, 2013," Kenya Gazette Supplement No. 105 (National Assembly Bills No. 19), July 22, 2013, http://bit.ly/1vyJYiY.

20 Otiato Guguyu, "High Court disbands Communications Authority board," Daily Nation, May 31, 2015, http://bit.ly/1LGgS7B.

21 Lilian Ochieng, "Ministry faults High Court move to disband telcos regulator board," Daily Nation, June 3, 2015, http://bit.ly/1AP6uHE.

22 Mr. Joe Mucheru takes over as Cabinet Secretary for the Ministry of ICT, see: http://www.information.go.ke/?p=1623

23 Lilian Achieng, "CA board disbanded amid protests from members", Daily Nation, February 6, 2016, http://www.nation.co.ke/business/CA-board-disbanded-amid-protests-from-members-/-/996/3064090/-/4sn6vpz/-/index.html

24 Lillian Ochieng, "End of wrangles as government names new Communications Authority board," Business Daily Africa, May 5, 2016, http://www.businessdailyafrica.com/Kenya-names-new-Communications-Authority-board/539546-3190074-126lkfe/index.html

25 Alexa, "Top Sites in Kenya," accessed March 6, 2016, http://www.alexa.com/topsites/countries;0/KE

(KFCB) stated it would seek to regulate the newly launched streaming service, Netflix, out f concerns that the site hosts video content that may be unsuitable for minors.[26] The KFCB followed up by proposing draft legislation in October. The Film, Stage Plays and Publication Act 2016,[27] if enacted, would require ISPs to ensure that content hosted on their networks is classified by the b ard, as well as "take reasonable steps to prevent the use of their services for hosting or distributing pornography, radicalisation materials, glamorisation of use of drugs and alcohol, hate speech and demeaning any religion and community and report all persons maintaining or hosting or distributing all content reasonably suspected to be in violation of this Act."[28] Failure to comply would be considered a criminal offense and subject to a fine, imprisonment f up to two years, or both. Such intermediary liability for online content may lead ISPs to block content preemptively.

Content Removal

The government has at times sought to remove controversial content from the internet, without much success thus far. In March 2016, the KFCB ordered Google's Kenya office o pull down a YouTube music video that the agency deemed inappropriate for promoting homosexual relationships. The office declined on g ounds that it lacks jurisdiction over content flagged on ouTube.[29]

In a murky case, the satirical website isuhuruinkenya.co.ke went offline for se eral hours on December 7, 2015 just a few days after it was registered,[30] prompting suspicions of government interference.[31] The site reports whether President Uhuru Kenyatta is in the country at the given time, adding weight to the popular perception of him as an absentee president. The site's creator said on Twitter that the national registrar, KENIC, had removed his site after receiving a complaint from the government.[32] KENIC published an official sta ement saying that it had not deleted the website's domain and that technical issues were responsible for its temporary inaccessibility. It explicitly denied being subject to government pressure to remove the website.[33]

Intermediaries can be held liable for illegal content, such as copyright and hate speech, though they are not required to actively monitor traffic assing through their networks unless they are made aware of illegal content.[34] Under the National Cohesion and Integration Act of 2008, which outlaws hate speech, a media enterprise can be fined up o KES 1 million (US$11,000) for publishing "utter-

26 STELLAR MURUMBA, "Netflix should be subjec ed to Kenyan rating standards, KFCB says," Business Daily Africa, January, 8 2016, http://bit.ly/22Pr4m5.

27 Vincent Matinde, "Kenyan govt takes aim at streaming services," ITWeb Africa, October 11, 2016, http://www.itwebafrica.com/ict-and-governance/256-kenya/236916-kenyan-govt-takes-aim-at-streaming-services

28 Film, Stage Plays and Publication Act 2016, Part IV, Section 39 (draft bill), http://kfcb.co.ke/wp-content/uploads/2016/10/DRAFT-BILL-KFCB-21-7-Draft-10.pdf

29 "Google has refused government demands to take down a gay music video in Kenya," Quartz. March 14, 2016, http://qz.com/638461/google-has-refused-government-demands-to-take-down-a-gay-music-video-in-kenya/

30 See site at: http://isuhuruinkenya.co.ke/

31 Eric Mugendi, "Asking 'Is Uhuru In Kenya?' Gets A Kenyan Website Shut Down," Tech Cabal, December 7, 2015, http://techcabal.com/2015/12/07/is-uhuru-in-kenya-shut-down/

32 Meruem Twitter post, December 6, 2015, https://twitter.com/kipropesque/status/673765645889204224

33 "KENIC deletes isuhuruinkenya.co.ke domain," Kictanet, December 7, 2015, https://www.kictanet.or.ke/?p=22887

34 Alice Munyua, Grace Githaiga and Victor Kapiyo, "Intermediary Liability in Kenya," (research paper, commissioned by Association for Progressive Communication) http://bit.ly/1GOXHDa.

ances" that can be characterized as hate speech under the law's broad definition [35] This provision can be invoked to block or take down online content, according to the Association of Progressive Communications.[36] Issues of intermediary liability are further complicated by the fact that the Kenyan judicial system and media are not fully conversant with legal norms involving the internet.

Media, Diversity, and Content Manipulation

Kenya's online information landscape is diverse and vibrant, representing a wide range of issues and viewpoints. However, in Kenya's increasingly partisan environment, observers note hired bloggers and Twitter bots on both sides of the political divide are increasingly crowding out diverse and independent viewpoints with partisan commentary on social media.

There are no state-run online news outlets, and the most popular news websites include the BBC, CNN, and Kenya's *Standard Online* and *Daily Nation*. While print outlets, television, and radio continue to be the main sources of news and information for most Kenyans, all major television stations have live-stream features, use YouTube to rebroadcast news clips, and actively engage audiences on Facebook and Twitter.

Bloggers and social media personalities have become highly influential o er the past few years, as the increase in fast and affordable internet in major cities and towns has enabled Kenya's growing class of digitally skilled citizens to become content creators and alternative sources of news and information. According to the Bloggers Association of Kenya (BAKE)—formed in 2011 to support Kenya's blogging community—there were an estimated 15,000 registered blogs in 2015,[37] covering a diverse range of topics such as fashion, the environment, food, politics, health, and human rights. The exponential growth in blogs has created an economically viable industry for bloggers who are increasingly sought by Kenyan businesses as a platform for advertising.[38]

The government does not impose any economic constraints on online media in Kenya, which has helped online outlets thrive. In recent years, print newspaper distribution has been undercut by online news sources, a trend which led the president to announce in March 2015 that government advertising would shift to digital platforms to reduce spending, calling them cheaper and more effective given their broad reach.[39]

Individual internet users are generally comfortable expressing themselves openly online, though the use of digital technologies to spread ethnic, racist, and xenophobic commentary continues to pose a serious challenge to freedom of expression in Kenya, particularly during politically contentious periods such as national elections. In the absence of a suitable framework to regulate online hate speech, many feel that the emphasis should be on self-regulation by internet users, with the government

35 Section 62 (1) defines ha e speech as "words intended to incite feelings of contempt, hatred, hostility, violence or discrimination against any person, group or community on the basis of ethnicity or race." Section 62 (2) holds: "A newspaper, radio station or media enterprise that publishes the utterances referred to in subsection (1) commits an offence and shall be liable on conviction to a fine not e ceeding one million shillings." See: National Cohesion and Integration Act, 2008, section 62, accessed September 12, 2014, http://bit.ly/1ZR1dbX.

36 Munyua, Githaiga and Kapiyo, "Intermediary Liability in Kenya."

37 Bloggers Association of Kenya (BAKE), The State of Blogging & Social Media in Kenya 2015 Report, 2, http://bit.ly/1JXAG4.

38 Bloggers Association of Kenya (BAKE), The State of Blogging & Social Media in Kenya 2015 Report, 3.

39 Charles Wokabi, "Uhuru directs State fi ms to place all their adverts on digital outlets," Daily Nation, March 3, 2015, http://bit.ly/1DSZFCv.

stepping in when needed to address hate crimes involving the internet.[40] Nonetheless, observers worry that self-censorship may rise following the growing number of bloggers and ordinary users arrested for criticizing the government.

Spotlight on Marginalized Communities

Freedom on the Net 2016 asked researchers from India, Indonesia, Kenya, Kyrgyzstan, Jordan, Mexico, Nigeria, and Tunisia to examine threats marginalized groups face online in their countries. Based on their expertise, each researcher highlighted one community suffering discrimination, whether as a result of their religion, gender, sexuality, or disability, that prevents them using the internet freely.

In Kenya, a Freedom House consultant conducted an original study of 18 LGBT (lesbian, gay, bisexual, transgender) people and the extent to which they rely on the internet to find community and share information.[1] The study found:

- Negative attitudes toward LGBT lifestyles are reflec ed in Kenyan religious practices, legal instruments, marketplaces, education institutions, and media outlets. The internet challenges this power structure by offering LGBT people space to develop communities and coordinate advocacy. Activists have also used YouTube to publish a video aimed at normalizing LGBT relationships, and created podcasts to create awareness of LGBT issues. Seventeen out of eighteen survey respondents believe that the internet offers them a safe space to meet other members of the LGBT community and allies
- Unfortunately, LGBT people face greater obstacles to internet access, and frequent threats from government officials, other in ernet users, and criminal hackers that foster self-censorship. Government proposals to increase surveillance of internet users to defend their security are also particularly problematic for LGBT people in Kenya, where same sex relationships are criminalized.
- The internet can also exacerbate offline discrimination. Online media that ely on a large readership for advertising are particularly likely to publish inaccurate, sensationalist stories on LGBT people, which often stir violence against members of the community.

1 "At Risk in a Safe Space: Online Threats to the LGBT Community in Kenya," research paper, October 2016, on file with F eedom House.

Digital Activism

The internet continued to grow as an important platform for political debate and mobilization around critical issues in Kenya. With the fourth largest Twitter activity in Africa (following Egypt, Nigeria, and South Africa),[41] Kenya's Twitter users regularly engage in political conversations online. In July 2015, when the news network CNN referred to Kenya as a "hotbed of terror" during a report about President Obama's visit to the country, Kenyans took to social media to dispel the mischaracterization of their country using the hashtag #SomeoneTellCNN that trended worldwide.[42]

In another example of hashtag activism, Kenyans created the #WhatWouldMagufuliDo campaign in November 2015 to praise newly elected Tanzanian President John Magufuli for his immediate efforts to curb corruption by placing limits on foreign travel by public servants and lavish state cel-

40 Centre for Human Rights and Policy Studies (CHRIPS) and Centre for Human Rights and Peace, Report of the Experts' Meeting on Addressing the Challenge of Hate Crimes on the Internet in Kenya, (Nairobi, Kenya: University of Nairobi, 2013) 4.

41 Nancy Agutu, "Kenyans 4th most active Twitter users in Africa, politics among hot topics," The Star, April 6, 2016, http://www.the-star.co.ke/news/2016/04/06/kenyans-4th-most-active-twitter-users-in-africa-politics-among-hot_c1326926

42 Josh Feldman, "Kenyans Mock CNN with #SomeoneTellCNN after They Report Kenya as 'Terror Hotbed,'" Mediaite, July 23, 2015, http://www.mediaite.com/online/kenyans-mock-cnn-with-someonetellcnn-after-they-report-kenya-as-terror-hotbed/

ebrations.[43] Through fun memes and tweets, the campaign sought to contrast the leadership priorities of the Kenyan president with his Tanzanian counterpart with the hopes of encouraging greater accountability.[44]

Violations of User Rights

Dozens of charges were filed under KICA Section 29 for criticizing government officials or their associates during the coverage period, continuing a problematic trend of abusing the law to silence ordinary netizens that began in 2014. In a positive step, Section 29 was declared unconstitutional in April 2016. Research revealed the use of FinFisher surveillance technology by Kenya's National Intelligence Service.

Legal Environment

Freedom of expression is enshrined in Article 33 of Kenya's 2010 constitution and includes the right to seek, receive, or impart information and ideas, while Article 31 provides for the right to privacy. These rights, however, do not extend to propaganda, hate speech, or incitement to violence. Hate speech is penalized under the 2008 National Cohesion and Integration Act, passed in response to widespread ethnic violence that ensued after the 2007 general elections.[45] Individuals found guilty of spreading hate speech, broadly defined, can be fined up o KES 1 million (US$11,000), sentenced to up to three years in prison, or both.

Section 132 of the penal code, which penalizes "undermining the authority of public office s," also constrains freedom of expression, both online and off.[46] Meanwhile, criminal defamation laws remain on the books, pending repeal or amendment to conform with the 2010 constitution.

Prior to April 2016, online expression was specifically ta geted under Section 29 of the Kenya Information and Communications Act (KICA) 2013, which penalized the use of ICTs to disseminate messages deemed to be "grossly offensive" or that cause "annoyance, inconvenience or needless anxiety to another person" with a fine f up to KSH 50,000, three years in prison, or both.[47] Section 29 of KICA was used to arrest and, in some cases, charge an unprecedented number of bloggers and social media users for their online activities in 2015 (see Prosecutions and Detentions for Online Activities). In a positive April court decision, the provision was declared unconstitutional for infringing on fundamental rights,[48] leading to a significant d op in arrests and prosecutions since.[49]

Recently proposed laws threaten to further restrict online freedom of expression. In July 2016, the Ministry of ICT called for stakeholder input into the Computer and Cyber Crimes Bill 2016.[50] The bill reportedly followed international standards such as the Budapest Convention on Cybercrime in its

43 "Africans on Twitter – 15 Hashtags That Defined 2015 (# OT2015)," January 4, 2016. http://yesiyesighana.com/world/4956-4956/

44 "Hilarious Memes From 'What Would Magufuli Do' Twitter Trend," Nairobi Wire, November 27, 2015, http://bit.ly/2f9oXpo.

45 Milly Lwanga, "Freedom of expression and harmful speech: The Kenyan situation," Article 19, September 27, 2012, http://bit.ly/1M0qSEJ.

46 The Republic of Kenya, Penal Code, chapter 63, http://bit.ly/1jxeeH7

47 Republic of Kenya, The Kenya Information and Communications Act, chapter 411A, 2009, http://bit.ly/1LyMfxo; amended in 2013: The Kenya Information and Communications (Amendment) Act, 2013, http://bit.ly/1M1zTDB.

48 Lilian Mutegi, "East Africa: Justice Mumbi Ngugi Declares Section 29(b) of the Kica Act Unconstitutional," April 19, 2016, http://allafrica.com/stories/201604201330.html

49 http://www.nation.co.ke/oped/blogs/dot9/walubengo/2274560-3396492-format-xhtml-jo0ret/index.html

50 Computer and Cyber Crimes Bill 2016, http://www.mygov.go.ke/?p=11226

efforts to address cybercrime such as computer fraud and child pornography.[51] However, Article 14 of the bill punishes "cyberstalking" and "cyberbullying," defined as communication that detrimentally affects" a person, with penalties of up to KES 20 million, imprisonment of up to ten years, or both.[52] If passed, the provision could be used in the same way as the unconstitutional KICA Section 29.

A number of positive laws have been proposed in recent years to protect the rights of Kenyan internet users. The Data Protection Bill 2013, though still in draft form as of mid-2016, aims to regulate the collection, processing, storing, use, and disclosure of information relating to individuals processed through automated or manual means.[53] The current absence of a strong data protection law threatens citizens' privacy rights amid rising concerns over unchecked government surveillance (see Surveillance, Privacy, and Anonymity).

Prosecutions and Detentions for Online Activities

An unprecedented number of Kenyan bloggers and social media users were arrested or summoned for questioning in 2015-2016, mainly for online commentary criticizing government officials, under Section 29(a) of the 2013 Kenya Information and Communications Act (KICA), which penalized the "misuse of licensed telecommunications equipment" before it was ruled unconstitutional by the Supreme Court in April 2016.[54] The trend of using the law as a tool to silence critical speech began in 2014.

Dozens of arrests and prosecutions were documented under KICA Section 29. In most cases, those arrested were held for some days for questioning before being released without charge. Some allegations of "misusing" telecommunications bordered on the absurd. In March 2016, university student Ezer Kipkirui was arrested for taking a photo of a long queue on a busy street in Nakuru town.[55]

Other examples include the following cases:

- Well-known and controversial blogger Robert Alai, who had been arrested several times in previous years for his online commentary, was a continual target in the past year. In December 2015, Alai was arrested after he posted a message on Facebook criticizing the Ethics and Anti-Corruption Commission. He was released on a bond in January 2016 after pleading not guilty.[56] While his case was dropped in June after Section 29 of the KICA Act was declared

51 Lilian Mutegi, "Kenya govt calls for public participation on Computer and Cyber Crimes Bill 2016," CI East Africa, July 14, 2016, http://allafrica.com/stories/201607140740.html

52 Computer and Cyber Crimes Bill 2016, Article 14, http://www.mygov.go.ke/wp-content/uploads/2016/07/MOICT-PUBLICATION-READY-COMPUTER-AND-CYBERCRIMES-BILL-2016-1-1-1.pdf

53 Commission for the Implementation of the Constitution, "The Data Protection Bill, 2012," http://bit.ly/1hNGLGB.

54 "Kenya: Win for freedom of expression as repressive law declared unconstitutional," Article 19 (press release), April 19, 2016, https://www.article19.org/resources.php/resource/38343/en/kenya:-win-for-freedom-of-expression-as-repressive-law-declared-unconstitutional

55 Shitemi Khamadi, "Ezer Kipkurio arrested for creating disturbance by taking a photo of Huduma Center in Nakuru," Kenya Monitor (blog), March 7, 2016, http://www.monitor.co.ke/2016/03/07/ezer-kipkirui-arrest-for-creating-disturbance-by-taking-a-photo-of-huduma-center-in-nakuru/

56 Nancy Agutu, "Robert Alai denies improper use of telecommunication equipment, freed on Sh100,000 bond," The Star, January 5, 2016, http://www.the-star.co.ke/news/2016/01/05/robert-alai-denies-improper-use-of-telecommunication-equipment-freed_c1270018

unconstitutional, his release was authorized under Section 87 (a) of the penal code which allows future re-arrest and prosecution.[57]

- Brian Otieno was arrested and charged with "misuse" of a telecommunications gadget in January 2016 for allegedly defaming a gubernatorial aspirant on social media.[58]
- Elijah Kinyanjui was arrested on January 12, 2016, and held for 12 hours for allegedly sharing a story that depicted the Nakuru governor's daughter Brenda Mutanu in a bad light on WhatsApp and Facebook.[59]
- Martha Wanjiru Miano, an employee of the Nyeri County Constituency Development Fund (CDF), was arrested in February 2016 and charged with "abusing" the brother of the Nyeri county governor on Facebook. She was later released and acquitted on procedural grounds.[60]

The authorities also targeted users and journalists for online commentary about the military's fight against the Al-Shahbab terrorist group. In January 2016, journalist Yassin Juma was arrested for his social media posts about an Al-Shahbab attack on Kenya Defense Forces in Somalia.[61] Also in January, Eddy Reuben Illah was arrested and charged with publishing prohibited material for allegedly sharing images depicting Kenyan soldiers killed by Al Shabaab through a WhatsApp group.[62] Prison warden Patrick Safari, popularly known as "Modern Corps," was also arrested for posting comments about the Al Shahbab attack, spending the night in prison for interrogation.[63] He had been previously arrested in July 2015 for an "annoying tweet" about Kenyan police.[64]

Section 132 of the penal code, which penalizes "undermining the authority of public office s," was also used to prosecute individuals for their online activities, including Anthony Njoroge Mburu, who was charged in January 2016 for posting allegedly false information on social media that was viewed as harmful to Kiambu Governor William Kabogo.[65]

Surveillance, Privacy, and Anonymity

The Kenya Information and Communications Act (KICA) prohibits unlawful monitoring and intercep-

57 VINCENT AGOYA, "Court drops case against blogger Robert Alai over offensive post," The Nation, June 2, 2016, http://nairobinews.nation.co.ke/news/court-drops-case-blogger-robert-alai/

58 "Newsletter: Freedom of Expression in Eastern Africa," Article 19, February 4, 2016, https://www.article19.org/resources.php/resource/38251/en/newsletter:-freedom-of-expression-in-eastern-africa

59 James Wamathai, "BAKE condemns the arrest and intimidation of Kenyans online," BAKE (blog), January 24, 2016, http://www.blog.bake.co.ke/2016/01/24/bake-condemns-the-arrest-and-intimidation-of-kenyans-online/

60 Faith Nyamai, "Court frees Nyeri blogger at centre of political storm, terms arrest un-procedural," Daily Nation, March 2, 2016, http://www.nation.co.ke/counties/nyeri/Nyeri-blogger-at-centre-of-political-storm-freed/-/1954190/3100668/-/13cacplz/-/index.html

61 Charles Mwaniki, "Police arrest blogger over attack posts," Business Daily Africa, January 24, 2016, http://www.businessdailyafrica.com/Police-arrest-blogger-over-attack-posts/-/539546/3047574/-/9tja4q/-/index.html

62 Shitemi Khamadi, "Eddy Reuben Illah charged with misuse of licensed telecommunication system," Kenya Monitor (blog), January 20, 2106, http://bit.ly/2fM0WJv

63 "BAKE condemns the arrest and intimidation of Kenyans online," BAKE (blog), press release, January 24, 2016, http://www.blog.bake.co.ke/2016/01/24/bake-condemns-the-arrest-and-intimidation-of-kenyans-online/

64 "Patrick Safari aka 'Modern Corps' arrested and charged for 'annoying tweet,'" Kenya Monitor (blog), July 30, 2015, http://bit.ly/1PC5YBq.

65 Shitemi Khamadi, :Anthony Njoroge Mburu alias Waime Mburu charged for publishing false statement on Facebook," Kenya Monitor (blog), January 23, 2016, http://www.monitor.co.ke/2016/01/23/anthony-njoroge-mburu-alias-waime-mburu-charged-for-publishing-false-statement-on-facebook/

tion of communications,[66] though the Prevention of Terrorism Act 2012 allows the authorities to limit constitutional freedoms, such as the right to privacy, during terrorist investigations.[67] Amendments to the Prevention of Terrorism Act in 2014 explicitly enable national security bodies to intercept communications "for the purposes of detecting, deterring and disrupting terrorism,"[68] which must be authorized by an interception order granted by the High Court.[69] The Kenyan government has stepped up its surveillance efforts in the past couple of years to deal with the threat of terrorism, which became particularly pronounced following the September 2013 Al-Shabab terrorist attack on the Westgate mall in Nairobi.

In October 2015, a report by Citizen Lab revealed a FinFisher server with IP addresses registered under Kenya's National Intelligence Service.[70] Known as a sophisticated and user-friendly spyware suite sold exclusively to governments for intelligence and law enforcement purposes, FinFisher has been involved in a number of high-profile su veillance abuses despite being marketed as a tool for figh - ing crime. Privacy International also reported in October 2015 that it had received a leaked memo listing Kenya among other countries that employ FinFisher's surveillance technology, such as Syria, Zimbabwe, Rwanda, and Uganda.[71]

User anonymity is comprised by SIM card registration requirements under the Kenya Information and Communications (Registration of Subscribers of Telecommunications Services) Regulations, 2013, which prescribes penalties of up to KES 300,000 (US$3,500) or imprisonment of up to three years for failure to abide by the registration requirements.[72] The regulations also grant the communications regulator with access to service providers' offices and ecords without a court order, raising concerns over the lack of judicial oversight.[73]

Anonymity and user privacy may be further restricted by government efforts to tackle cybercrime via public WiFi networks. In July 2015, the regulatory authority announced new regulations requiring users of devices with WiFi capabilities to register their devices with the Kenya Network Information Centre (KENIC).[74] If implemented, registration would require users to provide their ID card details and telephone numbers, which could be easily tracked by the government.[75] The regulations would require the installation of Closed Circuit Television (CCTV) cameras to record people using public WiFi.[76]

66 Kenya Information and Communications Act, Article 31, http://admin.theiguides.org/Media/Documents/Kenya%20Information%20Communications%20Act.pdf

67 Prevention of Terrorism Act 2012, Article 35, http://www.frc.go.ke/legislation/2013/03/prevention-of-terrorism-act-2012

68 Security Laws Amendment Act 2014, Article 69, http://kenyalaw.org/kl/fileadmin/pdfdownl ads/AmendmentActs/2014/SecurityLaws_Amendment_Act_2014.pdf

69 Prevention of Terrorism Act 2012, Article 36, http://www.frc.go.ke/legislation/2013/03/prevention-of-terrorism-act-2012

70 Citizen Lab, "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation," October 15, 2015, https://citizenlab.org/2015/10/mapping-finfish s-continuing-proliferation/

71 Nick Hopkins and Jake Morris, "UK fi m's surveillance kit 'used to crush Uganda opposition,'" BBC, October 15, 2015, http://www.bbc.com/news/uk-34529237

72 Kenya Information and Communications (Registration of Subscribers of Telecommunications Services) Regulations, 2014; Privacy International, The Right to Privacy in Kenya, http://bit.ly/1LkeJ04.

73 Section 13. "A licensee shall grant the Commission's office s access to its systems, premises, facilities, files, ecords and other data to enable the Commission inspect such systems, premises, facilities, files, ecords and other data for compliance with the Act and these Regulations." The Kenya Information and Communications (Amendment) Act, 2013, http://bit.ly/1M1zTDB.

74 Sean Gallagher, "Kenya to require users of public Wi-Fi to register with government," Ars Technica, July 1, 2015, http://arstechnica.com/tech-policy/2015/07/kenya-to-require-users-of-wi-fi- o-register-with-government/

75 Lilian Ochieng, "Tough new rules force all new users to list their gadgets," Daily Nation, June 30, 2015, http://www.nation.co.ke/news/CA-WiFi-Internet-Rules-Cybercrime/1056-2771118-hyhy28z/index.html

76 Liquid Telecom faults CCTV rule for public Wi-Fi. April 17, 2016, http://bit.ly/2fUj4Aj

Intimidation and Violence

Bloggers and ordinary users faced increasing intimidation and violence in recent years. In June 2015, Twitter activist Wanjeri Nderi said she was assaulted at a shopping mall by an unidentified individual who told her to "stop making noise" before attacking her. Known for her Twitter posts about corruption and injustice in Kenya, Nderi and her supporters believe she was targeted for her frequent criticisms of the government.[77]

Law enforcement officials used the accusation f "misusing" telecommunications equipment to harass and intimidate users for their online activities, even if no charge resulted (see Prosecutions and Detentions for Online Activities). In January 2016, for example, Judith Akolo was interrogated by the Directorate of Criminal Investigations after she retweeted a post from another Twitter user, Patrick Safari (@moderncorps), which questioned why a notice advertising police vacancies was published on the day of the deadline for submitting applications.[78]

Technical Attacks

There were no politically motivated cases of technical violence against civil society, independent news, or opposition websites during the coverage period, though leaked emails published by Wikileaks in June 2015 revealed the government's intentions to launch a technical attack against blogger Robert Alai's anti-corruption news website in April 2015.[79]

77 Shitemi Khamadi, "Wanjeri Nderu assaulted for tweeting on corruption," Kenya Monitor, July 3, 2015, http://bit.ly/1NkoWKI.

78 "Newsletter: Freedom of Expression in Eastern Africa," Article 19, February 4, 2016.

79 Daniel Finnan, "Kenyan government asked Hacking Team to attack dissident website," Radio France Internationale, July 17, 2015, http://rfi.my/1Kkbq4 .

Freedom House

Kyrgyzstan

	2015	2016
Internet Freedom Status	Partly Free	Partly Free
Obstacles to Access (0-25)	11	10
Limits on Content (0-35)	8	7
Violations of User Rights (0-40)	16	18
TOTAL* (0-100)	**35**	**35**

* 0=most free, 100=least free

Population:	**5.96 million**
Internet Penetration 2015 (ITU):	**30 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- More of the population has access to the internet than ever before, with the gradual spread of broadband infrastructure and the majority of mobile providers launching 4G Networks (see **Availability and Ease of Access**).
- Online journalists have faced legal sanctions including fines for posting con ent which criticizes state officials (see **Prosecutions and Detentions for Online Activities**).
- In March and May 2016, recorded telephone conversations between opposition figu es were leaked online, sparking speculation that the government is misusing its surveillance capabilities (See **Surveillance, Privacy, and Anonymity**).

Introduction

The internet in Kyrgyzstan remains fairly liberal, though concerns regarding government surveillance practices were heightened following leaked recordings of opposition leaders' phone calls, and at least one disproportionate fine was issued o a journalist for "damaging the honor" of a former president.

The environment for internet freedom in Kyrgyzstan has improved in recent years, with fewer restrictions since the overthrow of President Kurmanbek Bakiev's regime in 2010. Despite some improvements, a rural-urban divide in internet access persists, and internet penetration rates lag behind those of neighboring countries.

The government does not engage in widespread censorship, and websites which had been previously blocked are now available. The authorities have targeted online expression deemed extremist, and have expanded the range of expression that can be punished under anti-extremism laws. Though the internet largely remains a sphere of free expression in Kyrgyzstan, in some instances internet users were prosecuted for criticizing the government online and for "liking" controversial content on social media.

Like many states in the former Soviet Union, the Kyrgyzstan uses SORM technology for surveillance purpose, and recently required all ISPs and mobile providers to install the latest version of SORM to facilitate government surveillance. Evidence continues to emerge indicating that the government is abusing this technology to monitor the political opposition.

Obstacles to Access

Internet access in Kyrgyzstan is relatively limited, though internet penetration continues to increase, with the introduction of unlimited plans by mobile operators and the development of 4G services helping to improve access. There is still a digital divide between urban and rural areas, as telecommunication companies have fewer incentives to expand services and infrastructure outside major cities. The state-owned telecommunications company, KyrgyzTelecom, controls the majority of the market for fixed internet access, with a market share of 60 percent.

Availability and Ease of Access

Access to the internet in Kyrgyzstan continues to expand, though the percentage of the population with internet access is still low by global standards. Internet penetration rates reported by the International Telecommunication Union (ITU), Kyrgyzstan's State Communication Agency (SCA), and independent research groups vary. According to the ITU, the internet penetration rate in 2015 reached 30.25 percent, compared to 28 percent in 2014 and just 16 percent in 2009.[1] In contrast, the SCA reported that in 2015 there were 4,754,601 active internet users in Kyrgyzstan, or approximately 79 percent of population. The average connection speed in the fi st quarter of 2016 increased to 3.3 Mbps.[2]

1 International Telecommunication Union (ITU), "Percentage of individuals using the Internet," http://bit.ly/1eKDWOQ.
2 Akamai, "State of the Internet, Q1 2016 Report," https://goo.gl/TQH7L7.

Fixed-broadband access, via either fibe -optic cables or DSL, is accessible mainly in the capital, Bishkek, with broadband in the provinces provided only by the state-run internet service provider KyrgyzTelecom. Broadband speeds range from 24 Mbps for DSL to 100 Mbps for the FTTx (fiber o the *x*) network, which is well-developed in Bishkek. KyrgyzTelecom has launched a CDMA 450 mobile telephone and broadband network to expand telecom infrastructure into more rural areas, though it has only become partially active. CDMA 450 phones have become popular in rural areas with more than 30,000 subscribers as of October 2016.[3]

Mobile phone penetration is significantly higher than in ernet penetration, at 116 percent at the end of 2015[4] comparing with 128 percent as of the end of 2014, according to the SCA. Mobile phone companies say that their networks cover 90 percent of the country's populated territory, thus extending the possibility of internet use for most people as mobile web access expands. Beeline, one of the largest mobile phone carriers, launched a 3G network in 2010 that covers the entire country. Another large fi m, Megacom, launched its own 3G network in 2012, covering more than 50 percent of populated territory by 2013.[5] Megacom and Beeline announced the launch of 4G LTE networks in the main cities of Kyrgyzstan in March and May 2016, respectively, with plans for expansion across the entire country.[6] Saima Telecom has a 4G network covering Bishkek and some suburbs. GSM operator NurTelecom (under the brand O!) launched a 4G LTE network covering Bishkek and surrounding areas in 2014.[7] In July 2015, Megaline one of the biggest ISPs, launched an LTE network in Bishkek and suburbs.

In recent years, the price for internet has decreased, becoming more affordable for much of the population, though primarily in the capital where the infrastructure is well-developed and there is greater competition among providers. In 2015-2016 FTTX providers in the capital increased the bandwidth offered without increasing prices, with the maximum available bandwidth of 20 Mbps at an average price of US$17-25 USD per month. Rates in rural areas, served by KyrgyzTelecom, are significantly higher than in ur an areas. An internet connection of 128 Kbps cost US$8.50 per month in some rural regions in 2016; 1 Mbps cost about US$38. KyrgyzTelecom hosts 44 Wi-Fi hotspots in 14 different locations throughout Kyrgyzstan with free access up to 256 Kbps.

The development of mobile networks provides an alternative to fi ed broadband access. Beeline's cheapest data plan provides 50 MB per day for US$0.07. Megacom offers 100 MB per day for US$0.30. Mobile operator O! offers unlimited data for US$20 per month. In April 2016, the average monthly wage was KGS 13,544 (US$200).[8]

3 KyrgyzTelecom, "Results of modernization and development projects since 2011," http://kt.kg/about_us/press_center/#ui-tabs-2.

4 *Отчет агентства связи за 2015 год*, [Annual report of SCA for 2015] http://bit.ly/1OQXBnQ.

5 MegaCom, "продемонстрировал уверенный рост зоны покрытия сети 3,75G в 2013 году," [Megacom demonstrated steady growth of 3.75 network coverage in 2013] press release, January 16, 2014, http://megacom.kg/rus/press/news/3052.html

6 MegaCom, "MegaCom объявляет о масштабном запуске сверхскоростного 4G LTE!" [MegaCom announces large-scale launch super-high-speed 4G LTE!] March 10, 2016, https://www.megacom.kg/news/3708?locale=ru; Beeline, "Beeline объявляет о запуске сети 4G LTE во всех регионах Кыргызстана!" [Beeline announce about launching 4G LTE network in all regions of Kyrgyzstan] May 16, 2016, https://www.beeline.kg/kg/news/continueReading?articleCode=00050014.

7 O!, "Мобильный оператор O! первым из GSM-операторов Кыргызстана открывает возможность использования технологии передачи данных 4G LTE," [Mobile operator O! Is the fi st of GSM operators in Kyrgyzstan opens an opportunity to use 4G LTE data transfer technology] news release, May 8, 2014, http://bit.ly/1OuduiI.

8 National Statistical Committee of the Kyrgyz Republic (Stat KG), "Основные показатели социально-экономического развития Кыргызской Республики в январе- апреле 2016г," [Main indicators of social-economic development of Kyrgyz Republic in Jan-Apr 2016] May 20, 2016, http://bit.ly/1sJtR2O.

Spotlight on Marginalized Communities

Freedom on the Net 2016 **asked researchers from India, Indonesia, Kenya, Kyrgyzstan, Jordan, Mexico, Nigeria, and Tunisia to examine threats marginalized groups face online in their countries. Based on their expertize, each researcher highlighted one community suffering discrimination, whether as a result of their religion, gender, sexuality, or disability, that prevents them using the internet freely.**

In Kyrgyzstan, Elnura Emilkanova interviewed 25 blind internet users and two support staff to highlight the experiences of young internet users.[1] The study found:

- Kyrgyz, the national language, is increasingly the only language spoken by young people, particularly in rural areas, yet there is no speech to text software available in Kyrgyz. Most blind internet users rely on screen reader software called JAWS, which reads out text from a computer screen, but only in Russian and English. "I wish there was much more information online in the Kyrgyz language," said 25-year-old Ainuska Apsamatkyzy.
- Special software can help blind customers access the internet via mobile phone. Yet it is exceedingly rare to meet a blind person who uses mobile internet, since the cost of service is a financial bu den. The average disability pension in Kyrgyzstan is less than US$ 50 per month.
- Computer literacy training for the blind is severely underfunded. "On average a blind person spends at least six months learning the basic steps to be able to work with screen readers," said computer instructor Azat Toktombaev.

1 Elnura Emilkanova, *"If the Internet were Accessible to Me:" Access for the Blind in Kyrgyzstan,* research paper, August 2016, on file with Freedom House.

Restrictions on Connectivity

ISPs in Kyrgyzstan are not required to use government-owned channels to connect to the international internet and can establish their own. Kyrgyzstan's six ISPs have international internet connections via Kazakhstan. In the past, the blogging platform LiveJournal, which was blocked in Kazakhstan, was also accidentally blocked for some internet users in Kyrgyzstan, though this problem appears to have been resolved. The government of Kyrgyzstan does not currently place restrictions on any social media platforms or communication applications. In 2010, the state-owned ISP Kyrgyz-Telecom said it had completed the construction of a fibe -optic cable connection to China.[9]

Fixed-line internet service providers no longer charge differently for domestic versus international content. However, with the introduction of unlimited data plans, providers offer different bandwidths for domestic compared to international traffic. Mobile phone opera ors do not make this distinction in their data plans and provide the same bandwidth for accessing information, regardless of where it is hosted.

ICT Market

Kyrgyzstan's telecommunications sector is relatively liberalized and competitive compared to that of other countries in the region; however, the state-owned KyrgyzTelecom is still the largest ISP with a market share of about 60 percent. The other fi e fi st-tier ISPs (Elcat, Megaline, Saima Telecom, Beeline, NurTelecom) are privately owned.

9 Kyrgyztelecom, "Годовой отчет 2010, Кыргызтелеком," [Annual report 2010, Kyrgyztelecom] http://bit.ly/1WXWIK6.

There are three mobile phone operators providing voice and data services under brands Megacom (32 percent of the market), Beeline (41 percent), and O! (27 percent), Mobile operator O! has experienced market growth in the past two years due to its launch of 4G services. Megacom was nationalized in 2010 amid the political upheaval.

Regulatory Bodies

In July 2016, the State Committee of Information Technologies and Communication was created, taking on many of the regulatory functions previously performed by the State Communication Agency (SCA). The Committee's responsibilities include developing ICT policy, facilitating the development of the ICT sector, as well as governing the ICT sector. Whereas the SCA was a semi-independent regulatory body, the State Committee of Information Technologies and Communication is funded from the state budget and is therefore closely tied to the government. Though the Committee is a relatively new body, it is already apparent that it does not operate transparently. Meanwhile, the SCA has been absorbed as a department under the Committee, taking away many of its previous functions and removing its independence.

Limits on Content

Although the government has attempted to censor certain content on the internet, in general there are fewer restrictions placed on material that is available online. This may be because television remains by far the dominant medium through which citizens obtain information about their country, and thus censorship efforts have focused on broadcast media.[10] *The government focuses its online censorship efforts on content deemed extremist, though the number of websites blocked remains relatively low.*

Blocking and Filtering

The authorities in Kyrgyzstan do not engage in extensive blocking of material online, and social media outlets such as YouTube, Facebook, and Twitter are freely available. However, the government does block access to content deemed extremist. By the middle of 2016, approximately 30 websites were blocked for extremist content or content inciting national or religious hatred, including sites containing resources of radical Islamic group Hizb-ut-Tahrir. The courts have also occasionally blocked content for the purpose of protecting reputation and dignity, often of public figu es. In August 2015, a court ruled in favor of Ainagul Chylabaeva, blocking a website which accused the former public official f corruption and connections with criminal networks.

In previous years, a small number of websites have been subject to blocking. Kloop.kg, an independent news outlet, was blocked for several weeks in December 2014, after reposting a clip showing

10 According to the 2012 M-vector survey, TV still remains the primary source of information for 82.6 percent of the population. See, M-vector Consulting Agency, *Исследование поведения и восприятия медиа аудитории 2012 г. (3-я волна*) [Media Consumption & Consumer Perceptions Baseline Survey 2012 (2nd Wave)] Kyrgyzstan, March 2013, http://bit.ly/1jkOXQg.

children from Kazakhstan training in Islamic State camps.[11] *Fergana News*, another independent news site, was periodically blocked for a number of years until 2013.[12]

According to the 2005 statute on counteracting extremist activities,[13] the procedure for blocking websites begins with a request to the prosecutor.[14] A review committee may be assembled consisting of representatives with different expertise (linguistic, religious, or legal) that can confi m the extremist nature of the site. However, members of the committee are appointed by the government, calling its independence and objectivity into question. The court will ultimately issue a judicial decision to block the website. The process has been inconsistently enforced.

On May 13, 2013, the parliament passed amendments to the Law on Counteracting Extremist Activities, which allow the government to order the blocking of websites hosted outside the country for "extremist" content.[15] Parliamentarians said the amendments were inconsistent with other legislation, and proposed regulating online content under the rubric of mass media, which would give the government greater control over online content.[16] The amendments were intended to make the blocking process more transparent, since they oblige corresponding bodies to publish the list of blocked resources.[17] As of May 2016, no list of blocked sites has been created.

In May 2016, parliament adopted further amendments to the Law on Counteracting Extremist Activities. The amendments expand the range of activities subject to the law to include expressions of approval or justifications f extremism or terrorism online, provisions which are framed broadly and may be subject to misuse.[18]

Content Removal

There were no cases in which the government forced the removal of content online in 2015 or 2016. In most cases, content that the government deems illegal is hosted on servers outside of Kyrgyzstan, so they cannot require that the host providers remove it.

Media, Diversity, and Content Manipulation

There are no specific economic estrictions imposed by the government that negatively impact users' ability to publish content online, or that restrict online media outlets' ability to remain financially

11 Ulugbek Akishev, "Агентство связи Кыргызстана отозвало предписание о блокировке видео на Kloop.kg," [Communication agency of Kyrgyzstan called back their prescription about blocking video on Kloop.kg] *Kloop* (blog), December 16, 2014, http://bit.ly/1VOHV1P.

12 "Independent News Website Partly Blocked in Kyrgyzstan," Radio Free Europe/Radio Liberty, February 22, 2012, http://bit.ly/1WXZ1wW.

13 Dmitry Golovanov, "Kyrgyzstan: Extremism Outlawed," *IRIS Merlin*, August 2005, http://bit.ly/1Lhfh4I; The Statute on Counteracting Extremist Activities" February, 2009.

14 Representatives of the 10th department explained the procedure to the author in a private interview in December 2011.

15 "Во втором чтении приняты поправки в закон о противодействии экстремистской деятельности" [The amendments to the law "On Counteraction to Extremist Activities" have passed second reading] *FOR*, February 28, 2013, http://www.for.kg/news-216159-ru.html.

16 Поправки о закрытии экстремистских сайтов отправили на доработку [Amendments on closing extremist sites are sent to revision] November 26, 2012, http://bit.ly/18eWjdw.

17 President of Kyrgyzstan, "ЗВ Закон «О противодействии экстремистской деятельности» внесены изменение и дополнения," [Ammendments are made to the law "On Counteraction to Extremist Activities"] news release, May 13, 2013, http://bit.ly/1G9R0R3.

18 Ministry of Justice, О внесении изменений в некоторые законодательные акты Кыргызской Республики (On amendments in several legal acts of Kyrgyz Republic), July 1, 2016, http://cdb.minjust.gov.kg/act/view/ru-ru/111376.

sustainable. Yet the Kyrgyz blogosphere is not well-developed. There are several popular blog-hosting platforms in Kyrgyzstan (such as Namba.kg, Kloop.kg, Diesel.elcat.kg, and Taboo.kg), but most blogs focus on entertainment or reprint reports from other news agencies.

There are no particularly popular blogs specifically de oted to political or social issues. Most blogs are in Russian, though some are in the Kyrgyz language, but the latter are not as popular. The internet in general has become an important source of alternative information for users, but since it is primarily the wealthier segments of the population who can afford to consistently access the internet, these are the main participants in online communities.

Self-censorship exists online to a certain degree, primarily as a result of government restrictions on inciting national hatred. All posts on forums are strictly moderated to limit this type of content, and online journalists and bloggers generally try to avoid issues concerning ethnic relations. Other laws may increase self-censorship, such as amendments to the criminal code signed by the president in May 2014, which introduced criminal penalties of up to three years in prison for disseminating false accusations regarding the commission of crimes (see Legal Environment).

Online platforms such as forums and social networks are actively used for manipulating public opinion, usually by trolls hired by different political actors to influence discussions and exp ess favorable views.

Digital Activism

Digital activism efforts remain limited in Kyrgyzstan. However, in October 2015, social media users launched a campaign against the government's plan to spend US $40,000 on 120 chairs to be used in Kyrgyzstan's parliament, replacing chairs purchased as recently as 2010. The #120Кресел (#120Chairs) campaign received extensive coverage on Twitter and news outlets, and the government abandoned the plan.[19]

Violations of User Rights

While internet users are not generally imprisoned for their expression, a growing number of users faced fines and other legal sanctions for critical expression online in this coverage period. In addition, the government's capacity for surveillance of ICTs increased in recent years. A regulation requiring upgrades to SORM-3 technology, also instructed service providers to install black boxes on their networks, allowing intelligence agencies unfettered access without a court order.

Legal Environment

The rights to freedom of speech and freedom of expression are legally protected Kyrgyzstan's constitution. Article 31 guarantees the right to freedom of thought, expression, speech, and press. Article 29 protects privacy, including private correspondence (by phone, mail, electronics, or other methods), and forbids the collection or dissemination of confidential info mation without an individual's consent. Nevertheless, the judiciary is not independent and remains dominated by the executive

19 "Kyrgyz civil society forves parliament's hand in 120 seats campaign," *Global Voices*, October 15, 2015, https://globalvoices.org/2015/10/15/kyrgyz-civil-society-forces-parliaments-hand-in-120seats-campaign/.

branch. Corruption among judges, who are generally underpaid, is also widespread, hindering the fairness of decisions in freedom of expression cases and others.

Authorities in Kyrgyzstan have responded to the threat of international terrorism by passing legislative amendments which expand the state's power to crack down a wider range of activities.[20] The amended Law on Counteracting Extremist Activities criminalize public expressions of approval and justification f extremism or terrorism, raising concerns about possible restrictions on legitimate expression online.

In July 2011, the government decriminalized libel to bring legislation in line with the new constitution. Nevertheless, "insult" remains a criminal offense and is punishable by a fine. The criminal code contains several provisions (Articles 299 and 299-1) that prohibit "inciting national, racial, religious or inter-regional hostility." In some cases, the government has sought to apply these provisions to restrict nonviolent political speech.

On May 17, 2014, the president signed an amendment to the criminal code that criminalizes the dissemination of "knowingly false messages about the commission of crimes," with the stated goal of preventing individuals from making such accusations for political reasons or to damage someone's reputation.[21] The amendment includes fines and sen ences of up to three years in prison. Detracting from the progress made through the decriminalization of libel, this amendment could potentially have a chilling effect on online journalists and regular internet users,[22] given that it is unclear exactly how the law will be interpreted. On May 28, 2014, the Association of NGOs and NCOs (noncommercial organizations) of Kyrgyzstan challenged the constitutionality of the Constitutional Chamber of the Supreme Court of Kyrgyz Republic; the Court upheld the amendment as constitutional on January 14, 2015.[23]

Over the past few years, members of parliament have proposed laws similar to ones passed in Russia that restrict civil liberties, and could have implications for freedom of expression on the net. One was almost identical to a law passed in Russia obliging NGOs receiving financing f om international organizations to register as foreign agents. The bill was eventually rejected in May 2016. [24]

In February 2014, some members of parliament submitted a draft law penalizing gay "propaganda" similar to a law passed in Russia, which includes criminal and administrative penalties for "propaganda of non-traditional sexual relationships." The draft received substantial criticism and was withdrawn; however, it was submitted again in May and it passed the fi st reading in parliament in October.[25] The draft law includes penalties of fines or imprisonment up o one year for positive images of

20 Ministry of Justice, "О внесении изменений в некоторые законодательные акты в сфере противодействия терроризму и экстремизму" [On amendments to some legal acts in the sphere of countering terrorizm and extremism] August 2, 2016, http://cdb.minjust.gov.kg/act/view/ru-ru/111441.

21 Media Policy Institute, "Депутат ЖК инициировала закон, предусматривающего наказание за заведомо ложные обвинения, содержащихся в публичных выступлениях, публикуемых в СМИ," [The deputy of JK initiated the bill, providing punishment for deliberately false accusation in public speeches published in mass-media] October 22, 2013, http://bit.ly/1OxK6GL.

22 ARTICLE 19 and PEN International, "Joint Submission to the UN Universal Periodic Review of Kyrgyzstan," June 14, 2014, http://bit.ly/1WY0tPV.

23 РЕШЕНИЕ КОНСТИТУЦИОННОЙ ПАЛАТЫ ВЕРХОВНОГО СУДА КЫРГЫЗСКОЙ РЕСПУБЛИКИ [Decision of Constitutional Chamber of Supreme Court of Kyrgyz Republic] January 14, 2015 http://constpalata.kg/wp-content/uploads/2015/01/Umetalieva-NPO-NKO-111.pdf

24 "Депутаты отклонили законопроект об иностранных агентах," [Deputies rejected the bill on foreign agents] *24 News*, May 12, 2016, http://24.kg/vlast/31834_deputatyi_otklonili_zakonoproekt_ob_inostrannyih_agentah/.

25 Resolution of Jogorku kenesh, сведения о законопроекте 6-11804/14 (Bill details 6-11804/14).

non-traditional sexual relationships shared through mass media or on the internet. In mid-2016, it was no clear when parliament will next formally consider the bill.

Another bill currently before parliament proposes to equate online news outlets as a form of mass media, requiring them to have a license and to operate with the same responsibilities as traditional media outlets.[26]

Prosecutions and Detentions for Online Activities

Authorities in Kyrgyzstan generally do not arrest netizens for expression. However, government officials, including the p esident, have demonstrated a low tolerance for personal criticism, seeking to discourage and discredit online critics by pursuing civil suits.

- In September 2015, a regional court in Kyrgyzstan upheld a decision to fine Dayirbek Oru - bekov, an editor for the online news agency Maalymat.kg, KGS 2 million (US$30,000), as compensation for damaging the honor and dignity of the president. Orunbekov[27] had posted an article accusing members of the transitional government of being responsible for the violent ethnic clashes in 2010 in the south of Kyrgyzstan.[28] He was originally charged with "knowingly disseminating false information about the commission of crimes" but that case was dismissed. Orunbekov filed a coun er-suit, seeking KGS 1 million and a public apology, but his claim was denied by the courts in February 2016.[29] In July 2016, the Maalymat.kg domain name was suspended after the court seized Orunbekov's assets.[30]

- In June 2015, Uran Botobekov, a journalist for the news portal Kabarordo.kg, was fined GS 1.8 million (US$28,000), for accusing Ikram Ilmiyanov, former deputy chief of staff of the president's office, f corruption.[31] Botobekov left Kyrgyzstan for Turkey in January 2016,

26 "Генпрокуратура Кыргызстана предлагает «законодательно к СМИ отнести интернет-издания и сайты, зарегистрированные в зоне kg»," [Prosecutor General's Office suggests " o legalize internet agencies and sites, registered in .kg zone, by inclusding them in the list of mass-media"] *24 News*, June 6, 2011, http://bit.ly/1jsVNT9.

27 "Аламудунский райсуд обязал журналиста Орунбекова выплатить президенту 2 миллиона сомов," [Alamudun district court obliged the journalist Orunbekov to pay KGS 2 million to the President] Azattyk, June 29, 2015, http://rus.azattyk.org/content/news/27100173.html; "В Бишкеке прекращено делопроизводство в отношении обвиняемого за ложное сообщение журналиста," [In Bishkek, case dropped against journalist accused of disseminating of knowingly false messages] April 16, 2015, http://bit.ly/1Ougtri; "Суд не удовлетворил иск журналиста Орунбекова к президенту Атамбаеву" [The court didn't satisfy the suit against the President Atambaev] Central Asia, February 15, 2016, http://www.centrasia.ru/news2.php?st=1455542220.

28 "Аламудунский райсуд обязал журналиста Орунбекова выплатить президенту 2 миллиона сомов," [Alamudun district court obliged the journalist Orunbekov to pay KGS 2 million to the President] *Azattyk*, June 29, 2015, http://rus.azattyk.org/content/news/27100173.html; "В Бишкеке прекращено делопроизводство в отношении обвиняемого за ложное сообщение журналиста," [In Bishkek, case dropped against journalist accused of disseminating of knowingly false messages] April 16, 2015, http://bit.ly/1Ougtri; "Суд не удовлетворил иск журналиста Орунбекова к президенту Атамбаеву" [The court didn't satisfy the suit against the President Atambaev] *Central Asia*, February 15, 2016, http://www.centrasia.ru/news2.php?st=1455542220.

29 Горсуд согласился с решением районного по иску Илмиянова [City court agreed with decision of district court on Ilmiyanov case] October 12, 2015, http://rus.azattyk.org/a/27301198.html

30 "Наложен арест на сайт maalymat.kg, принадлежащий Дайырбеку Орунбекову," [Website maalymat.kg belonging to Dairbek Orunbekov seized] *Zanoza*, July 19, 2016, http://zanoza.kg/doc/341798_nalojen_arest_na_sayt_maalymat.kg_prinadlejashiy_dayyrbeky_orynbekovy.html.

31 "Горсуд согласился с решением районного по иску Илмиянова" [City court agreed with decision of district court on Ilmiyanov case] *Azattyk*, October 12, 2015, http://rus.azattyk.org/a/27301198.html.

after which he was subject to a smear campaign initiated by Russian state TV, accusing the journalist of having to ties to former Kyrgyz president Bakiev as well as spying for Turkey. [32]

- In May 2016, Abdullo Nurmatov from Kara-Suu in the south of Kyrgyzstan, was given a one year suspended sentence for "storing and disseminating extremist content." He had "liked" photos posted by the controversial religious leader Imam Rashod Kamalov on the Odnoklassniki social network. [33] On September 10, Nurmatov was detained for 48 hours by the State Committee of National Security and then placed under house arrest.[34] Abdullo said he had been tortured to provide credentials to his account in "Odnoklassniki" and email account.

- In January 2016, Michael McFeat, a Scottish employee of gold mining company Kumtor, was arrested on charges of inciting racial hatred after jokingly referring to a Kyrgyz delicacy as "horse penis" in a post on his Facebook page. [35] Following public outrage, McFeat was pressured to remove the offending post and produce a written apology. Though he was not ultimately prosecuted, McFeat was later deported, supposedly due to issues with his visa. [36]

Surveillance, Privacy, and Anonymity

Like many former Soviet states, Kyrgyzstan maintains and updates its surveillance technology in line with Russia. Kyrgyzstan's surveillance network is modeled after Russian System for Operational-Investigative Activities (SORM) technology, and in August 2012, Kyrgyzstan updated its surveillance network to match current Russian interception systems.[37]

On June 30, 2014, the government adopted a resolution with new instructions for ISPs and mobile service providers to update their systems to the latest version of SORM technology. These instructions included requirements for service providers to store the data of their subscribers for up to three years, and to allow the authorities direct, real-time access to communications networks.[38] Service providers are also required to purchase and update equipment at their own expense to ensure compliance.

These new regulations effectively codified the po ential for mass surveillance without judicial oversight, and evidence of abuse continues to emerge. In March 2016, a recording of telephone com-

32 "На федеральном канале «Россия 1» показали сюжет про журналиста Урана Ботобекова," [Federal TV channel "Rossiya 1" showed a story about the journalist Uran Botobekov] *Institute of Media Policy*, February 19, 2016, http://www.media.kg/news/na-federalnom-kanale-rossiya-1-pokazali-syuzhet-pro-zhurnalista-urana-botobekova/.

33 "Киргизия: Житель Кара-Суу получил один год условного срока за «лайки» в соцсетях," [Kyrgyzstan: Kara-suu resident given one year suspended sentence for "likes" in social networks] May 18, 2016, http://www.media.kg/news/kirgiziya-zhitel-kara-suu-poluchil-odin-god-uslovnogo-sroka-za-lajki-v-socsetyax/.

34 "В Кыргызстане судят пользователя за «лайки» в «Одноклассниках»" [A user is in court in Kyrgyzstan for "likes" in "Odnokalssniki"] *Digital* Report, May 2, 2016, https://digital.report/v-kyirgyizstane-sudyat-polzovatelya-za-layki-v-odnoklassnikah/.

35 "Briton faces fi e years in jail for Kyrgyz sausage horse penis slur," *The Telegraph*, January 03, 2016, http://bit.ly/1mZC0wJ.

36 "My terror over Kyrgyzstan horse sausage hate mob who tried to kill me," *Sunday Post*, January 10, 2016, http://bit.ly/29MdBWL.

37 Andrei Soldatov and Irina Borogan, "Russia's Surveillance State, "*World Policy Journal* (2013) World Policy Institute, http://bit.ly/1cZerr4.

38 Ministry of Justice, Инструкция о порядке взаимодействия операторов электросвязи и операторов мобильной сотовой связи с государственными органами Кыргызской Республики, осуществляющими оперативно-розыскную деятельность (Instruction on cooperation of communication operators and mobile operators with state bodies of Kyrgyz Republic in operative investigative activities), June 30, 2014, http://cdb.minjust.gov.kg/act/view/ru-ru/96622.

munications between opposition figu es discussing a potential political upheaval were leaked to the public. Those involved were accused of attempting to forcibly seize power and they remain detained by authorities.[39] In May 2016, telephone conversations between leaders of the People's Parliament opposition group were also leaked online, revealing discussions about seizure of power and also leading to their arrest.[40] It is not clear how these recordings were obtained but the pattern of targeted opposition leaders suggests abuse of SORM equipment by the government.

Since February 2012, the Civil Initiative on Internet Policy, together with the Kyrgyz State Committee on National Security and several human rights organizations, have been working on amendments to the statute on the Conduct of Investigations—the body responsible for regulating these issues—that would clarify the circumstances surrounding the use of interception technology and provide a more adequate legal framework. The bill is yet to reach parliament for consideration.

There are currently no strict restrictions on anonymous communication on the internet in Kyrgyzstan. Websites do not need to register, encryption software is freely available, and real-name registration is not required to post content online. However, on February 17, 2014, the government issued a new regulation requiring mobile operators to sell new SIM cards only after they have been registered (previously, SIM cards could be registered within one year of purchase). This new regulation came into force on March 8, 2014, making it more difficult for individuals o use ICT tools anonymously.[41]

Intimidation and Violence

In general, there is not a significant le el of violence or harassment against ICT users in Kyrgyzstan, though some isolated incidents could be related to online activities.

- In February 2016, Turat Akimov, the editor in chief of the newspaper Деньги и власть (Money and power) and corresponding website bishkekinfo.kg, was violently attacked near his home. The attacker struck him with a steel pole and fled the scene. Akimov has published material critical of the government,[42] and says the attack was in retaliation for his professional activities.

- In February 2014, a youth group participating in a rally against LGBTI (lesbian, gay, bisexual, transgender, and intersex) people burned a photo of Ilya Lukash and called him a "destroyer of family values." Lukash is an active blogger and an advocate for human rights of LGBTI people; he has also made statements against Kyrgyzstan joining the Eurasian Customs Union and protested in solidarity with the Ukrainian "Euromaidan" demonstrations. Following this incident, Lukash said on Facebook that the increasing pressure and harassment had forced him to leave Kyrgyzstan.

39 "В сети появилась аудиозапись, где якобы оппозиционеры обсуждают формирование правительства в случае захвата власти" [An audio record appeared in Internet of opposition leaders discussing seizure of power] *24 News,* March 27, 2016, http://www.24.kg/obschestvo/29731_v_seti_poyavilas_audiozapis_gde_yakobyi_oppozitsioneryi_obsujdayut_formirovanie_pravitelstva_v_sluchae_zahvata_vlasti/

40 "В сеть слили переговоры якобы членов "Народного парламента"" [Conversations between members of the People's Parliament leaked online] Zanoza, May 12, 2016, http://zanoza.kg/doc/338066_v_set_slili_peregovory_iakoby_chlenov_narodnogo_parlamenta.html.

41 Government Public Relations Agency, "Об утверждении Правил оказания услуг подвижной радиотелефонной связи," [On approval of regulations of mobile telecommunication services] press release, February 25, 2014, http://bit.ly/1G9UmDN.

42 "Неизвестные избили журналиста Турата Акимова," [Unidentified attac ers beat journalist Turat Akimov] *Bishkek Evening*, February 20, 2016, http://www.vb.kg/doc/334765_neizvestnye_izbili_jyrnalista_tyrata_akimova.html.

Technical Attacks

Instances of politically motivated cyberattacks are rare, though government web resources are occasionally targeted. In June 2016, the website of the State Committee on Defense Affairs,[43] and in July 2016 website of the State Committee of National Security,[44] were both hacked, demonstrating that state run websites continue to operate with some security weaknesses.

In 2005, the OpenNet Initiative recorded the extensive use of distributed denial-of-service (DDoS) attacks against opposition and news websites, demonstrating a precedent for such attacks.[45]

43 "Сайт Госкомитета по делам обороны был взломан хакерами," [Website of the State Committee on Defense Affairs hacked] *Zanoza*, June 21, 2016, http://zanoza.kg/doc/340365_sayt_goskomiteta_po_delam_oborony_byl_vzloman_hakerami.html.

44 "Взломан сайт ГКНБ," [Website of SCNS hacked] *Kabar*, July 27, 2016, http://kabar.kg/rus/society/full/109156.

45 OpenNet Initiative, "Country Profile: yrgyzstan," December 18, 2010, http://opennet.net/research/profiles/ky gyzstan.

Freedom House

Lebanon

	2015	2016
Internet Freedom Status	Partly Free	Partly Free
Obstacles to Access (0-25)	13	13
Limits on Content (0-35)	12	12
Violations of User Rights (0-40)	20	20
TOTAL* (0-100)	**45**	**45**

* 0=most free, 100=least free

Population:	**5.6 million**
Internet Penetration 2015 (ITU):	**74 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Partly Free**

Key Developments: June 2015 – May 2016

- The Ministry of Telecommunications launched a major plan to expand fiber-optic infrastructure to bring greater internet access and higher speeds throughout the country (see **Availability and Ease of Access**).
- Activists used social media to reclaim public space from corporations, document harassment against women, and rally thousands of people in the "You Stink" protests against the country's garbage crisis (see **Digital Activism**).
- Human rights activist Nabil al-Halabi was arrested on May 30 for Facebook posts that called for the Interior Ministry to "cleanse itself up" after a corruption scandal. Police detained al-Halabi for four days and pressured him into signing a pledge to refrain from further criticism (see **Prosecutions and Detentions for Online Activities**).
- Three individuals were arrested in the city of Sidon for defaming the city and its religious figu es through Facebook posts. Numerous individuals were briefly detained or interrogated by the Cybercrime Bureau for criticizing public figures online (see **Prosecutions and Detentions for Online Activities**).

Introduction

The internet freedom environment in Lebanon remained static over the past year with the Cybercrimes Bureau continuing to interrogate users for criticizing public figures online.

One of the main events over the coverage period was Lebanon's "You Stink" protests against the country's garbage crisis, which escalated into widespread contempt for public mismanagement and the political class. Civil society activists took to social media and rallied thousands of followers to several demonstrations, principally in the capital Beirut. However, the authorities often responded with excessive force, and in one case in August 2015, live rounds were shot at protestors.[1]

Generally speaking, activists and journalists face potential arrest, interrogation, and threats of bodily harm for online posts that criticize the government, religious officials, or the army. The Bureau of Cybercrime and Intellectual Property Rights (Cybercrime Bureau) remains highly active in targeting activists, often in a manner that demonstrates little respect for the rule of law. Police have conducted early morning house raids to arrest activists and journalists for nonviolent defamation charges. Numerous attempts to reform the country's media laws have failed over the years and strict defamation laws remain a significant impediment to free speech and citizen journalism online.

Lebanese citizens have historically boasted a strong tradition of freedom of the press and media pluralism. With respect to information and communication technologies (ICTs), however, the country has struggled to keep up with its more technologically advanced neighbors in the Arab world. Although the government introduced a plan to expand fiber-optic cables in mid-2015, a lack of competition in the ICT market has plagued innovation and development. Online censorship is rare, but websites owners, particularly news sites, often receive informal requests to remove content that may be seen as defamatory. In total, 50 websites were blocked over the coverage period, mainly for content related to escort services, Israel, gambling, or alleged child pornography. Surveillance remains a strong concern in the country, particularly given the impunity of the security forces and a perceived lack of transparency and accountability in all areas of government.

Obstacles to Access

Lebanon continues to struggle with poor telecommunications infrastructure, slow speeds, an urban-rural divide, and a lack of competition in the ICT sector. The state company Ogero maintains a monopoly over internet services in the country, while two state-owned mobile phone companies essentially split the mobile market between themselves. The country's ICT development has been consistently stalled by mismanagement and political tensions, although there were some signs of improvement over the past year, notably the "Digital Telecom Vision 2020" plan to replace old copper cables with fiber-optics across the country.

Availability and Ease of Access

According to the International Telecommunication Union (ITU), an estimated 74 percent of individu-

1 See "You Stink Protests fi e up Beirut" *Alyawm Alsabeh,* August, 22, 2015, http://bit.ly/2e5rQcs. and "Beirut Riot Police Fire Live Ammo and Blast Protestors with Water Cannons," *Vice News*, August 22, 2015, https://news.vice.com/article/beirut-riot-police-fi e-live-ammo-and-blast-protesters-with-water-cannons.

als use the internet in Lebanon as of 2015, a marked increase from 44 percent five years ago.[2] There are an estimated 22.76 fixed broadband subscriptions per 100 inhabitants, up from 7.63 in 2010. The figure rises to 53.5 for mobile broadband subscriptions, ranking Lebanon 57th worldwide, above the likes of Israel (58th), Tunisia (67th) and Jordan (114th), although well behind the Gulf Arab countries.[3]

Prices for internet access are set by the government. A decree by the Ministry of Telecommunications lowered fees on broadband by 44 to 68 percent as of July 2014, depending on bandwidth rates.[4] That same month, mobile phone providers expanded the capacity of broadband bundles between 55 percent and 300 percent without changing the initial prices. Therefore, the 500 megabyte bundle was offered for a fixed price of $10 (excluding value-added tax) for both fixed and prepaid mobile users.[5] ISPs cannot lower prices unless a decree is issued by the Ministry of Telecommunications.[6] Tariff decree number 6297, adopted on November 9, 2011, allowed for 20 percent discounts on DSL prices in educational institutions, and decree number 8058, issued on April 25, 2012, made internet access free between midnight and 7a.m., and free all day in public parks.[7]

Despite the ministry's slow response to much-needed repairs and upgrades outside of major urban areas, some progress has been achieved. For instance, in an attempt to curb the internet penetration disparity between urban and rural areas, a recent initiative called "the Dari bundle" allows some 200,000 citizens living in 210 remote towns with no access to DSL to get free phone sets and monthly mobile internet pricing equal to the fixed DSL price.[8] Nevertheless, some 300 villages in the rural regions of Keserwan, Batroun, Nabatiyeh, and Bekaa still lacked access, mainly due to a lack of a fixed telephone network in the area.[9] Many in Lebanon, particularly in rural areas, experienced constant cuts to telecommunications services due to harsh weather conditions and energy cuts.

On July 2, 2015, Minister of Telecommunications Boutros Harb launched the "Digital Telecom Vision 2020" plan to renovate telecommunications infrastructure. This plan aims to bring fiber-optic connections to nearly 15,000 economic enterprises as well as government institutions.[10] The plan also includes progressively expanding the fiber-optic network, from neighborhoods with high population density to more rural areas throughout the country. Harb estimated the initial cost of the plan at more than US$ 600 million.[11] Nonetheless, beyond the launch of the initiative, there have been few noticeable steps taken to improve connectivity and the ministry continues to lack transparency.[12]

Restrictions on Connectivity

2 International Telecommunication Union, "Statistics," June 2016, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

3 International Telecommunication Union, "The State of Broadband," September 2015, http://www.broadbandcommission.org/Documents/reports/bb-annualreport2015.pdf.

4 Telecommunications Regulatory Authority, *Annual Report 2014*, [in Arabic] http://www.tra.gov.lb/Annual-reports.

5 Telecommunications Regulatory Authority, *Annual Report 2014*, [in Arabic] http://www.tra.gov.lb/Annual-reports.

6 Livia Murray, "Four reasons Lebanon's internet is so slow," *Executive Magazine*, April, 8, 2015, http://bit.ly/1aufiX .

7 Ministry of Telecommunications, *Progress Report 2013,* http://www.mpt.gov.lb/documents/AnnualReports/MOT_brochure_en-corr.pdf

8 Caretaker Telecoms Minister Nicolas Sehnaoui, Facebook page, January 20, 2014, http://on.fb.me/1bEu47U.

9 «هذه المناطق اللبنانية محرومة من الإنترنت حتى إشعار آخر»،[These Lebanese Regions have no access to internet till Further Notice], *An-Nahar*, April, 9, 2015, http://bit.ly/1UC5O1o.

10 "Minister Boutros Harb Launches the 2020 Plan," Republic of Lebanon Ministry of Telecommunications, July 2015, http://www.mpt.gov.lb/index.php/ar/2013-02-17-13-15-34/mpt-news-ar/50-latest/373-2015-07-01-15-17-30.

11 Launching a vision for Digital Media, *AlMustakbal,* July 2, 2015, http://www.almustaqbal.com/v4/article.aspx?Type=NP&ArticleID=667004.

12 "Plan of (In) Action," *Executive,* January 11, 2016, http://www.executive-magazine.com/opinion/plan-of-inaction.

The Lebanese government maintains a monopoly over the internet backbone, as well as over the fixed and mobile telephone industry in general, allowing it to exercise tight control over internet service providers (ISPs). Lebanon has three international border gateways—in Beirut, Jdeideh, and Tripoli—where three underwater fiber-optic cables connect the country via the IMEWE, Cadmos, and Berytar cables.[13] The gateways are operated by Ogero, a state company headed by Abdulmenaim Youssef who, in an apparent conflict of interest, also occupies a position within the Ministry of Telecommunications that oversees the operations of Ogero.

ICT Market

The Lebanese telecommunications industry is government-owned and tightly regulated. In addition to running the backbone, Ogero sets internet prices and shares in the management of online subscriptions, together with two dozen private ISPs.[14] Lebanon has two government-owned mobile phone companies, Alfa and Touch, which are run by the private companies Orascom Telecom Holdings and Zain, respectively.[15] Because the government sets prices and issues permits for the number of subscriptions allowed, there is little competition in the industry, and the two companies split the market evenly between themselves.[16] The fixed-line telephone and internet network is owned and operated by Ogero, from whom all companies must purchase services.

Since no law regulates their licensing, private ISPs currently obtain a permit by decree from the Ministry of Telecommunications.[17] Crucially, political influence can significantly interfere with the allocation of contracts to private ISPs and mobile phone operators.[18] Lebanese authorities discovered that some companies had installed large amounts of equipment in several areas in order to provide illegal internet services from foreign-based connections. Telecommunications Minister Harb issued several complaints to the public prosecutor in an effort to put an end to "people extending internet services through illegal means."[19]

Regulatory Bodies

Lebanese media and telecommunications laws are regulated by three semi-independent advisory bodies that report to the Council of Ministers. The National Council for Audiovisual Media and the Committee for Establishing Model Bylaws and Practices deal mainly with audiovisual media (TV, radio, and satellite), while the Telecommunications Regulatory Authority (TRA) is responsible for liberalizing, regulating, and developing the telecommunications sector. Overall, the three bodies remain largely powerless and fail to live up to their expectations as independent regulators in a modern state. While in theory the TRA is independent from the government, in reality, dominant Lebanese

13 Livia Murray, "Four reasons Lebanon's internet is so slow," *Executive Magazine*, April, 8, 2015, http://bit.ly/1aufiX .

14 Telecommunications Regulatory Authority , "Facts and Figures," December 2011, http://www.tra.gov.lb/Market-Data-Facts-and-figu es.

15 Touch, "About Us," http://bit.ly/1MhupRM; and Alfa, "About Alfa," https://www.alfa.com.lb/aboutus/companyinfo.aspx.

16 "The Next Step," *The Business Year,* http://www.thebusinessyear.com/publication/article/2/48/lebanon-2012/the-next-step.

17 According to the Telecommunications Regulatory Authority (TRA), it is TRA's prerogative to assess and grant license to ISPs, but the past three ministers of telecommunication have considered that the TRA has no legal authority to do so, and the ministry has used an old law as a basis for their right to grant such license. See below for conflicts bet een the TRA and the Telecommunications Ministry.

18 Jad Melki, et. al., *Mapping Digital Media: Lebanon*, Open Society Foundations, May 2012, 89, http://osf.to/1EOX3Kt.

19 "Lebanon telecoms minister launches crackdown on illegal internet providers," *The Daily Star*, March 8, 2016, http://www.dailystar.com.lb/News/Lebanon-News/2016/Mar-08/341143-lebanon-telecoms-minister-launches-crackdown-on-illegal-internet-providers.ashx#.Vt6-A2MyoAM.twitter.

political groups possess a great deal of influence over the institution, often rendering it powerless.[20] For this reason, the Ministry of Telecommunications remains the strongest player in the ICT domain. In fact, the past three telecommunications ministers have gone so far as to claim that the TRA has no real authority, given that the law establishing its powers has not yet been implemented.[21] Tellingly, since its launch in 2007, many of the TRA's objectives have not been met, namely the transition from analog to digital networks and the privatization of the telecommunications sector.

Limits on Content

Lebanon does not engage in significant filtering of internet content. Fifty websites were reportedly blocked over the coverage period, mainly for content related to escort services, Israel, gambling, and alleged child pornography. Websites owners, particularly news sites, often receive informal removal requests from public officials or powerful figures. Despite these limitations, Lebanon retains one of the most diverse digital landscapes in the Arab world, and several nongovernmental organizations engage in digital activism on political and social issues.

Blocking and Filtering

Over the past year, 50 websites remained blocked in Lebanon, the same figure as last year.[22] Among the remaining websites blocked were:

- 23 websites related to escort services, blocked in accordance with articles 523 and 524 of the penal code;
- 11 Israeli sites, in accordance with Decree 12562 of April, 19, 1963, which called for the boycotting of Israel;
- 8 gambling websites, according to Law 417 of 1995, which gives the "Casino Du Liban" exclusive rights to the gambling industry;
- 5 pornographic websites for allegedly promoted child pornography;
- 2 websites for breeching copyright, following a request from the U.S. government;
- 1 website, identified as being a forum for Lesbians in the Arab region, was blocked. Article 534 of the penal code criminalizes "sexual intercourse contrary to the order of nature" with up to one year in prison, and has been used to prosecute LGBTI (lesbian, gay, bisexual, transgender, and intersex) individuals.[23]

While many of these blocking orders are rooted in the law, the move to block six pornographic websites for alleged child pornography drew the ire of some digital rights activists for the way that they

20 Jad Melki, et. al., *Mapping Digital Media: Lebanon*, Open Society Foundations, May 2012, 34 and 82.
21 Sami Halabi, "Redialing discord?" *Executive Magazine*, July 3, 2011, http://bit.ly/1JUw5xC.
22 Social Media Exchange, "Mapping Blocked Websites in Lebanon 2015," March, 26, 2015, http://bit.ly/1NiBh2Z.
23 Sophie Chamas, "The fight goes on for Le anon's LGBT community," Al Monitor, June 15, 2015, http://www.al-monitor.com/pulse/originals/2015/06/lebanon-lgbt-gay-rights-article-534-helem-legal-agenda.html.

were chosen.[24] According to reports, the order came after an alleged child molester in Lebanon was reported to the Bureau of Cybercrimes from a police station in Manchester, UK. Sources from the Bureau of Cybercrimes who were present during the interrogation of the accused individual revealed that the websites were chosen because they appeared in the browser history of his personal laptop, and not necessarily because they published child pornography.[25] A prominent Lebanese blogger and social media expert wrote that the websites were among the most famous pornographic websites worldwide and were unlikely to feature child pornography, given that they are not censored in other countries that ban child pornography.[26]

Websites are blocked through court order. Commonly, the court receives a complaint and files it with the Cybercrimes Bureau for further investigation, later issuing a final order to the Ministry of Telecommunications, which then blocks the websites through Ogero. Website owners are not notified that their websites have been blocked but must appeal the blocking within 48 hours in order to have it overturned. In November 2014, the head of the Cybercrimes Bureau stated that terrorist content was being monitored and that the bureau had the ability to filter it.[27] Digital media specialists in Lebanon have expressed doubt over the bureau's abilities in this regard, though the overreaching intention to filter the web remains a cause for concern for some.

YouTube, Facebook, Twitter and international blog-hosting services such as WordPress and Blogger are freely available. In fact, Facebook, Google, YouTube, Microsoft's Live.com, and Wikipedia rank among the top 10 most visited websites in Lebanon.[28] In 2010, the government-owned phone company Ogero installed equipment to block VoIP throughout the network, but subsequently backed down under pressure from businesses, civil society, and politicians. Furthermore, the VoIP service Vonage was blocked, although other VoIP services such as Skype and WhatsApp are available.[29] VoIP services are restricted by law under the 2002 Telecom Act[30] and the government has been somewhat vague as to its enforcement.[31]

Content Removal

While filtering remains rare, there have been limited incidents in which government security officials pressured individuals and ISPs to remove certain comments—mainly criticism of government officials or the army—from social media pages, blogs, or websites. For example, in November 2014 Judge Nadim Zwein issued a decree obliging the newspaper *Al-Akhbar* to remove a report from its website discussing corruption at the American University of Beirut (AUB) in response to a request

24 Samir Kassir Eyes, «القاضي العام يأمر بحجب ستة مواقع إباحية في إطار فحص التحرش بالأطفال»,[General Prosecutor Orders the blocking of Six Porn sites], Skeyes Center for Media and Cultural Freedom, September, 2, 2014, http://www.skeyesmedia.org/ar/News/Lebanon/4728.

25 Eyes, «القاضي العام يأمر بحجب ستة مواقع إباحية في إطار فحص التحرش بالأطفال», [General Prosecutor Orders the blocking of Six Porn sites].

26 Imad Bazzi, «كيف ولماذا حجبت المواقع الإباحية في لبنان؟»[How and Why Six Porn Websites were Banned in Lebanon], September, 3, 2014, http://trella.org/4234.

27 Dhouha Ben Youssef, "Arab IGF III: What we will remember," Nawaat, December 3, 2014, http://nawaat.org/portail/2014/12/03/arab-igf-iii-what-we-will-remember/.

28 Alexa, "Top Sites in Lebanon," accessed October 16, 2016, http://www.alexa.com/topsites/countries/LB.

29 Telecoms 2013 Progress Report, January 3, 2014, http://bit.ly/1oa28kP.

30 Imad Atalla, "Lebanon is stifling our digital freedom," *The Daily Star*, June 8, 2010, http://bit.ly/1QoURu9..

31 Telecoms 2013 Progress Report, January 3, 2014, http://bit.ly/1oa28kP.

from the university.[32] Meanwhile, online media outlets and blogs usually have a disclaimer on their comments section making clear that they may remove any comments that include foul language or fall outside of the ethical codes. According to one expert, there is no law that clarifies who can be held liable for user generated content, such as comments. Nonetheless, there have been no recent cases of intermediaries being prosecuted.[33]

Media, Diversity, and Content Manipulation

Despite evidence of some filtering, taboo subjects that would normally be banned from mainstream media outlets, such as pornography, content supportive of Israel, and sectarian hate speech, are generally available online. However, self-censorship is prominent in the blogosphere and in the country's top media outlets, which are owned by powerful figures from all sides of the political spectrum. Users often fear repercussions from the government or certain political and sectarian groups. Due to the fact that promoting or supporting LGBTI issues is a crime under the penal code, content about the LGBTI community operates in a legal gray zone and may result in censorship.

Lebanese users have access to a wide variety of local and international information sources. Reflecting Lebanon's pluralistic society, Lebanese media is highly partisan and controlled by the dominant political-sectarian actors, mainly through direct ownership of prominent media outlets.[34] For example, former prime minister Saad Hariri owns Future TV, *al-Mustaqbal*, *the Daily Star*, and a host of other online and offline media outlets. Similarly, Speaker of Parliament Nabih Berri owns National Broadcasting Network and its affiliates, while Hezbollah controls a vast network of media outlets, including al-Manar TV and al-Nour radio. The heads of these media outlets are chosen by these dominant political figures, and their news content clearly advances a particular partisan message.

While ensuring plurality, this also creates a climate in which the public sphere is dominated by the agendas of powerful political-sectarian leaders and their allies, suffocating the voices of those who fall outside the main groups.[35] At the same time, politicians are known to bribe the few independent news outlets and journalists that do exist, particularly during election periods. Independent digital media outlets struggle for sustainability due to Lebanon's relatively weak digital advertising market. The majority of advertising revenue continues to go to television and other traditional media, while digital sources make up around 13 percent of total advertising spending as of 2015.[36] One of the main obstacles to boosting the digital advertising market is Lebanon's slow and unreliable internet.[37]

Digital Activism

Lebanese users employed digital tools during the "YouStink" protests against the government's failing waste management policies in the capital Beirut. As Mohamad Najem, co-founder of Social Me-

32 «قاضي الأمور المستعجلة يُلزم جريدة «الأخبار» إزالة تقرير عن موقع إلكتروني», [Judge forces Al Akhbar Newspaper to remove a Report from its Website], Samir Kassir Foundation, November 21, 2014, http://www.skeyesmedia.org/ar/News/Jordan/4874.

33 Interview with President of ICT committee in the Beirut BAR association and Dr. Charbel Kareh, Head of communication committee in Internet Society - Lebanon chapter, April, 8, 2015.

34 Melki et. Al., *Mapping Digital Media: Lebanon*, 21-22.

35 Melki et. Al., *Mapping Digital Media: Lebanon*, 56-58.

36 Marwan Mikhael and Lana Saadeh, "Digital Advertising in Lebanon," Blominvest Bank, October 23, 2015, http://blog.blominvestbank.com/wp-content/uploads/2015/10/Digital-Advertising-in-Lebanon.pdf.

37 Elias Sakr, "Online advertising untapped in Lebanon," *The Daily Star*, April 20, 2012, http://bit.ly/1Q1IH9T.

dia Exchange (SMEX), stated, "Social media has been by default the space activists and communities go to disseminate their messages."[38] Najem and other activists drafted a successful online petition pressuring service providers Alfa and Touch to address network congestion during the protests.[39] YouStink's official Facebook page had almost 200,000 followers by mid-2016 and continues to rally Lebanese to protest, to disseminate information about the garbage crisis, and to shame Lebanese officials into taking action.[40]

Over the past year, another online campaign successfully lobbied to reclaim a public space through a mix of petitions and organizing. The al-Dalia campaign relates to a public space next to the iconic Raouchi Rock in Beirut where many families gathered to fish and enjoy sunset views.[41] The space was bought by a powerful Lebanese political and business family who wanted to build on the site. Instead, the site was officially protected by the Global Heritage Fund.[42] Al-Dalia was awarded the Wajih Ajouz Award for best online campaign in Lebanon given by the Samir Kassir Foundation.[43]

A group of female activists launched an online forum where victims or witnesses of sexual harassment can report incidents and pin the location on a map for later use as evidence.[44] The Samir Kassir Foundation also launched a smart phone application by the name LOG&Learn with the aim of fact-checking misinformation often propagated about the little-known oil and gas sector in Lebanon.[45]

Violations of User Rights

Lebanon's weak legal environment, overzealous interrogations by the Cybercrime Bureau, and ongoing surveillance remained a grave threat to user rights over the past year. The country continues to lack a legal framework for online media, instead applying harsh defamation laws have been used to curtail investigative reporting and criticism of public authorities. While no users were reportedly sentenced to jail time over the coverage period, the Cybercrime Bureau continued to interrogate and detain individuals for their online speech, largely as an intimidation tactic.

Legal Environment

The Lebanese constitution guarantees freedom of expression as well as freedom of the press, although those rights have not always been respected in practice. No legal provisions relate specifically to online speech, although many activists have been anticipating a new law for over a decade. Meanwhile, courts apply these and other traditional media laws to the online sphere in an inconsistent and often contradictory fashion.[46] This has produced a confusing legal environment with overlapping jurisdictions and contradictory laws governing online content, including the civil laws, penal

38 Interview with Mohamad Naajem, co-founder of Social Media Exchange (SMEX)

39 "Alfa and Touch Boost Coverage at August 29 Protest," SMEX, http://www.smex.org/petition-to-alfa-touch/v.

40 YouStink official acebook page, https://www.facebook.com/tol3etre7etkom/?fref=ts.

41 Aldalia Campaign official acebook page, https://www.facebook.com/dalieh.org/.

42 "Dalia Raouchi placed on Global Heritage Fund 'Watch List'," *Al-Akhbar,* Oct 21, 2015, http://al-akhbar.com/node/244265.

43 "AlDalia campaign wins the Wajih Ajouz Award for best online campaign in 2015," Samir Kassir Foundation, December 13, 2015, http://www.skeyesmedia.org/ar/News/Lebanon/5543.

44 Harass Tracker Addresses Sexual Harrasment, *SMEX,* March 4, 2016, http://bit.ly/2eVINFo.

45 "As subject of oil and gas heats up, app helps get facts straight," *The Daily Star,* March 2, 2016, http://www.dailystar.com.lb/News/Lebanon-News/2016/Mar-02/340100-as-subject-of-oil-and-gas-heats-up-app-helps-get-facts-straight.ashx.

46 Melki, et. al., *Mapping Digital Media: Lebanon*, 86.

code, publications law, audiovisual law, elections law, and military code of justice.[47] Three serious attempts to develop new media laws have generated heated national debates in the past six years, although none so far have led to any concrete results.[48]

From a legal perspective, the most serious threat to internet users and online journalists remains the country's slander and libel laws. Under Article 588 of the Lebanese penal code, defaming the president carries a sentence of 3 to 12 months in prison, while defaming the army or other public figures carries a sentence of up to 6 months.[49] The appeals process is often drawn out and highly politicized. In practice, however, most online users targeted with such accusations are quickly released, or cases are dropped under public or political pressure. Violations of press freedom typically receive an immediate and passionate reaction from the public, serving as a powerful check against the government's actions.

Prosecutions and Detentions for Online Activities

Court trials and prison sentences against individuals for online posts were not common over the coverage period. Instead, security forces often detained users or called them in for interrogations, particularly at the Bureau for Cybercrimes. The bureau was created in 2006 without a formal legislative decree setting out its activities or defining a "cybercrime."[50] In fact, the bureau often acts with little regard to the law. The bureau often pressures users to apologize, delete the controversial content, and sign a letter promising not to harm the person or group in the future. While some cases have reached the court, they are not publically known.[51]

Prominent activist Nabil al-Halabi was arrested on May 30, 2016 over Facebook posts in which he accused the interior ministry of corruption and potential collusion with sex traffickers. Al-Halabi is a lawyer and director of the Lebanese Institute for Democracy and Human Rights. In April, Interior Minister Nohad Machnouk had accused him of libel and defamation, filing a suit with the public prosecutor's office in Beirut. Internal Security Forces arrested al-Halabi during an early morning house raid for failing to appear in court to respond to defamation charges brought on by a senior advisor to Machnouk. Al-Halabi's lawyer claimed his client had not been officially informed of the latter charges.[52] He was detained for four days and not released until after he was pressured into signing a pledge not to criticize Machnouk in the future.[53]

Ali Jomaa, Youssef Kleib, and Youssef Fnas were all arrested together outside of a mosque in the city of Sidon, in southern Lebanon for writing Facebook posts that were considered "defaming to citizens of Sidon and its Mufti Sheikh Salim Sousan."[54] The three individuals were released the next day.

47 Melki, et. al., *Mapping Digital Media: Lebanon*, 89.

48 International Research and Exchange Board, "Development of Sustainable Independent Media in Lebanon," in *Media Sustainability Index 2010/2011,* (Washington D.C.: IREX, 2012)*http://bit.ly/1NqhOyU*.

49 Lebanese Army, "Slander and libel and sanctions in Lebanese law crimes," [in Arabic], 2010, http://bit.ly/1IYP0Wp.

50 Legal Agenda, "Bureau of Cybercrimes: An Unorganized Online Censorship," [in Arabic] http://bit.ly/1KavsU6.

51 Interview with Mohamad Naajem, co-founder of Social Media Exchange (SMEX)

52 "Lebanon: Lawyer Held for Facebook posts," Human Rights Watch, May 31, 2016, https://www.hrw.org/news/2016/05/31/lebanon-lawyer-held-facebook-posts.

53 "Lebanon lawyer denies wrongdoing, demands apology over house raid," *The Daily Star*, June 3, 2016, http://www.dailystar.com.lb/News/Lebanon-News/2016/Jun-03/355191-lebanon-lawyer-denies-wrongdoing-demands-apology-over-house-raid.ashx.

54 "Arrests in Sidon over posts that were considered defaming to Sidon and its Mufti," (Arabic) *an-Nahar*, January 10, 2016, http://bit.ly/2eVgR4t.

After journalist Ali Khalifeh shared satirical, altered images of the late former prime minister Rafik Hariri on Facebook, security forces stormed his house outside of Sidon. He was not home at the time and subsequently went to the police station, where he was reportedly subjugated to a three hour interrogation by Judge Rahif Ramadan at the Justice Palace of Sidon on charges of "defacing and spreading online images" of the assassinated prime minister.[55]

Four other individuals were interrogated by the Cybercrimes Bureau for Facebook posts that criticized the judiciary system, the former president, and even a song by the pop star Mohamed Iskandar.[56]

Surveillance, Privacy, and Anonymity

The laws regulating surveillance and the acquisition of communications data are vague and widely disputed. Attempts to develop clear privacy laws and regulations have failed, mainly because of their highly politicized nature. Currently, the typical process for acquiring user data involves a request from the Internal Security Forces (ISF) to the Ministry of Interior (or from the army to the Ministry of Defense), which is then sent to the prime minister for approval. The order is then sent to the telecommunications minister for execution—although in some instances the latter has refused to hand over the data to the ISF. This process was approved by the cabinet of ministries in 2009 as part of an agreement to share communications data with security and military officials. However, those who dispute this process, particularly the last three telecommunications ministers, cite the need to obey privacy laws, and insist that the government's 2009 decision is limited to metadata and does not cover requests for the content of communications and other specific data. During their respective periods in office, the ministers argued that large-scale, broad requests from the ISF should be accompanied by a court order.

While ISPs and mobile phone providers are state-owned, observers noted that data is only shared with security forces if they received a court order for a limited time interval and a limited number of users. Lebanon's first draft law on personal data protection was reportedly under discussion at the parliament over the coverage period.[57] Individuals are not usually required to show any form of ID for obtaining a prepaid SIM card, however some points of sale required it for security reasons.

Intimidation and Violence

Physical acts of violence in retaliation for online speech were rare in Lebanon. However, traditional journalists were subject to excessive violence against protestors during the "YouStink" protests, particularly on August 22 and 23, 2015. Cameramen and reporters from numerous outlets were beaten by security force, and in many cases their cameras were broken.[58]

55 "Lebanese police summon man for photoshopping Rafic Hariri pos ers," *The New Arab*, February 9, 2016, https://www.alaraby.co.uk/english/news/2016/2/9/lebanese-police-arrest-man-for-photoshopping-rafi -hariri.

56 The Museum of Censorship, http://www.censorshiplebanon.org/Categories/Internet, accessed July 2016.

57 Interview with President of ICT committee in the Beirut BAR association and Dr. Charbel Kareh, Head of communication committee in Internet Society - Lebanon chapter, April, 8, 2015.

58 "Numerous Attacks on Journalists during YouStink Protests," Samir Kassir Foundation, August 24, 2015, http://www.skeyesmedia.org/ar/News/Lebanon/5346.

Technical Attacks

Only two incidents of website hacking were widely reported over the past year. Both the Arabic and English Facebook pages of the online media outlet "Now Lebanon" were hacked by a group calling itself "The Online Syrian Revolutionary Army."[59] Hacker affiliated to the so-called Islamic State also hacked the website of Future TV.[60]

59 "NowLebanon Facebook pages were hacked," Samir Kassir Foundation, July 8, 2015, http://www.skeyesmedia.org/ar/News/Lebanon/5272.

60 "SKeyes Monthly Report," *NNA*, December 8, 2016, http://nna-leb.gov.lb/ar/show-news/195263/nna-leb.gov.lb/ar.

Freedom House

Libya

	2015	2016
Internet Freedom Status	Partly Free	Partly Free
Obstacles to Access (0-25)	20	20
Limits on Content (0-35)	12	13
Violations of User Rights (0-40)	22	25
TOTAL* (0-100)	**54**	**58**

* 0=most free, 100=least free

Population:	**6.3 million**
Internet Penetration 2015 (ITU):	**19 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- Telecommunications services have been regularly disrupted due to vandalism and technical disruptions. In the coastal town of Sirte, Islamic State militants disabled all phone networks and banned satellite connections (see **Restrictions on Connectivity**).
- Two people were arrested for social media posts criticizing the military or police units, including blogger Ali Asbali, who was imprisoned for 120 days (see **Prosecutions and Detentions for Online Activities**).
- Disputes over political legitimacy have fil ered into the digital sphere, with competing governments reportedly taking over each other's online accounts (see **Technical Attacks**).

Introduction

Internet freedom declined in Libya due to increased polarization in online media and the unprecedented arrest of two bloggers in Benghazi.

The situation in Libya was tenuous over the coverage period, with an ongoing political crisis, fighting between armed militias, and the Islamic State group securing a stronghold in the coastal town of Sirte. A new unity government—the Government of National Accord (GNA)—was formed in January 2016 after a series of UN-sponsored talks between two competing governments. The Tripoli-based government is linked to the General National Congress (GNC), a legislative body that had been elected in 2012 and unilaterally reinstated itself in 2014 after rejecting the outcome of Libya's June 2014 elections. The other government was based in the eastern the cities of Tobruk and Beida and linked to the House of Representatives (HOR), the legislative body that was elected in those June 2014 elections. UN-sponsored talks to form the GNA unity government partly succeeded in reducing violence between the competing governments.[1] However, while the GNA received some degree of domestic support and international recognition and managed to establish a presence in the capital Tripoli, spoilers linked to both competing factions refused to respect the legitimacy of the new government. On January 25, 2016 HOR crucially voted to reject the GNA.[2] The GNA's authority failed to penetrate large swaths of territory, which remained outside of all formal state and government control. Amid this vacuum, the Islamic State consolidated a stronghold in the coastal city of Sirte and fighting continued during art of the coverage period in the southern region between Touareg and Tebu tribes.[3] General lawlessness and violence between local tribes, militias, and gangs continued in pockets around the country.[4]

The national crisis has had a devastating effect on internet freedom in Libya. Prices for internet connections and SIM cards have soared due to limited availability and difficulties transpo ting goods within the country. Telecommunications services have been regularly disrupted due to attacks on power stations, the destruction of infrastructure or the theft of supplies, and the shutting down of networks—in the case of Sirte, which is under Islamic State rule. In one striking example, an armed militia stole 500 telegraph poles from trucks belonging to the national electric utility and took the drivers hostage.[5] Marking one of the most significant instances f online censorship since the revolution, the news site *al-Wasat* was blocked in February 2014 in response to its articles against the GNC and GNC-affilia ed militias. Since then, *al-Wasat's* online site has been subject to cyberattacks,[6] while print copies of *al-Wasat's* newspaper were reportedly seized by soldiers aligned with the self-proclaimed Libyan National Army (LNA)[7], a group led by retired general Khalifa Hafter and

1 Feras Bosalum and Ahmed Elumami, "Libya Parties agree to more talks; two factions call ceasefi e," *Reuters*, January 16, 2015, http://www.reuters.com/article/us-libya-security-idUSKBN0KP0VL20150116.

2 "Libya parliament rejects UN-backed unity government," *Al Jazeera*, January 25, 2016, http://www.aljazeera.com/news/2016/01/libya-parliament-rejects-backed-unity-government-160125160858643.html.

3 Rebecca Murray, "In a Southern Libya Oasis, a Proxy War Engulfs Two Tribes," *Vice News*, June 7, 2015, https://news.vice.com/article/in-a-southern-libya-oasis-a-proxy-war-engulfs-two-tribes.

4 Rebecca Murray, "African Migrants in Libya Face Kidnapping, Torture, and Robbery on Smuggling Route to Europe," *Vice News*, May 8, 2016 https://news.vice.com/article/african-migrants-in-libya-face-kidnapping-torture-and-robbery-on-smuggling-route-to-europe.

5 Sami Zaptia, "GECOL reports theft of 500 telegraph poles by armed militias," *Libya Herald*, April 12, 2016, https://www.libyaherald.com/2016/04/12/gecol-reports-theft-of-500-telegraph-poles-by-armed-militias/.

6 "RSF urges Libya's new Prime Minister to protect media freedom," *RSF*, March 31, 2016, updated May 19, 2016, https://rsf.org/en/news/rsf-urges-libyas-new-prime-minister-protect-media-freedom.

7 "RSF deplores censorship of Libyan weekly Al Wassat," *RSF*, May 12, 2016, https://rsf.org/en/news/rsf-deplores-censorship-libyan-weekly-al-wassat.

linked to the HOR. The overall lack of rule of law has contributed to an environment in which militias routinely violate basic human rights with impunity. Numerous bloggers and activists have been killed since the revolution, while others have been attacked and/or held hostage by militias.[8] Meanwhile, in an unprecedented case, blogger Ali Asbali—who had criticized LNA general Khalifa Hafter in his online posts— was reportedly held in Benghazi's Gernada prison for four months by unidentified men in militia uniforms.[9] The polarized, fraught environment has led many activists and social media users to self-censor.

Historically, access to the internet was limited to the elite. Thousands of cybercafes sprang up after 2000, however, eventually offering cheap internet to both urban and rural users.[10] Over the following decade, the state telecom operator reduced prices, invested in a fibe -optic network backbone, and expanded ADSL, WiMax, and other wireless technologies throughout the country.[11] In its initial stages, there were few instances of online censorship in Libya.[12] However, it was not long until the regime of Muammar Qadhafi began to target opposition news websites, particularly after the lifting of UN sanctions in 2003 led to increased access to surveillance and filtering equipment.[13] Since the overthrow and death of Qadhafi in 2011, the country has witnessed a flury of self-expression, resulting in an increase in news sites and massive growth in Facebook use.[14] However, the 2011 civil war and subsequent fighting has taken a heavy toll on the country's information and communications technology (ICT) sector, damaging infrastructure and sidelining an earlier US$10 billion development plan that had been set to be complete by 2020.[15] Laws that once prohibited criticism of the revolution that brought Qadhafi to power have been changed to outlaw criticism of the 2011 revolution that removed him. In short, significant obstacles to access remain in the country and numerous violations against user rights were witnessed over the coverage period.

Obstacles to Access

Internet access has been badly affected by the ongoing conflict. Electricity outages and physical damage to infrastructure have limited connectivity, as well as the media blackouts imposed by Islamic State militants. Quality of service remains poor and the ICT sector remains monopolized by state-owned entities. Nonetheless, there has been an increase in the number of internet users, particularly among youth.

Availability and Ease of Access

Internet penetration has traditionally been very low in Libya. According to figures from the Interna-

8 Amnesty International Annual Libya report 2015/2016, https://www.amnesty.org/en/countries/middle-east-and-north-africa/libya/report-libya/.

9 "Missing blogger and friends in Benghazi jail," *Libya Herald*, May 4, 2016. https://www.libyaherald.com/2016/05/04/missing-blogger-and-friends-in-benghazi-jail-report/.

10 The Arabic Network for Human Rights Information, "Libya: The Internet in a conflict zone" 2004, http://bit.ly/1GpLE4l.

11 Henry Lancaster, *Libya – Telecoms, Mobile and Broadband*, Budde Comm,July 10, 2015, accessed August 21, 2013, http://bit.ly/1Owy3Lq.

12 Doug Saunders, "Arab social capital is there – it's young and connected," *The Globe and Mail*, March 5, 2011, http://bit.ly/1GdIIro.

13 OpenNet Initiative, "Libya," August 6, 2009, http://opennet.net/research/profiles/liby .

14 Intelligent Positioning. "Libya is World's fastest growing country on Facebook,"November 21, 2011, accessed May 13, 2015, http://bit.ly/1lCyJuP.

15 Lancaster, *Libya – Telecoms, Mobile and Broadband*.

tional Telecommunication Union, internet penetration improved to 19.02 percent at the end of 2015, up from 14 percent fi e years earlier.[16] Some 350 telecommunications towers in 19 different locations provide WiMax and other internet services. WiMax subscribers make up the majority of total subscriptions in the country according to the latest data published by the government, with some 448,135 subscribers compared to 149,963 subscribers for ADSL and 76,885 for LibyaPhone.[17] Broadband was introduced in 2007, although the number of fi ed broadband subscriptions has declined every year since 2010 and now stands are just under 1 subscription per every 100 inhabitants in 2015.[18] Since July 2014, WiMax service has been unstable in many parts of the country, especially in Benghazi and other cities in the east, partly due to the destruction of WiMax towers during fighting [19]

Mobile phone use is ubiquitous, with just under 10 million mobile subscriptions in Libya, representing a penetration rate of 157 percent.[20] Prices dropped precipitously after the introduction of a second mobile provider in 2003, resulting in greater affordability and opening the market to competition, although both operators are still owned by the state-owned Libyan Post Telecommunications and Information Technology Company (LPTIC). By 2013, the price of a prepaid SIM card from the main provider, Libyana, was LYD 5 (US$ 4), compared to LYD 1,200 (US$ 873) in 2003. Smartphones and 3G connectivity have been available since 2006, though the prohibitive cost of compatible handsets impedes their wider dissemination.[21] The service from Almadar, another mobile company, has been unreliable in the eastern part of the country since the 2011 revolution.

Similarly, the cost of a home internet connection remains beyond the reach of a large proportion of Libyans, particularly those living outside major urban areas. A dial-up internet subscription cost LYD 10 (US$ 7) per month, an ADSL subscription was LYD 30 (US$ 22) for a 20 GB data plan,[22] and WiMax service was LYD 30 (US$ 22) for a 15 GB data plan, after initial connection fees.[23] By comparison, Libya's gross domestic product (GDP) per capita, when calculated on a per month basis, was only US$ 387 in 2015.[24] The price of one of the high-end WiMax receiver devices decreased in 2014 from 220 (US$ 160) LYD to 190 LYD (US$ 138)[25] and a lower-end USB receiver device costs 90 LYD (US$ 66). WiMax modems are in short supply, resulting in high prices for second-hand devices sold on the site Open Souk, Libya's online marketplace.[26]

Many foreign and Libyan organizations and individuals in need of reliable internet service have been driven towards two-way satellite internet technology. As two-way technology has become more popular, connection fees and equipment costs have lowered. Prices were recently at US$ 525 for the

16 International Telecommunication Union, "Percentage of Individuals Using the Internet," 2000-2015, http://bit.ly/1cblxxY.
17 Data about internet users in Libya on: LPTIC, Facebook page, accessed May 10, 2015, http://on.fb.me/1LnX6MM.
18 International Telecommunications Union, "Fixed (wired-) broadband subscriptions," 2015, http://bit.ly/1cblxxY.
19 "The disruptions of the Internet services in Libya," [in Arabic] *Alwasat News,* accessed May 13, 2015, http://bit.ly/1PGIJGq.
20 International Telecommunications Union, "Mobile-cellular subscriptions," 2011, http://bit.ly/1cblxxY.
21 "Libyana Introduces 3G Services for First Time in Libya," *The Tripoli Post*, September 26, 2006, http://bit.ly/1GHB7ME.
22 Libya Telecom & Technology, "Libya A.D.S.L: Packages & Price," accessed October 5, 2016, http://www.ltt.ly/en/personal/adsl/index.php?c=63.
23 Libya Telecom & Technology, "Libya Max: Libya Max 400," accessed October 5, 2016, http://www.ltt.ly/en/personal/wimax/index.php?c=55.
24 The World Bank, "GDP per capita (current US$)," accessed October 4, 2016, http://data.worldbank.org/indicator/NY.GDP.PCAP.CD.
25 Libya Telecom & Technology, "Reduction in MyFi Prices", accessed October 5, 2016, http://www.ltt.ly/news/d.php?i=239.
26 See Open Sooq, http://ly.opensooq.com/; or Opensooq, Facebook Company Page, http://on.fb.me/1PtWjgm.

hardware, while a monthly subscription costs US$ 121 for a fast connection, depending on the number of users.[27]

Most people access the internet from computers in their homes and workplaces, with mobile phones being the next most common point of access. The cybercafe industry was decimated in many parts of Libya; instead, cafes and restaurants partner with local internet businesses to offer Wi-Fi hotspots with different data plans. The adult literacy rate was last recorded at 91 percent and a wide range of websites and computer software is available in Arabic.[28] However, limited computer literacy, particularly among women, has been an obstacle to universal access.

The Libyan civil war significantly disrup ed the country's telecommunications sector. There have been few improvements to ICT equipment since the Qadhafi era, p ompting frustrated Libyans to create the Facebook page titled, "I hate Libyan Telecom and Technology," which has attracted over 24,000 followers.[29] Upgrades have been proposed in an effort to respond to demands for increased capacity, such as the laying of the European Indian Gateway and Silphium submarine cables[30] (construction appeared to have begun on the Silphium cable by mid-2016),[31] the construction of additional WiMax towers,[32] the creation of Wi-Fi hotspots, the installation of a long distance fibe -optic cable within the country,[33] and the development of next-generation broadband.[34] Although there have been many announcements of partnerships between Libyan telecommunication companies and foreign companies, such as Alcatel Lucent[35] and Samsung,[36] the status of these contracts are unknown, reflecting the lack f transparency in the Libyan ICT sector.

According to Akamai, Libya has the world's lowest average connection speed at 0.7 Mbps.[37] ICT experts say this is due to poor infrastructure, a lack of quality of service (QoS), technology constraints, and a continued lack of regulations. Furthermore, broadband is not widely available, bandwidth limitations exist for fi ed-line connections, wireless users face slower speeds due to heavy congestion during peak hours, and there is a general lack of resources and personnel to perform maintenance and repairs.

Restrictions on Connectivity

Libya witnessed repeated shutdowns to internet service due to vandalism, technical disruptions, and efforts to cut the flow f information. The Islamic State (IS), which built a stronghold in the

27 See Giga, http://www.giga.ly/; or Giga, Facebook page, https://www.facebook.com/Giga.ltd or https://www.facebook.com/Giga.ltd/photos/a.411508128898799.86518.407758202607125/1123252627724342/?type=3&theater

28 "The World Factbook," https://www.cia.gov/library/publications/the-world-factbook/fields/2103.htm .

29 See I hate Libya Telecom and Technology (LTT), Facebook Business Page, https://www.facebook.com/ihateltt.

30 "The Activation of The New Upgraded Submarine Cable System between Libya and Italy," *The Tripoli Post*, December 25, 2011, http://bit.ly/1jACXK6.

31 LPTIC Facebook Post, July 16, 2016, https://www.facebook.com/LPTIC/photos/a.612688788829160.1073741828.612651818832857/980954825335886/?type=3&theater.

32 "ZTE suggest Libya will boast nationwide WiMax network by Aug-13," *TeleGeography*, January 24, 2013, http://bit.ly/1G6o1hd.

33 "Italian Company to Install Fiber-Optic Network," *Libya Business News*, September 29, 2012, http://bit.ly/RbnhMm.

34 Tom Westcott, "Improving Libya's Internet Access," *Business Eye*, *Libya Herald,* February 2013, 18, http://bit.ly/1LOQhHm.

35 Callum Paton, "Alcatel Lucent to install high-speed internet link between Benghazi and Tripoli," *Libya Herald*, January 28, 2014, http://bit.ly/1MBHnMc.

36 Jamel Adel, "Internet services to get a boost with Al-Madar/Samsung agreement," *Libya Herald*, April, 16, 2015, http://bit.ly/1LbiB3o.

37 Akamai, "State of the Internet: Q1 2016," https://www.akamai.com/uk/en/multimedia/documents/state-of-the-internet/akamai-state-of-the-internet-report-q1-2016.pdf.

coastal town of Sirte, has targeted communications infrastructure for destruction. In August 2015, IS reportedly damaged a cable in Sirte that effectively cut off internet, landline, and some mobile phone communications linking eastern and western Libya[38], but LPTIC said traffic was erouted within a few days.[39] IS also disabled all phone networks in Sirte, banned satellite dishes, and regularly confisca ed personal cell phones to check their contents.[40] Power and telecommunication services remain unstable across Libya, with increasingly frequent cuts[41] due to increasing demand, infrastructure damage, and even blackmail by militias seeking to extract concessions from different administrations, such as the case of a militia cutting off electricity to secure the release of one of its leaders.[42] Illustrating this dangerous environment, employees of GECOL, the national electricity utility, repaired war-damaged cables in an active war zone and under sniper fi e.[43] In early March 2016, the LTT announced that widespread disruption to internet connectivity in the west of Libya had been caused by a damaged undersea cable.[44]

ICT Market

The state-run Libyan Post Telecommunications and Information Technology Company (LIPTC), formerly the General Post and Telecommunications Company (GPTC), is the main telecommunications operator and is fully owned by the government. In 1999, the GPTC awarded the fi st internet service provider (ISP) license to Libya Telecom and Technology (LTT), a subsidiary of the state-owned fi m.[45] Since the fall of the regime, 25 ISPs and 23 VSAT operators have been licensed to compete with state-owned ISPs. Many are based in Tripoli and have strong ownership ties to the government.[46] LIPTC owns two mobile phone providers, Almadar and Libyana, while a third provider, Libya Phone, is owned by LTT.

There has been a noticeable increase in the number of companies and agencies working to provide alternative methods to connect to the internet, such as through satellites (VSAT).[47] On the other hand, there have been few developments within the mobile market. Although there were plans to put Almadar on the stock exchange and to issue the country's fi st tender for a private mobile license, the country has yet to witness any significant liberalization in the sec or.[48]

38 "IS stops phone communications between west, east and south Libya: report," *Libya Herald*, August 26, 2015, https://www.libyaherald.com/2015/08/26/is-stops-phone-communications-between-west-east-and-south-libya-report/.

39 LPTIC Facebook statement, August 29, 2015. https://www.facebook.com/LPTIC/posts/805337812897589

40 "'We feel we are cursed': Life under ISIS in Sirte, Libya," Human Rights Watch, May 18, 2016, https://www.hrw.org/report/2016/05/18/we-feel-we-are-cursed/life-under-isis-sirte-libya.

41 Sami Zaptia, "Electricity sector failing to meet demand despite huge investments over years," *Libya Herald*, April 25, 2016, https://www.libyaherald.com/2016/04/25/electricity-sector-failing-to-meet-demand-despite-huge-investments-over-years/.

42 Saber Ayyub, "Khoms military leader released after electricity to Tripoli cut," *Libya Herald*, March 14, 2016, https://www.libyaherald.com/2016/03/14/khoms-military-leader-released-after-electricity-to-tripoli-cut/.

43 Adam Ali, "Benghazi GECOL engineers work on under risk of sniper fi e," *Libya Herald*, July 17, 2015, https://www.libyaherald.com/2015/07/17/benghazi-gecol-engineers-work-under-sniper-fi e/.

44 Saber Ayyub, "Damaged internet sea cable fi ed by tomorrow says LTT," *Libya Herald*, March 6, 2016, https://www.libyaherald.com/2016/03/06/damaged-internet-sea-cable-fi ed-by-tomorrow-says-ltt/.

45 United Nations Economic Commission for Africa, "The Status of Information for Development Activities in North Africa," (paper presented at the twentieth meeting of the Intergovernmental committee of experts, Tangier, Morocco, April 13-15, 2005) http://bit.ly/1X4OiAG; OpenNet Initiative, "Internet Filtering in Libya - 2006/2007," http://bit.ly/1LbkQDM; "Telecoms in Libya, "[in Arabic] Marefa, accessed August 30, 2012, http://bit.ly/1jAL3Cu.

46 Lancaster.

47 Satellite Providers, "Internet Providers in Libya," accessed July 12, 2015, http://www.satproviders.com/en/list-of-all-services/LIBYA.

48 Reuters, "Mobile operators Libyana to be fl ated," *Libya Business News*, September 18, 2013, http://bit.ly/1VT5nuV.

Regulatory Bodies

Libya's regulatory environment remains very unclear given ongoing disputes over the country's political governance. During the Qadhafi era, decisions on licensing ere made by the government-controlled GPTC (now Libyan Post Telecommunications and Information Technology Company, LPTIC).[49] After the revolution, the transitional government established the Ministry of Communications and Informatics to oversee the country's telecommunications sector. The ministry runs the sector through two main bodies: LPTIC and the General Authority of Telecommunications and Informatics (GATI), formerly the General Telecom Authority (GTA). GATI is responsible for policymaking and regulations, while LPTIC is a holding company for all telecommunications service providers in the country. Libya's top-level domain, ".ly," falls under the responsibility of LTT. Registrations are handled by Register.ly[50] on behalf of NIC.ly.[51]

In 2014, the Ministry of Communications and Informatics appointed a committee to draft a new Telecommunication Act to set standards for the sector and replace the existing regulations surrounding ICTs. The act will also aim to create an independent Telecommunication Regulatory Authority (TRA) to oversee the industry.[52]

Limits on Content

Limits on content are rare in Libya. The lifting of restrictions in 2011 resulted in a diverse online media landscape and an improved market for online advertising. Facebook, in particular, has become an important news source for many Libyans; many government bodies post official statements directly to the social network. Nonetheless, the quality of the content published on these platforms remains poor and highly polarized. Decades of oppressive rule and the continued threat posed by militias has contributed to some degree of self-censorship among users, particularly on sensitive subjects.

Blocking and Filtering

After several years of openness, the fi st instance of politically motivated blocking since the Qadhafi era was seen in early 2015 with the blocking f *Alwasat*.[53] The news site, which published views against the GNC and its military wing, Libya Dawn, was blocked on February 10, 2015 by the LTT, apparently due to a legal order from a court in Tripoli. An announcement revealing the blocking order was not made until April 2015, when LPTIC posted a statement to its Facebook page saying that their website had been hacked by a group of "outlaws" that issued the decision to block *Alwasat* incorrectly and in violation of freedom of expression.[54] Human rights activists and social media users protested the decision using the hashtag "#No2FajrCensorship" on the occasion of World Press Freedom Day on May 3, 2015. Although the official blockage f *Alwasat* appears to have ended, cyberat-

49 Ministry of Justice, "the establishment of the GPTC," [in Arabic] accessed July, 9, 2015, http://bit.ly/1OSyXk3.

50 Register.ly, http://register.ly.

51 NIC, http://nic.ly/ar/index.php.

52 The Ministry of Communication and Informatics, *Libyan National Frequency Plan,* accessed July, 10, 2015, http://bit.ly/1Llbcwk.

53 See "Organizations and media figu es and human rights condemns blocking" [in Arabic] *Alwasat News*, April 8, 2015, accessed May 11, 2015, http://bit.ly/1G6sEbk.

54 See Explanation about blocking "Alwasat News" on LPTIC, Facebook Post, February 25, 2015, http://on.fb.me/1GdNeGm; LPTIC's Statement regarding the blockage of Facebook in Tripoli, LPTIC, Facebook Post, [Arabic] February 22, 2015, https://goo.gl/PWAlG2; In English, https://goo.gl/iFDX1g.

tacks against the website have continued.[55]

YouTube, Facebook, Twitter and international blog-hosting services are freely available. Some pornographic websites have been blocked since the end of the civil war based on a decision made by an ad hoc Temporary Steering Committee formed after the fall of Qadhafi and the liberation f Tripoli.[56] Prior to the war, "indecency" was prohibited by law but sexually explicit sites were never blocked. The LTT has not unblocked the content, perhaps due to the conservative outlook of some political factions vying for influence in the futu e of Libya. A 2006 law mandates that websites registered under the ".ly" domain must not contain content that is "obscene, scandalous, indecent or contrary to Libyan law or Islamic morality."[57]

In February 2014, LTT blocked an additional set of pornographic sites and mistakenly blocked the Wordpress.com domain for a few days. It was unblocked following requests from Libyan bloggers.[58] On April 18, 2015, Facebook was reportedly inaccessible for a few hours in some areas of Tripoli. LPTIC denied responsibility for the interruption, instead releasing a statement reiterating its commitment to free speech and insisting that the interruption had been caused by armed groups taking control of the LTT.[59]

There is little transparency and no legal framework related to the blocking of websites in Libya, as regulations have yet to be formulated. Officiall , all regulations from the Qadhafi era emain valid. When accessing a banned website, users are shown a message from the authorities noting that the site has been blocked.

Content Removal

Authorities do not frequently request private providers or intermediaries to delete content. Rather, there are coordinated efforts to "report" Facebook pages for deletion, particularly for political views against militias. Separately, many Qadhafi-era go ernment webpages containing information on laws and regulations from before the uprising are inaccessible, as is the online archive of the old state-run Libyan newspapers. Some of these websites may have become defunct after the officials running them were ousted or hosting fees were left unpaid, but others were likely taken down deliberately when the revolutionaries came to power.

Media, Diversity, and Content Manipulation

After a sudden opening of the online media landscape after the fall of Qadhafi, negati e trends such as self-censorship, verbal harassment, and a lack of quality reporting now characterize Libya's online sphere. The 2011 revolution brought a notable increase in the number of bloggers writing within Libya, particularly on issues related to political activism, hope for the future, and government criti-

55 "RSF urges Libya's new prime minister to protect media freedom," Reporters Without Borders, March 31, 2016, updated May 19, 2016. https://rsf.org/en/news/rsf-urges-libyas-new-prime-minister-protect-media-freedom.

56 Libya Herald, "LTT blocks pornographic websites," *Libya Business News*, September 13, 2013, http://bit.ly/1k5Iwki

57 OpenNet Initiative, "Internet Filtering in Libya - 2006/2007," http://bit.ly/1LbkQDM ; "Regulations," Libya ccTLD, accessed August 30, 2012, http://nic.ly/regulations.php.

58 Libyan Internet users reporting inaccessibility to their WordPress blogs; Nezar Abudayna, Twitter Post, February 10, 2014, 1:19PM, http://bit.ly/1X4QVT3; Abdulrazig Almansori, Facebook Post [in Arabic], February 10, 2014, https://goo.gl/gOwxdF.

59 See LPTIC's Statement regarding the blockage of Facebook in Tripoli, LPTIC, Facebook Post, [Arabic] February 22, 2015, https://goo.gl/PWAlG2; In English, https://goo.gl/iFDX1g.

cism. However, a sizable number of Libyan bloggers, online journalists, and ordinary citizens continue to practice some degree of self-censorship due to continued instability and increasing threats and violence against journalists over the past years.[60] Social taboos such as mass allegations of sexual abuse by soldiers or conflicts bet een warring tribes and rival cities are off-limits. Online commentators also shy away from expressing religious opinions for fear of being marked as an atheist or a Shiite sympathizer, both of which can be life-threatening. Many commentators avoid criticizing the 2011 revolution, General Haftar, and various heads of local militias mainly out of fear of retribution from armed groups and nonstate actors.

Despite the growth in self-censorship, the online media landscape remains much more diverse than under the previous regime, with few dominant news providers and several privately owned outlets. However, political conflicts and polarization ha e spilled over into the digital sphere. Many of Libya's online outlets have clear political agendas and lack quality journalism and professionalism, instead publishing incitement and propaganda. The low levels of reliability and credibility have made it difficult for many to find neutral and objecti e sources of news about Libya.[61]

The online advertising market has grown slowly and websites related to the Amazigh (whose language was banned under Qadhafi) and other minorities ha e flourished [62] Interestingly, Facebook is often the platform of choice for city and even government officials o publish updates and official communication. The social networking site was third most visited website in the country after Google and YouTube and has become the main source of news about Libya for a large number of users inside and outside the country.[63]

Digital Activism

Over the past years, Libyans have used Facebook and Twitter to mobilize around a variety of causes. Recent campaigns include supporting peace and moves toward a unity government, promoting social justice causes, defending freedom of expression and commemorating individuals murdered for their activism.[64] Since 2014, Libyan activists have promoted democratic values, campaigned against incitement, and dismissed propaganda on Facebook. Most of these campaigns started and spread through hashtags, reflecting the im act of hashtag activism on creating change in Libya. For example, the hashtag #ليبيا_الى_السلام (Libya toward peace) and Facebook page called for an end to the long-running civil war and sparked a national campaign.[65] There was also the campaign #نعم_لتوقيع_المسودة (Yes to signing the draft) which built pressure on political representatives from the two warring governments to sign a UN-backed agreement that would build toward a government of national accord.[66]

60 Reporters Without Borders, "2013 World Press Freedom Index: Dashed Hopes After Spring," accessed in March 2013, http://bit.ly/1bMr3Xz.

61 See Mohamed Eljarh, "The State of Journalism and Media in the New Libya," *Middle East Online*, January 12, 2012, http://bit.ly/1G6txQZ.

62 Tracey Shelton, "Libya's media has its own revolution," *Global Post*, March 18, 2012, http://bit.ly/1OwCwh3.

63 Alexa, "The Top Sites in Libya," accessed October 4, 2016, http://www.alexa.com/topsites/countries/LY.

64 Brave New Libya (blog), "Hashtag activism, from the Digital World to the streets of Libya (Part II)," August 5, 2015. https://bravenewlibya.wordpress.com/tag/ltt/.

65 Brave New Libya (blog), "Hashtag activism, from the Digital World to the streets of Libya (Part II)," August 5, 2015. https://bravenewlibya.wordpress.com/tag/ltt/; see also Facebook page "Libya Toward Peace" http://bit.ly/2duu6JG.

66 Brave New Libya (blog), "Hashtag activism, from the Digital World to the streets of Libya (Part II)," August 5, 2015. https://bravenewlibya.wordpress.com/tag/ltt/.

Violations of User Rights

Amid the ongoing constitutional crisis and weak rule of law, there were flagrant violations of users' rights in the country. Several online journalists have faced threats, detention, kidnappings, and in some cases violent attacks from militias. Armed factions carried out attacks with impunity, while appropriate oversight of the country's surveillance apparatus remained shrouded in doubt.

Legal Environment

Freedom of opinion, communication, and press are guaranteed by Libya's Draft Constitutional Charter, released by the Libyan Transitional National Council in September 2011.[67] However, delays in the drafting of a constitution and the general absence of law enforcement have contributed to weak rule of law in the country.

Several Qadhafi-era laws remain on the books due to the absence of any significant legal reform in the country since the revolution, such as harsh punishments for those who publish content deemed offensive or threatening to Islam, national security, or territorial integrity. A law on collective punishment is particularly egregious, allowing the authorities to punish entire families, towns, or districts for the transgressions of one individual.[68] Because of their vague wording, these laws can be applied to any form of speech, whether transmitted via the internet, mobile phone, or traditional media.

When new laws have been passed, changes have been cosmetic. In February 2014, the GNC amended Article 195 of the penal code to outlaw any criticism of the 2011 "February 17 Revolution" or its officials, as well as members of the GNC,[69] using similar language to that used to outlaw criticism of Qadhafi s "Al-Fateh Revolution."[70] The judiciary has gained in independence since 2012, when, in a landmark decision, the Supreme Court of Libya declared a law that criminalized a variety of political speech unconstitutional.[71] More recently, however, state bodies remain subject to pressure from a variety of armed militias.

Prosecutions and Detentions for Online Activities

In a new occurrence, this year witnessed at least two instances of bloggers detained for criticizing the military or police forces. In March 2016, unidentified men in militia uniforms detained and interrogated blogger Ali Asbali.[72] Asbali had written about the rise in kidnappings and extrajudicial killings in the country and criticized LNA General Khalifa Hafter in his online posts. He was reportedly

67 Libyan Transitional National Council, "Draft Constitutional Charter for the Transitional Stage," September 2011, http://bit.ly/1RIRpvc.

68 IREX, *Media Sustainability Index – Middle East and North Africa 2005*, (Washington D.C.: IREX, 2006), 36, http://bit.ly/1GdOOrH.

69 Reporters Without Borders, "Free expression in new Libya approached with same draconian Gaddafi-era la ," IFEX, February 19, 2014, http://bit.ly/1RbDNYw.

70 Amnesty International, "Three years on, Gaddafi-era laws used o clamp down on free expression," ReliefWeb, February 12, 2014, http://bit.ly/1hF31SQ.

71 Human Rights Watch, "Libya: Law Restricting Speech Ruled Unconstitutional," June 14, 2012, http://bit.ly/1jpemIu.

72 "Asbali: During the 120 days in prison, from the moment of my arrest and until my release, I did not know the reason," *AlWasat News*, August 6, 2016. http://alwasat.ly/ar/mobile/article?articleid=113936.

kept in Benghazi's Gernada prison for 120 days until he was released in July 2016, without any legal charges ever being leveled against him.[73]

On May 2, 2016, Al Senoussi Boujnah was arrested in Benghazi for criticizing the local police Criminal Investigations Unit in a Facebook post. A police official sta ed Boujnah was accused of insulting and defaming the institution. He was released after two days.[74]

Surveillance, Privacy, and Anonymity

Uncertainties remain over the actions of domestic intelligence agencies in the new Libya. LPTIC's involvement in political and security affairs remains vague among many Libyans, though it has made efforts to communicate better through increased press access and frequent press releases on its Facebook page.[75]

A July 2012 report from the *Wall Street Journal* indicated that surveillance tools leftover from the Qadhafi era had been estarted, seemingly in the fight against loyalists f the old regime.[76] Others suspect that these tools were activated to target those with an anti-Islamist agenda. During an interview on al-Hurra TV in March 2012, the Minister of Telecommunications stated that such surveillance had been stopped because the interim government wanted to respect the human rights of Libyans. An organization representing IT professionals in Libya refuted his remarks in an online statement, saying telecom sector employees had confi med that the surveillance system was reactivated.[77] Its status in 2015 was unclear. Given the lack of an independent judiciary or procedures outlining the circumstances under which the state may conduct surveillance, there is little to prevent the government, security agencies, or militias who have access to the equipment from abusing its capabilities.

The Qadhafi egime had direct access to the country's DNS servers and engaged in widespread surveillance of online communications. State of the art equipment from foreign fi ms such as the French company Amesys,[78] and possibly the Chinese fi m ZTE, were sold to the regime, enabling intelligence agencies to intercept communications on a nationwide scale and collect massive amounts of data on both phone and internet usage. Correspondents from the *Wall Street Journal* who visited an internet monitoring center after the regime's collapse reportedly found a storage room lined floo -to-ceiling with dossiers of the online activities of Libyans and foreigners with whom they communicated.[79]

Intimidation and Violence

The breakdown of the rule of law and the growing influence f militias has resulted in a worrying

73 "Missing blogger and friends in Benghazi jail," *Libya Herald*, May 4, 2016. https://www.libyaherald.com/2016/05/04/missing-blogger-and-friends-in-benghazi-jail-report/.

74 "Criminal investigation releases Al Senoussi Boujnah," *Libya24*, May 4, 2016, http://www.libya24.tv/news/35899.

75 "LPTIC confusion and political in fighting, chai man abroad since summer," *Libya Herald*, January 29, 2015, http://bit.ly/1Phs4tM.

76 Margaret Coker and Paul Sonne, "Gadhafi-Era Spy actics Quietly Restarted in Libya," *Wall Street Journal*, July 2, 2012, http://on.wsj.com/1jpeCY2.

77 Libya Telecom & Technology, Facebook post [in Arabic], March 31, 2012, 7:16am, http://on.fb.me/1LN9G5n.

78 Ivan Sigal, "Libya: Foreign Hackers and Surveillance," *Global Voices Advocacy*, October 26, 2011, http://bit.ly/1k5L2qv.

79 Paul Sonne and Margaret Coker, "Firms Aided Libyan Spies," *Wall Street Journal*, August 30, 2011, http://on.wsj.com/1KvvJDg.

uptick in politically motivated threats and violence against journalists and activists.[80] Several incidents—such as the killing of civil society Abdel Basset Abu al-Dhahab in a car bomb in Derna in March 2016,[81] or the kidnapping of the Hamza Ahmed Abdel-Hakim, the rapporteur of the Libyan National Commission for Human Rights, in Tripoli in December 2015[82]—have weakened freedom of expression over the past year, with the results spilling over online.

Tension and conflict has esulted in an overall increase in online hate speech, defamation, harassment, and even death threats. Militias and extremists continue to use Facebook to target and silence activists.[83] For example, in late 2014 anonymous users set up a Facebook page featuring the names, photos, and addresses of Benghazi activists calling for their assassinations and kidnapping. The page was taken down after online activists reported it.[84]

Technical Attacks

Websites are highly vulnerable to cyberattacks in Libya, with prominent news sites such as *Libya Herald* employing protection measures against distributed denial-of-service (DDoS) attacks. Anti-militia Facebook pages were consistently hacked or closed down after mass reporting by users, a significant concern given that most Libyans consider Facebook to be their main source of news.

Libya's political turmoil has spilled over into the digital arena. For example, the official ebsite of the Prime Minister, pm.gov.ly, was taken over by the GNA's Presidency Council from the prime minister of the former Tripoli-based National Salvation Government, even though the latter declared his government was still operational.[85] The takeover of the official ebsite also occurred at a time when the Tobruk-based HOR had not yet voted to accept the authority and legitimacy of the GNA—when a vote was eventually held, the HOR decided *not* to accept the authority of the GNA.

80 Human Rights Watch, "Libya: Investigate Killing Political Activist," July 26, 2013, http://bit.ly/1LP2Kel.

81 "Tributes and anger over 'assassination' of Libyan activist," *Middle East Eye*, March 17, 2016, http://www.middleeasteye.net/news/anger-after-assassination-veteran-libyan-activist-516081195.

82 "Human Rights activist freed by Tripoli militia," *Libya Herald*, July 8, 2016 https://www.libyaherald.com/2016/07/08/human-rights-activist-freed-by-tripoli-militia/.

83 Nadia Burnat, "The attempt to silence Libya's activist generation," *Middle East Eye,* February 13, 2015, accessed on 13 May 2015, http://bit.ly/1GHFuY0.

84 See Radio France Internationale," Mysterious Facebook "hit list" causes uproar in Libya,"Soundcloud, 4:02, http://bit.ly/1MBU2Pt.

85 See "Serraj takes over Ghwell's website while Thinni's goes off the air," *Libya Herald*, April 7, 2016, https://www.libyaherald.com/2016/04/07/serraj-takes-over-ghwells-website-while-thinnis-goes-off-the-air/ ; also see Statement by Government of National Accord posted on pm.gov.ly on April 7, 2016, http://bit.ly/2bwnBIc

Freedom House

Malawi

	2015	2016
Internet Freedom Status	Partly Free	Partly Free
Obstacles to Access (0-25)	15	16
Limits on Content (0-35)	12	10
Violations of User Rights (0-40)	13	15
TOTAL* (0-100)	**40**	**41**

* 0=most free, 100=least free

Population:	**17.2 million**
Internet Penetration 2015 (ITU):	**9 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Partly Free**

Key Developments: June 2015 – May 2016

- Average connection speeds decreased due to poor infrastructure management and lack of investment (see **Availability and Ease of Access**).
- Three opposition parliamentary members were arrested for treason in February 2016 for a private WhatsApp group conversation that authorities said evidenced a coup plot (see **Prosecutions and Arrests for Online Activities**).
- In December 2015, a mobile provider obtained a court injunction against the rollout of the government's so-called "spy machine" monitoring system over surveillance and privacy concerns (see **Surveillance, Privacy, and Anonymity**).

Introduction

Internet freedom in Malawi suffered from declining quality of access and problematic arrests of opposition members for messages exchanged on WhatsApp.

In the past year, Malawi's President Arthur Peter Mutharika began showing autocratic tendencies similar to his elder brother and former President Bingu wa Mutharika, whose repressive tenure ended when he died in 2012. Previous governments focused on traditional media and civil society, but in a shift, the governing Democratic Progressive Party (DPP) under the younger Mutharika has specifically targeted online activities, indicating that the authorities perceive the potential of digital media to empower journalists and citizens as a threat.

Parliament passed the controversial Electronic Transactions Bill (E-Bill) in July 2016, after this report's coverage period. If signed into law by the president, it will allow for restrictions on online communications to "protect public order and national security," and "facilitate technical restriction to conditional access to online communication," an unclear provision that could be interpreted as enabling blocks on social media or communications platforms. Further, "offensive communication" via ICTs that disturbs the privacy rights of any person is penalized with a fine and 12-month prison sen ence, and could be used by public officials o punish their online critics.

In February 2016, the authorities arrested three opposition members of parliament based on a private WhatsApp group chat in which they allegedly schemed to unseat the president. The circumstances in which the conversation came to the government's attention remain unclear. Some analysts believe the content was leaked to the authorities; some feared the messages were altered or fabricated. The MPs were released on bail, but charges of treason were pending in October 2016.

Meanwhile, access remained one of primary obstacles to internet freedom in Malawi, as unprecedented inflation and cur ency depreciation fueled economic instability, negatively impacting the ICT sector and citizens' ability to afford basic goods, including mobile services. In a positive development, the launch of the government's so-called "spy machine," which was widely criticized for its potential to allow government access to user data without judicial oversight, was halted after a telecom provider obtained a court injunction against the monitoring system. No websites were blocked in the country, and users have increasingly turned to online platforms to express critical viewpoints.

Obstacles to Access

Economic turmoil and high taxes make access to ICTS prohibitively expensive for the majority of Malawians, resulting in low access rates across the country. Average connection speeds decreased from the previous year, due to poor infrastructure management and lack of investment.

Availability and Ease of Access

Malawi, a densely populated country that suffers from widespread poverty, has one of the lowest rates of internet access in the world. According to the International Telecommunication Union (ITU),

internet penetration stood at 9 percent in 2015, up from 6 percent in in 2014.[1] Fixed broadband subscriptions are extremely rare.[2] Mobile phone penetration is also low at 35 percent,[3] compared to an average of 76.2 percent across the continent.[4] A survey of 12,000 citizens between November 2014 and January 2015 published by Malawi's National Statistics Office in anuary 2016 reported more positive data, with 85 percent of households surveyed owning a mobile device, and 30 percent of households using one to access the internet.[5]

Meanwhile, connection speeds for Malawian users are frustratingly slow, decreasing to an average of 1.7 Mbps from 1.9 Mbps a year prior, compared to a global average of 6.3 Mbps, according to Akamai's "State of the Internet" report.[6]

Slowing speeds have coincided with rising costs, likely due to poor infrastructure management and lack of investment. Malawi's flagging economy in the ast year has reinforced its status as a least developed country, with soaring inflation having a negati e impact on the ICT sector. Low rates of internet and mobile phone access in Malawi are largely a result of the high cost of service for consumers, including 17.5 percent value-added tax (VAT) on mobile phones and services, and 16.5 percent VAT on internet services.[7] In May 2015, the Malawian parliament implemented an additional 10 percent excise duty on mobile phone text messages and internet data transfers.[8] The increased tariffs could reduce uptake of important digital services like mobile banking and money services.[9]

Consequently, access to the internet is extremely expensive for average Malawians. According to 2015 research by the Alliance for an Affordable Internet, 500MB of mobile data costs over 24 percent of the country's GNI per capita, which is well above the target of 5 percent or less set by the UN Broadband Commission in 2011 as a goal for broadband affordability.[10] The price of data packages also vary considerably by provider. As of mid-2016, a monthly data bundle for 20GB cost US$29 with Airtel, but US$43 with TNM.

A low literacy rate of 64 percent also hinders access to ICTs, and there is a significant digital divide along gender lines. Unreliable electricity and the high cost of generator power strain ICT use. Less than 10 percent of the country has access to electricity, giving Malawi one of the lowest electrific - tion rates in the world, according to the World Bank.[11] The electricity grid is concentrated in urban centers, but only 25 percent of urban households have access, compared to a mere 1 percent of rural households. Half of Malawi's private sector enterprises rely on backup generators. The high cost

1 International Telecommunication Union (ITU), "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1FDwW9w.

2 ITU, "Fixed (Wired) -broadband Subscriptions, 2000-2015," http://bit.ly/1FDwW9w.

3 ITU, "Mobile-cellular Telephone Subscriptions, 2000-2015," http://bit.ly/1FDwW9w.

4 ITU, "Key 2005-2016 ICT data," http://bit.ly/1cblxxY.

5 Suzgo Khunga, "High costs prohibit cellphone usage—survey," MWNation, January 26, 2016, http://mwnation.com/high-costs-prohibit-cellphone-usage-survey/

6 Akamai, "State of the Internet, Q1 2016 Report," https://goo.gl/TQH7L7; Akamai, "Average Connection Speed," map visualization, *The State of the Internet*, Q1 2016, accessed August 1, 2016, http://akamai.me/1LiS6KD.

7 Frontier Economics, *Taxation and the Growth of Mobile Services in Sub-Saharan Africa,* GSMA, 2008, http://bit.ly/1Pk9rVc; Gregory Gondwe, "Internet VAT bites consumers," Biztech Africa, July 24, 2013, http://bit.ly/1Zim7Ai.

8 WangaGwede, "Malawi hikes tax on internet, duty on SMS: Goodall says local resources to finance 2015/16 budget " *Nya*sa Times, May 23, 2015, http://bit.ly/1Mh08jG.

9 "J-Lu takes a swipe at Malawi's SMS and internet tax, labels it 'Retrogressive and anti-democratic,'" Malawian Watchdog, May 25, 2015, http://bit.ly/1OoNIe5.

10 "The Affordability Report 2015-16," Alliance for Affordable Internet, http://a4ai.org/affordability-report/report/2015/#

11 Latest available data is from 2012. World Bank, "Access to electricity (% of population)," accessed October 1, 2016, http://bit.ly/1zN9Eaf.

of infrastructure development in rural areas makes companies unwilling to invest in the country's remote regions.

Restrictions on Connectivity

Due to Malawi's landlocked location, it is connected to the international fiber net ork in Mozambique, Zambia, South Africa, and Tanzania through the SEACOM and EASSy networks. In January 2016, Tanzanian operator SimbaNET finished its construction f a third network, which established a connection between the capital, Lilongwe, and Tanzania.[12] Minister of Information, Communications, Technology and Civic Education Patricia Kaliati launched SimbaNet's connection in May 2016, touting the network's promise to decrease internet prices by 75 percent.[13]

The government of Malawi does not have centralized control over the international gateway, which the ITU characterizes as competitive.[14] Malawi has a total of six fiber ga eways to the SEACOM and EASSy cable landings, three each through MTL and the Electricity Supply Corporation of Malawi Limited (ESCOM). The state-owned Malawi Sustainable Development Network Programme (SDNP), a licensed ISP, oversees the local traffic hub that connects the count y's internet service providers (ISPs), but does not have the capacity to block content or restrict connectivity.[15]

The country's ICT backbone is entirely national in nature, with no regional integration yet in place. The scarcity of regional internet exchange points forces telecoms to rely on upstream service providers that are usually based outside in Europe or North America. As a result, data that should be exchanged locally within Malawi or regionally must pass outside Africa in an unnecessary and expensive use of upstream bandwidth.

ICT Market

Malawi's ICT market is reasonably competitive with 50 licensed ISPs, the majority of which are privately owned with the exception of the Malawi Sustainable Development Network Programme (SDNP).[16] One ISP, MTL, also serves as the country's telecommunication backbone, leasing its infrastructure to most ISPs and mobile phone service providers in the country.[17] Previously a government-owned entity, MTL was privatized in 2005; at present, the government retains 20 percent of MTL shares while Telecomm Holdings Limited holds the other 80 percent.

Mobile phone services are offered by four providers—Airtel Malawi, Telecom Networks Malawi, MTL, and Access Communications.[18] The licensing of the mobile phone company La-Cell in October 2015 helped increase Malawi's market competition in the mobile sector.[19]

12 "Cable Compendium: a guide to the week's submarine and terrestrial developments," TeleGeography, January 15, 2016, http://bit.ly/2efQzwe

13 Linda Tembo, "Optic fiber cable o improve ICT in Malawi," Zodiak Online, May 9, 2016, http://bit.ly/2fhzcbp

14 ITU, "Malawi Profile (La est data available: 2013)," ICT EYE, accessed May 1, 2016, http://bit.ly/1Pk9X5I.

15 Author interview with IT engineer for a local mobile phone company on March 25, 2015.

16 Henry Lancaster, *Malawi - Telecoms, Mobile and Broadband - Market Insights and Statistics, Executive Summary,* BuddeComm, last updated October 25, 2016, http://bit.ly/1OoOUOx.

17 "Fibre optic backbone yielding fruits – MTL," Mkali Journalist (blog), June 11, 2013, http://bit.ly/1jeMOpm.

18 Henry Lancaster, *Malawi - Telecoms, Mobile and Broadband - Market Insights and Statistics, Executive Summary.*

19 Ida Kazembe, "Govt licenses new mobile service provider – Lacell Public Tele Communication Company," Malawi News Agency, via All Africa, October 5, 2015, http://allafrica.com/stories/201510071727.html

Regulatory Bodies

The Malawi Communications Regulatory Authority (MACRA) is the country's sole communications regulator, established under the 2008 Communication Act to ensure reliable and affordable ICT service provision throughout Malawi. Its mandate is to regulate the entire communications sector and issue operating licenses for mobile and fi ed-line phone service providers, ISPs, and cybercafés.

Political connections are often necessary to obtain such licenses. Moreover, the institutional structure of MACRA is subject to political interference, with its board comprised of a chairman and six other members appointed by the president, and two ex-officio membe s—the secretary to the Office f the President and Cabinet and the Information Ministry secretary.[20] The director general of MACRA, whose appointment is also overseen by the president, heads the authority's management and supports the board of directors in the execution of its mandate.

Limits on Content

There were few restrictions placed on online content during the coverage period. Anecdotal reports of critical online posts "disappearing" suggests that informal content removals demanded by government officials is common.

Blocking and Filtering

The current government of Malawi does not block or fil er internet content aside from child pornography. Social media platforms are freely available in Malawi. Former presidential regimes have censored internet content in the past.[21]

Content Removal

Online content critical of the government frequently disappeared without explanation during the period under review. Observers have reported anonymously that the government forces editors of online news websites to take down content deemed objectionable, though the practice is underreported and the extent of content affected is not known. In 2015, an article on *Nyasa Times* that accused President Peter Mutharika's Special Aide Ben Phiri of corruption and bribery disappeared from the news website within 30 minutes of publication. Observers believed the apparent takedown was in keeping with the media's common practice of yielding to government pressure exerted behind the scenes.

Media, Diversity, and Content Manipulation

Malawi's online media landscape does not reflect a wide di ersity of viewpoints, primarily due to the low level of internet use. Economic conditions make it difficult for jou nalists and media groups to launch online outlets. The high cost of using the .mw domain—currently administered by the Malawi

20 International Research & Exchanges Board (IREX), "Malawi," *Media Sustainability Index 2012*, http://bit.ly/1Gz5PHM.

21 During violent anti-government protests in July 2011, MACRA reportedly ordered ISPs to block certain news websites and social media networks, including Facebook and Twitter, in a supposed effort to quell the spread of violence. See, Michael Malakata, "Malawi blocks social media networks to quell protests," *Computer World*, July 22, 2011, http://bit.ly/1L9Bn93.

SNDP on behalf of the Malawian government—is also an obstacle to publishing locally-produced content. According to an official at the SDN , the cost of using the .mw domain is US$100 per month for two months after registration and US$50 per month thereafter.

Furthermore, online advertising is low due to a limited understanding of the internet among businesses, which are hesitant to advertise with independent media outlets. As a result, even Malawi's oldest media house, the Times Media Group, laid off numerous staff from its online division in early 2016 due to flagging p ofits [22]

Nevertheless, the growing blogosphere is regarded as an important aspect of journalism in Malawi, with Malawian journalists frequently winning the Media Institute of Southern Africa's annual blogging award. Media publishers such as Blantyre Newspapers Limited often host bloggers on their websites to enhance their image as independent news sources.

Internet users and commentators practice a degree of self-censorship but are generally more open to discussing topics of controversial nature. In contrast, online journalists usually exhibit caution when handling news associated with ethnic, racial, or religious minorities.

There was little to no government or partisan manipulation of online content evident during the coverage period. Since the current government was elected in May 2014, progovernment trolls have reduced their activity. In the past, government-aligned commentators infiltra ed social media and online news websites to undermine critical commentary.

Digital Activism

The most influential ICT ool in Malawi remains the mobile phone. Text messages are used to organize demonstrations, garner political support, and conduct opinion polls. Significant social media commentary and activism followed the government's May 2015 announcement that internet and text messaging services would be subject to a 10 percent excise duty (see Availability and Ease of Access). The campaign had not elicited a response in mid-2016.[23]

Violations of User Rights

The controversial Electronic Transactions Bill (E-Bill) was passed in July 2016 and awaited the president's assent as of October 2016, despite criticism of the bill's potential to limit internet freedom. Three opposition parliament members were arrested and charged with treason in February 2016 based on a private WhatsApp group chat that was interpreted as a plot to stage a coup against the ruling party.

Legal Environment

Malawi has strong constitutional guarantees for freedom of the press and expression, though there are several laws that restrict these freedoms in practice. The 1967 Protected Flag, Emblems and Names Act and the 1947 Printed Publications Act both restrict the media from reporting on the

22 "Media release 26th February 2016, Blantyre TIMES GROUP BUSINESS RE-ENGINEERING," The Times Group, February 26, 2016, http://www.times.mw/media-release-26th-february-2016-blantyre-times-group-business-re-engineering/

23 Thom Khanje, "Consumers scorn SMS/internet tax," The Times Group, May 25, 2015,http://bit.ly/1L2z365.

president, among other limitations.[24] Libel is punishable with up to two years imprisonment if prosecuted as a criminal charge, though most libel cases are processed as civil offences or settled out of court. Malawi's judiciary is generally regarded as independent.

In an effort to provide a regulatory framework for ICTs and address cybercrime, parliament passed the controversial Electronic Transactions Bill (E-Bill) in July 2016, after this report's coverage period. It awaited the president's assent in late 2016.[25] First drafted in October 2013, the E-Bill stalled before being reintroduced in November 2015. Critics have highlighted its potential to limit internet freedom for years.

Article 28 allows for restrictions on online communications to "protect public order and national security," a broad provision open for abuse.[26] The same article would also "facilitate technical restriction to conditional access to online communication," an unclear clause that could be interpreted to enable blocks on social media or communications platforms.[27] Article 90 penalizes "offensive communication" via ICTs that disturbs the privacy rights of any person with fines or a maximum 12-month prison sentence—a provision that public officials could exploit o punish critical speech by online journalists or internet users.[28]

Prosecutions and Detentions for Online Activities

Members of the political opposition were arrested for online activities during the coverage period, marking a disconcerting development. Malawian netizens have not generally faced legal sanctions for communicating online before, though online journalists were periodically arrested in relation to their work in previous years.

In February 2016, the authorities arrested three opposition members of parliament (MP) for the content of a closed WhatsApp group chat that they said was evidence of a plot to stage a coup.[29] Human rights observers condemned the arrests as politically motivated. Reports said the arrests came after the ruling party received a tip about the WhatsApp conversation. Some analysts believe the private messages were leaked to the authorities, and some speculated that the content of the messages had been altered either before or after the arrests occurred. One of the MPs said his mobile phone was impounded during his detention and was missing data when it was returned, including call history, texts, contacts, and WhatsApp.[30] The MPs were released on bail, but charges of treason were pending in October 2016.[31]

24 Freedom House, "Malawi," *Freedom of the Press 2015*, https://freedomhouse.org/report/freedom-press/2015/malawi.

25 Jacqueline Nhlema, "Malawi Parliament passes E-Bill," Zodiak Online, July 6, 2016, http://bit.ly/2fUnt62

26 Media Institute of Southern Africa (MISA), "Southern Africa: Malawi Parliament Rejects Bill to Gag Online Media," press release, November 29, 2015, http://allafrica.com/stories/201511303064.html

27 Part IV, Article 28, Electronic Transactions Bill 2015, gazetted May 15, 2015, www.parliament.gov.mw/docs/bills/BILL11_2015.pdf

28 Part X, Article 90, Electronic Transactions Bill 2015, gazetted May 15, 2015.

29 Lameck Masina, "Malawi government faulted over arrests of coup suspects," Voice of America, February 26, 2016, http://www.voanews.com/a/malawi-government-faulted-over-arrests-of-coup-suspects/3209056.html

30 Alfred Chauwa, "Police extract Msungama's mobile phone data: 'Malawi WhatsApp coup plot,'" Nyasa Times, March 2, 2016, http://bit.ly/2eOWrsF

31 Owen Khamula, "Malawi police say they are 'still investigating' WhatsApp coup plot," Nyasa Times, June 17, 2016, http://www.nyasatimes.com/malawi-police-still-investigating-kabwila-chakwantha-treason-case/; Luke Bisani, "Malawi police angers WhatsApp treason suspects," Malawi 24, October 4, 2016, http://bit.ly/2fLZCX6

Surveillance, Privacy, and Anonymity

Government surveillance of ICT activities is suspected in Malawi, in large part due to the regulatory authority's efforts to implement technology known as the Consolidated ICT Regulatory Management System (CIRMS), known locally as the "spy machine." MACRA described the system, purchased from the U.S.-based company Agilis International for US$6.8 million in 2011, as a tool for to monitor the performance of mobile phone companies and improve quality of service. However, news reports said that the machine would also allow MACRA to obtain data from telephone operators, including the time, duration, and location of calls, SMS messages sent and received, the type of handset used, and other subscriber details, without judicial oversight.[32] After a series of legal challenges, the Supreme Court said the system was in accordance with the Communications Act in September 2014.[33]

In December 2015, one of Malawi's two mobile phone companies, Telekoms Network Malawi (TNM), obtained another injunction to halt the machine's rollout based on concerns over the machine's potential to allow government access to user data.[34] In response to the repeated legal challenges, the regulator began engaging with the South African fi m, Global Voice Group, to implement a different telecom network management system in July 2016.[35] It is unclear whether this new system to replace the "spy machine" will enable unchecked government surveillance.

Potential restrictions on anonymous communication include SIM card registration requirements announced in June 2014, to be implemented by January 2015. As of mid-2016, they had not been enforced.[36]

By law, service providers are required to hand over user information when presented with a court-issued warrant; however, such legal safeguards have failed to prevent abuse in the past, particularly under the late President Bingu wa Mutharika 's regime. In 2012, the former government suspected a group led by then-Vice President Joyce Banda of scheming to overthrow it, and obtained transcripts of the group's mobile phone and SMS communications from service providers. The arrest of three opposition MPs for their WhatsApp messages in February 2016 raised suspicions that the current government may be carrying out similar practices (see Prosecutions and Detentions for Online Activities), though WhatsApp messages are more difficult o intercept than SMS.

Intimidation and Violence

There were no reports of physical assaults, extralegal detentions, or harassment of opposition activists, bloggers, or ordinary internet users in the past year.

Technical Attacks

There were no technical attacks against independent news websites, activists, or ordinary users reported during the period under review.

32 Gregory Gondwe, "'Spy Machine' brings telecoms fears," Biztech Africa, November 14, 2011,http://bit.ly/1Mhgs3V.

33 Tikondane Vega, "MACRA gets Supreme Court nod to use CIRMs 'spy' machine," Mana Online, September 15, 2014, http://bit.ly/1Nr9aAo.

34 Anita Dakamau, "TNM risks losing license over anti-spy machine stand," Malawi Punch, April 20, 2016, http://bit.ly/2fLZgj6

35 "Malawi taxpayer hit over messed up 'spy machine': Macra risk massive pay-out to US fi m Agilis," Nyasa Times, July 2, 2016, http://www.nyasatimes.com/malawi-taxpayer-hit-messed-spy-machine-macra-risk-massive-pay-us-fi m-agilis/

36 WangaGwede, "Malawi to start mandatory SIM card registration," Nyasa Times, January 11, 2014, http://bit.ly/1NrjecG.

Freedom House

Malaysia

	2015	2016
Internet Freedom Status	Partly Free	Partly Free
Obstacles to Access (0-25)	8	9
Limits on Content (0-35)	14	16
Violations of User Rights (0-40)	21	20
TOTAL* (0-100)	**43**	**45**

* 0=most free, 100=least free

Population:	**30.3 million**
Internet Penetration 2015 (ITU):	**71 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- For the fi st time, the government reneged on pledges never to censor the internet and blocked websites that had reported on a billion dollar corruption scandal implicating Prime Minister Najib Razak, including the UK-based *Sarawak Report,* news websites, and the publishing platform Medium (see **Blocking and Filtering**).
- *The Malaysian Insider,* an online news outlet in operation for eight years, went out of business as an indirect result of government blocking (see **Media, Diversity, and Content Manipulation**).
- Politicians, journalists and Facebook users were investigated for online speech, including former Prime Minister Mahathir Mohamad, who criticized the government in a blog post (see **Prosecutions and Detentions for Online Activities**).
- In April 2016, a 19-year-old laborer was arrested for posting comments considered insulting to the crown prince of the southern state of Johor on Facebook; in June, he was sentenced to one year in prison (see **Prosecutions and Detentions for Online Activities**).

Introduction

Internet freedom declined amid corruption allegations, as the government implemented political censorship for the first time and prosecuted critics for online speech.

Internet access continued to improve in 2015 and 2016. The Barisan Nasional coalition government has promoted internet use through policies to develop cheaper community internet access and affordable mobile phones in rural areas. Yet this investment has also fueled popular political mobilization and a challenge to the government's decades-long rule.[1] In response, officials have increasingly used legal measures to control online criticism.

During this coverage period, the government implemented political censorship for the first time, and blocked access to popular websites and blogs, including *Sarawak Report, Malaysia Chronicle,* and *The Malaysian Insider* among others, for publishing "unverified contents" which could "create unrest." Among other reports, the sites had published allegations that money linked to a state investment fund had ended up in Prime Minister Najib Razak's bank accounts.[2] Najib denied receiving money for personal use. Digital media outlets reporting on corruption allegations implicating Najib and other officials faced defamation suits and criminal investigations. These measures heightened economic constraints online internet-based media organizations. *The Malaysian Insider* went out of business in March 2016, in part because of the block.

Police interrogated, arrested, or charged multiple bloggers and Facebook users under the Sedition Act and the Communications and Multimedia Act (CMA) for online comments about sensitive issues in 2015 and 2016. In 2016, the government said it was amending the CMA to address social media "misuse" and "false news." Other officials proposed revisiting an old plan to register bloggers and social media users to ensure they do not "abuse the internet."

Obstacles to Access

Internet access in Malaysia is considered excellent for the region, despite a digital divide between rural and urban areas. Government policies that promote access are reducing this gap. Mobile phone access is increasing, providing internet service for many young and rural users. An open market allows fierce competition among providers, resulting in attractive pricing and high quality service.

Availability and Ease of Access

In October 2015, the government reported more that 20 million internet users in Malaysia, with nearly 17 million active on social media.[3] The International Telecommunication Union reported 71

1 In 1973, the Barisan Nasional, which translates as National Front, absorbed the Alliance Party coalition which had governed Malaysia since 1957.

2 Beh Lih Yi, "Sarawak Report whistleblowing website blocked by Malaysia after PM allegations," *The Guardian*, July 20, 2015, http://bit.ly/1CLd2rU; Tom Wright, "Fund Controversy Threatens Malaysia's Leader," *Wall Street Journal,* June 18, 2015, http://www.wsj.com/articles/fund-controversy-threatens-malaysias-leader-1434681241

3 "Malaysia has over 20.1m internet users," The Sun Daily, October 28, 2015, http://bit.ly/1TffRZa.

percent penetration in 2015, citing the Department of Statistics.[4] The ambitious official pledge in 2012 was to increase it to 80 percent.[5]

Internet penetration is concentrated in developed or urban areas. Government statistics show that the highest internet penetration in 2015 was in the highly developed Klang Valley area, which comprises the capital city Kuala Lumpur (80 percent), the nation's most developed state of Selangor (73 percent), and at the administrative capital Putrajaya (99 percent). Penetration remained low in the less populated states of Sabah (52 percent) and Sarawak (54 percent), situated in East Malaysia where most residents belong to indigenous groups. [6] That distribution remained largely unchanged in 2016.

The most recently available government statistics from 2012 showed a slight gender imbalance in access rates, with men representing 56 percent of both internet and mobile users. The most prolific users were aged 20 to 29 (21 percent).

The introduction of wireless WiMax technology in 2008 helped bring broadband to regions that are difficult o reach via cable; four WiMax providers were in operation as of 2016. Cybercafes also play an important role in providing access outside cities. Free Wi-Fi connections are available in many urban spaces, including malls, restaurants, hotels and tourist destinations.

A 2010 National Broadband Initiative expedited broadband and mobile expansion.[7] Around 250 community centers offering broadband internet were established nationwide and nearly 500,000 netbooks were distributed to students and low income citizens in rural and suburban areas in 2011.[8] In 2012, the "1Malaysia" affordable broadband package offered decent broadband speeds for under MYR 38 (US$12) per month in fi e states with lower penetration rates.[9] By 2013, internet centers were expanding to cities,[10] and the government and local councils had introduced schemes to provide free or inexpensive Wi-Fi nationwide.[11] The average monthly cost of fi ed internet access is MYR 99 (US$30) per month.[12] As of June 2015, there were 562 1Malaysia internet centers nationwide with 471,855 registered users; 120 mini community broadband centers located at Information Departments in underserved areas nationwide; 44 community broadband libraries in rural areas, and 5,860 1Malaysia wireless villages, which bring access to small, remote communities. Internet access was available in a total of 30,959 hotspot locations.[13]

The average internet speed is still comparatively slow, however. The government responded to complaints of slow internet speed in September 2015, saying that Malaysians were choosing not to

4 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1cblxxY.

5 Performance Management and Delivery Unit, *Economic Transformation Programme Annual Report 2012*, 188, http://bit.ly/1Ojrifj.

6 Malaysian Communications and Multimedia Commission, *Communications and Multimedia Pocket Book of Statistics Q2 2015,* http://bit.ly/1QEHrIs

7 Sira Habu and Shaun Ho, "RM1bil initiative to promote high-speed broadband usage," *The Star Online*, March 25, 2010, http://bit.ly/1ANKARp.

8 Roshda Md Yunan, "Rural Broadband Initiatives in Malaysia" Ministry of Information Communication and Culture Malaysia, (The ASEAN Rural Connectivity Conference for Education and Development, Hanoi, Vietnam, September 21-23, 2011), http://bit.ly/1iUMuvf.

9 "1Malaysia Broadband Affordable Packages for 5 States," *Malaysian Wireless*, September 8, 2012, http://bit.ly/17B08xE.

10 *New Straits Times*, "1Malaysia Internet Centre Comes to KL," *World News,* March 26, 2013, http://bit.ly/1NI1vxB.

11 Choong Mek Zhin, "DBKL to make it a requirement for restaurants to provide Wi-Fi services," *The Star Online*, January 9, 2012, http://bit.ly/1AvwYeE.

12 Author's market survey.

13 Malaysian Communications & Multimedia Commission, *Communications and Multimedia Pocket Book of Statistics Q2 2015.*

spend more for fast, more reliable connections, since 71 percent of internet users preferred slower broadband packages offering speeds between 384 Kbps and 1 Mbps.[14] In 2016, the fastest broadband service was offered by Time, which advertised connections as fast as 100 Mbps. Other internet service providers such as TM UniFi offer speeds as high as 20 Mbps. Faster fiber connections a e also offered by Maxis, Celcom, and P1.[15]

Mobile internet access is easily available, affordable, and popular among young people. Mobile penetration surpassed the country's total population in 2011 and was approaching 150 percent in 2015, indicating that some individuals have multiple phone lines.[16] The government has incentivized smartphone adoption, including a MYR200 smartphone rebate for young adults aged 21-30 with a monthly income of MYR 3,000 or less.[17] The boom in social networking sites such as Facebook, Twitter and Instagram, and data messaging applications such as WhatsApp, WeChat, Viber, LINE, and others, have also increased smartphone usage.

In 2013, mobile operators such as Celcom and Maxis introduced 4G LTE wireless broadband service, which is faster than some fiber b oadband services, with download speeds up to 75 Mbps. Older 3G and 3.5G connections offer speeds of up to 384 Kbps and up to 7.2 Mbps, respectively.

Those already connected to the internet are consuming more bandwidth. According to the Malaysian Internet Exchange (MyIX), Malaysia's internet traffic sho ed the biggest annual percentage increase in more than a decade in 2013—a 51 percent jump to 349,277 Mbps from 230,631 Mbps. Usage is expected to continue to rise.[18]

Restrictions on Connectivity

The primary options for broadband internet connectivity in Malaysia are fibe , ADSL, and wireless. Telekom Malaysia, the country's largest – and formerly state-owned – telecommunications company, retains a monopoly over the fi ed-line network. The government continues to hold a 29 percent share in Telekom Malaysia.[19]

Malaysia's internet backbone was operated by TMNet during the coverage period, a responsibility previous shared with Jaring.[20] Formerly owned by the ministry of finance, aring was Malaysia's fi st internet service provider, installing its fi st international satellite leased-circuit at 64 Kbps, connecting Kuala Lumpur to Stockton in the United States. Jaring became a private entity in 2014, but went into liquidation in 2015.[21] TMNet is a subsidiary of the now-privatized Telekom Malaysia, Malaysia's largest internet service provider, and the owner of the nation's last mile connections. Since there is

14 "Most Malaysians choose slower, cheaper Internet, says Salleh Said Keruak," *The Star Online*, Sept 28, 2015, http://bit.ly/1WRyRei.

15 Nick Davison, "What is the Fastest Broadband Internet Service in Malaysia?," *Expat Go Malaysia*, Aug 6, 2014, http://bit.ly/1x3W1VA.

16 Malaysian Communications & Multimedia Commission, *Communications and Multimedia Pocket Book of Statistics Q3 2014;* Malaysian Communications and Multimedia Commission, *Communications and Multimedia Pocket Book of Statistics 2013*, http://bit.ly/1NI2cqt ; ITU, "Mobile cellular Telephone Subscriptions, 2000-2012," http://bit.ly/1cblxxY.

17 "Malaysia's Internet usage rises 51% in 2013, says industry body".

18 "Malaysia's Internet usage rises 51% in 2013, says industry body," *The Malaysian Insider,* April 7, 2014, http://bit.ly/1GxtusV.

19 Summary of shareholding in Telekom Malaysia, http://bit.ly/290zliY

20 "The Internet Backbone and Service Markets in Malaysia," http://studentsrepo.um.edu.my/1937/7/CHAP4.pdf

21 Steven Patrick, "Jaring, the fi st Malaysian ISP, winds up," *The Star Online,* May 4, 2015, http://www.thestar.com.my/Tech/Tech-News/2015/05/04/Jaring-the-fi st-Malaysian-ISP-winds-up/.

no local loop unbundling, TMNet enjoys a virtual monopoly of the broadband market (see "ICT Market").[22]

There were no reported cases of government-imposed restrictions on access to the internet for political reasons during this coverage period. In the past there were reports of mobile phone jammers being used by the authorities during political rallies, though this was denied by the government.[23] In recent years, some local authorities have introduced restrictions on cybercafes to curb illegal online activities, particularly gambling, which can result in closure if detected on cafe premises. Select states have capped the number of cybercafe licenses available, making it difficult for legitima e new venues to open.[24]

In 2015, the government issued 171 licenses to network facilities providers (up from 161 in 2014).[25]

ICT Market

The government issued 159 internet service provider licences in 2015 (up from 158 in 2014).[26] TMNet was the largest ISP during the coverage period. The largest mobile provider, Maxis Communications, was founded by Ananda Krishnan, who also owns Malaysia's biggest satellite broadcaster and enjoys close ties to former Prime Minister Mahathir Mohamad.[27] Two new mobile phone providers, YTL Communications and Umobile, have joined the market since 2008. Though ostensibly unrelated to the government, observers believe they benefit f om political connections.

Fiber connections are the standard for the fastest household internet connectivity. Fiber home broadband connection in Malaysia is provided by Astro IPTV. Other providers of broadband and mobile internet connections include Celcom, DiGi, Maxis, Time Internet, Telekom Malaysia, Tune Talk, U Mobile and Yes, which is a wireless 4G provider.[28]

Regulatory Bodies

Regulation of the internet falls under the purview of the Malaysian Communications and Multimedia Commission (MCMC), which is overseen by the Minister of Information, Communications, and Culture. The 1998 Communication and Multimedia Act (CMA) gives the information minister a range of powers, including licensing the ownership and operation of network facilities. Similar rules serve as a means of controlling the traditional media,[29] though this has not been documented among internet companies.

The CMA provides for the ministry to appoint the MCMC chairman and three government commissioners, plus two to fi e commissioners from nongovernmental entities.[30] The current three are all from the private sector. Since 2008, the process for appointing members of the MCMC advisory

22 Telekom Malaysia website, http://www.123helpme.com/telekom-malaysia-expansion-view.asp?id=159596.
23 Patrick Lee, "Rais: We did not jam networks during Bersih, *"Free Malaysia Today*, June 14, 2012, http://bit.ly/1vBS8HM.
24 Peter Boon, "Cyber cafe licences not issued anymore—Ministry," *Borneo Post Online*, Oct 15, 2012, http://bit.ly/1wj3DiD.
25 Malaysian Communications & Multimedia Commission, *Communications and Multimedia Pocket Book of Statistics Q3 2014.*
26 Malaysian Communications & Multimedia Commission, *Communications and Multimedia Pocket Book of Statistics Q3 2014.*
27 Colin Kruger, "Billionaire eyes Australian media," *The Sydney Morning Herald*, May 28, 2011, http://bit.ly/1DZAsJk.
28 Malaysian internet and mobile providers, http://bit.ly/28QSfcB
29 "Malaysa," in *Freedom of the Press 2016*, https://freedomhouse.org/report/freedom-press/2016/malaysia.
30 Malaysian Communications & Multimedia Commission Act 1998, http://www.agc.gov.my/Akta/Vol.%2012/Act%20589.pdf.

board has become more transparent and participatory, involving consultations with diverse stakeholders and the inclusion of civil society members on the board. Yet the MCMC remains a driving force in efforts to curtail online speech, including investigations into online portals and bloggers.

Limits on Content

Facing a high profile corruption scandal, the government started to block popular news sites and blogs perceived as critical for the first time. The prime minister and one of his ministers have also filed defamation suits against news portals. Some news sites have been excluded from government press conferences, and some downsized or went under, due to financial pressures exacerbated in a worsening media climate.

Blocking and Filtering

A provision of the CMA explicitly states that none of its wording "shall be construed as permitting the censorship of the internet." The Multimedia Super Corridor, an information technology development project, includes a 10-point Bill of Guarantees that promises no censorship to member ICT businesses.[31]

In July 2015, however, the MCMC ordered service providers to block access to the UK-based whistleblower site *Sarawak Report* over articles on the misallocation of resources from the 1Malaysia Development Berhad (1MDB) state investment fund, which the government called detrimental to national security.[32]

Local content providers were subsequently singled out for similar reasons. Two news portals, *Malaysia Chronicle* and *The Malaysian Insider,* were blocked in October 2015 and February 2016 respectively, both for publishing articles about 1MDB deemed to be critical of the government and the prime minister.[33] Officials described the con ent as "obscene, indecent, false, menacing or offensive," and a threat to national security.[34] Two editors with *The Malaysian Insider* were questioned by police in relation to reports (see "Prosecutions and Detentions for Online Activities"); the website closed down in March (see "Media, Diversity, and Content Manipulation"). The government also blocked a handful of prominent blogs which were critical of the government, such as *Syed Outsyed The Box,* a blog whose owner reported having reposted content from *Sarawak Report,* and *Din Turtle*, which publishes socio-political commentary.[35]

The government also blocked access to more international content. The Hong Kong-based commentary site *Asia Sentinel* was blocked in Malaysia on January 21, 2016, for "violating national laws" after it published an article on Prime Minister Najib.[36] The blog-publishing platform Medium was blocked

31 Malaysia National ICT Initiative, "MSC Malaysia 10-Point Bill of Guarantees," accessed August 2013, http://bit.ly/1UZZ6xb; Malaysian Communications and Multimedia Commission, "Communications and Multimedia Act 1998," accessed August 2013, http://bit.ly/1zKzZ7k.

32 Human Rights Watch, "Malaysia: End Website Blocking, Politicized Investigations," July 22, 2015, http://bit.ly/1EoEOFL.

33 "Malaysia Chronicle website blocked in Malaysia," FreeMalaysiaToday, Oct 24, 2015, http://bit.ly/1TKUUVN; "The Malaysian Insider news portal blocked by government," Channel News Asia, Feb 25, 2016, http://bit.ly/1T935LQ.

34 "Salleh Said Keruak: TMI breached Communications Act," The Star Online, Feb 26, 2016, http://bit.ly/1LNKhtD.

35 "Several blogs blocked for alleged violation of the laws," The Mole, Jan 28, 2016, http://bit.ly/1TfgYIo.

36 "Putrajaya blocks access to Asia Sentinel, says portal," FreeMalaysiaToday, Jan 21, 2016, http://bit.ly/1RcLOex.

on January 22, after it refused to take down articles posted by the banned *Sarawak Report*.[37] Both remained inaccessible in mid-2016.

The government has not systematically targeted political content in the past. Until recently, there were no restrictions on websites except for those which violate national laws governing pornography.[38] In 2013, officials said a total 6,640 sites had been blocked since 2008.[39] In October 2014, the government said the Malaysian Communication and Multimedia Commission (MCMC) had shut down or blocked at least another 1,400 websites that were deemed inappropriate.[40] The Commission blocked 1,263 websites in 2015,[41] and another 399 in the first two months of 2016.[42] No list of affected content is available, but site owners can appeal if mistakenly blocked. Many government-linked companies and public universities restrict access to the *Malaysiakini* news website and others perceived as politically sensitive.

Content Removal

The MCMC periodically instructs websites to remove content, including some perceived as critical of the government,[43] although no such instructions were made publicly in the review period. Requests are generally nontransparent and lack judicial oversight or avenues for appeal. Medium was blocked during the coverage period after refusing a government request to remove content (see "Blocking and Filtering").

Some blog owners and Facebook users have been told to remove their contents by the MCMC, especially when the contents touch on sensitive issues involving race, religion and royalty. Religion is particularly sensitive. In 2009, the MCMC directed *Malaysiakini* to take down two videos containing sensitive religious and political content. When *Malaysiakini* Editor-in-Chief Steven Gan refused, the MCMC urged the attorney general to prosecute him, though the case was never pursued.[44]

Media, Diversity, and Content Manipulation

During this review period, the government blocked a number of news portals (see "Blocking and Filtering"). As a result, the eight-year-old outlet *The Malaysian Insider* was forced to shut down, citing commercial reasons, laying off 59 staff.[45] Other news portals downsized during the same period, but as a result of economic challenges rather than censorship. *The Rakyat Post* went offline temporarily

37 "Spurned by Medium, MCMC strikes back, users suffer," Digital News Asia, Jan 27, 2016, http://bit.ly/1TLbYuG; https://medium.com/medium-legal/the-post-stays-up-d222e34cb7e7#.z1yom7jzk.

38 "Internet providers need time to block porn site RedTube, says MCMC", *The Malaysian Insider*, December 22, 2014, http://bit.ly/1LIWqiG.

39 Bernama, "More than 6,000 websites blocked for violations since 2008," *Malay Mail Online*, July 5, 2013, http://bit.ly/181FRRQ.

40 Elizabeth Zachariah, "Malaysia has blocked 1,400 'inappropriate' websites, says Ahmad Shabery," *The Malaysian Insider*, Oct 14, 2014,http://bit.ly/1ANQFNX.

41 'Investigations against authors of online postings worrying,' BeritaDaily, May 27, 2016, http://bit.ly/28Vcjeh.

42 '399 websites blocked by MCMC this year', Hakam website, March 8, 2016, http://bit.ly/28VV7B3.

43 The Malaysians Communications and Multimedia Content Code, http://bit.ly/1DWt2Vm.

44 One showed Muslim demonstrators desecrating the head of a cow—an animal Hindus consider sacred—to protest the relocation of a Hindu temple; the second showed a political speech. See Reporters Without Borders, "Malaysiakini Website Refuses to Bow to Censorship," September 24, 2009, http://bit.ly/1DZHRbB.

45 'Independent Malaysian news site closes amid government clampdown on media', The Guardian, March 15, 2016, http://bit.ly/28VLqbs.

before coming back with a smaller team of staff.[46] At the end of this coverage period, *The Ant Daily* was no longer in operation.

However the influence f online news portals remains robust, with several among the nation's most popular websites.[47] More established news portals such as *Malaysiakini* and *Malay Mail Online* have been joined by relative newcomers such as *FreeMalaysiaToday* and *Berita Daily*. Many other, much smaller news portals continue to contribute to diversity of information online,[48] and online news outlets represent an increasingly serious challenge to traditional media.

In 2013, a judge ordered the home ministry to grant *Malaysiakini* the right to reapply for a print license.[49] The ministry had repeatedly refused to grant the license, and challenged a 2012 appeals court ruling which characterized *Malaysiakini's* right to publish a newspaper as fundamental.[50]

Combative political reporting online may have caused the government or its supporters to try to censor a handful of news websites in the lead-up to 2013 elections. The sites were simultaneously targeted by hackers, and the exact nature of the interference remains unclear.[51] At least two outlets filed a complaint with the MCMC, which ne er responded.

While cyberattacks on news portals have declined, some digital journalists were subjected to informal, inconsistent bans from select government press conferences in the past two years.[52] An uptick in police reports filed against jou nalists contributed to a sense of official harassment [53] In 2014, Prime Minister Najib and his party Umno sued *Malaysiakini* for defamation, followed by three additional news websites in 2015 (see "Prosecutions and Detentions for Online Activities").[54] Following in the prime minister's footsteps, another minister filed a defamation suit against *Malaysiakini* in December 2015, saying he had failed to receive a satisfactory reply over its report he said had misquoted him. Minister Abdul Rahman Dahlan said that his legal action against *Malaysiakini* was "not to curb media freedom but to remind news portals to be more careful and to not compromise on facts."[55]

YouTube, Facebook, Twitter, and international blog-hosting services, as well as other social media platforms, were freely available during the coverage period, with the exception of Medium, which was blocked in January 2016. In 2014, the government briefly conside ed proposals to ban Facebook to curb online abuse. However, the proposal was shot down following complaints from civil society. [56] Expanded internet access has led to the emergence of a vibrant blogosphere. English and Malay

46 'The Rakyat Post closes shop,' The Star Online, Feb 29, 2016, http://bit.ly/299eoAg.

47 Akil Yunus, "The Star Online ranks as top news portal in Malaysia," *The Star Online* , December 22, 2014, http://bit.ly/1J-Ga6gb; "Top Sites in Malaysia," Alexa Web Information Company, accessed January 29, 2013, http://bit.ly/1JQCKOt.

48 List of newsportals in Malaysia, http://bit.ly/294nuQ7.

49 Reporters Without Borders, "Court Rejects Government Appeal Against Print Version For News Website," October 31, 2013, http://bit.ly/1wjDgJm.

50 Hafiz atim, "Malaysiakini wins court battle over print licence," *Malaysiakini*, October 1, 2012, http://bit.ly/V5bcKG; Human Rights Watch, "Malaysia," in *World Report 2013*, January 31, 2013, http://bit.ly/ZbdTes.

51 Oiwan Lam and Leila Nachawati, "Malaysia: News Sites Face Attacks on Eve of Elections," *Global Voices Advocacy*, May 4, 2013, http://bit.ly/1AvO2kY.

52 "Malaysiakini & The Malaysian Insider banned from covering PMO," *Selangor Kini*, July 8, 2014, http://bit.ly/1De24Fa; Nigel Aw, "Mkini barred from PM's office twice in t o weeks," *Malaysiakini*, July 8, 2014, http://bit.ly/1wjpy9c.

53 Mohamad Fadli, "Police report against FMT columnist," *Free Malaysia Today*, January 26, 2015, http://bit.ly/181MWC4.

54 "Najib and Umno sue Malaysiakini," *The Star Online*, June 4, 2014, http://bit.ly/1EuzNOR.

55 "Minister to sue Malaysiakini over 'reverse migration' report," Malaysiakini, Dec 8, 2015, http://bit.ly/1n7IDfO.

56 Karen Arukesamy and Bernard Cheah, "Govt not in favour of Facebook ban," *The Sun Daily*, October 1, 2014, http://bit.ly/ZrAS8H.

are the dominant languages, and many civil society groups, including those representing ethnic minorities, have a dynamic online presence.

Prime Minister Najib has his own blog and almost six million followers on both Facebook and Twitter.[57] Other government representatives are embracing ICTs, including Communications and Multimedia Minister Salleh Said Keruak, who uses his blog to counter criticism against the government and the prime minister.[58] The police force has Facebook and Twitter accounts where office s provide updates on policing activities and occasionally respond to accusations of abuse from members of the public.[59] The police chief came under fi e in 2014 for warning government critics on Twitter,[60] though the practice continued during the coverage period, when an artist was threatened for launching memes representing the prime minister as a clown (see "Digital Activism").[61]

Some of this engagement is manipulative in nature. Both government and opposition figu es are known to pay online commentators, known as cybertroopers, to generate favorable content and denigrate their opponents.[62] Since traditional media restrictions caused opposition groups to embrace online platforms relatively early, the government has struggled to catch up. The Barisan Nasional's dedicated bloggers, Unit Media Baru, deny accepting payment for their efforts.[63] The ruling party, Umno, maintains paid bloggers, but in December 2014, Prime Minister Najib expressed his disappointment when some of them publicly criticized government policies.[64]

In 2012, the government admitted paying international public relations fi m FBC Media MYR 83.8 million (US$26.5 million) between 2008 and 2010 to boost Prime Minister Najib's image abroad.[65] *Sarawak Report* also said Abdul Taib Mahmud, the then chief minister in the state of Sarawak, had separately contracted FBC Media for online publicity campaigns.[66] FBC Media, which denied wrongdoing, collapsed in 2011.[67] In 2015, *Sarawak Report* said that at least one former FBC media expert was still in the government's employment.[68]

Issues considered potentially sensitive online include Islam's official status, race, oyalty, and the special rights enjoyed by Bumiputera, who are ethnic Malays and other indigenous people, as opposed

57 Najib Razak, Facebook page, accessed Feb 28, 2016, http://on.fb.me/1CSMPmi; *NajibRazak* (blog), accessed Feb 28, 2016, http://bit.ly/1FxF5Hi

58 Salleh Said Keruak, http://sskeruak.blogspot.my/.

59 Polis Diraja, Facebook page, http://on.fb.me/1yWkBtd.

60 V Shuman, "PDRM, why not change your name to Polis Raja di Social Media (PRdSM)?" *The Ant Daily*, February 12, 2015, http://bit.ly/1LMd9Um; "Top cop's use of Twitter to issue sedition warnings raises eyebrows," *The Malaysian Insider*, February 12, 2015, http://bit.ly/1wjwzHc.

61 "Malaysian police threaten internet users for sharing clown memes of prime minister," Global Voices, Feb 13, 2016, http://bit.ly/1KUpMkf.

62 Joanna Yap, "PRS' Cyber-Troopers Ready for Coming Polls," *Borneo Post Online*, March 22, 2012, http://bit.ly/1EuCcsR; Lim Guan Eng, "Najib's new army of cyber troopers with a history of dirty tricks is proof that the 13th general election will be the dirtiest election yet," *DapMalaysia*, November 21, 2011, http://bit.ly/1MUPtib.

63 Yu Ji, "Taking the battle online," *The Star* Online, February 8, 2012, http://bit.ly/1FYNhEn.

64 Hasbullah Awang Chik, "Umno bloggers defend 'friendly fi e' after Najib's 'bangang' label," *The Malaysian Insider*, December 1, 2014, http://bit.ly/1AO0QlF.

65 Mariam Mokhtar, "Sorry no cure, BBC," *Free Malaysia Today*, February 17, 2012, http://bit.ly/1vCc51h; *Harakah Daily*, "BBC's Worldwide Apology Exposes Malaysian Govt's Image," *Malaysia* Today, February 13, 2012, http://bit.ly/1Ducumz.

66 "New Revelations Link FBC Media to BN's Dirty Tricks Blogging Campaigns—Latest Expose!" *Sarawak Report*, August 7, 2011, http://bit.ly/1zhPRgo.

67 Ian Burrell, "TV company at centre of global news fixing ow goes into administration," October 28, 2011, http://ind.pn/1FYNTd8.

68 "Too Much Partying By Najib's PR Guru Paul Stadlen?" *Sarawak Report*, Feb 11, 2015, http://bit.ly/1z8M6e4.

to the ethnic Chinese and Indian minorities. Discussing these topics can lead to prosecution, and some internet users exercise self-censorship.

Digital Activism

Online tools have been effective for political mobilization and exposing the government's grip on traditional media. Opposition supporters used social media to mobilize following the jailing of opposition leader Anwar Ibrahim for fi e years in February 2015 for sodomy, a charge his supporters say was politically motivated.[69]

The Coalition for Free and Fair Elections, which organizes for political reform, leveraged online platforms to bring tens of thousands of supporters to the streets during the Bersih 2.0 and Bersih 3.0 political rallies in 2011 and 2012, respectively. During the 2013 general election, digital campaigns to get out the vote contributed to a record 80 percent turnout of registered voters, in what observers described as the most closely fought election since independence.[70] Social media continued to be used to gather supporters for opposition rallies during the coverage period, including Bersih 4 in August 2015, when the MCMC threatened to block websites used to publicize the event,[71] and a march in the capital demanding Prime Minister Najib's resignation in January 2016.[72]

In February, after police used an official witter account to warn a graphic artist who uploaded an image of Prime Minister Najib as a clown, internet users shared clown images of the prime minister under a hashtag meaning "we are all seditious."[73] The artist was subsequently prosecuted (see "Prosecution and Detentions for Online Activities").

Violations of User Rights

The government continued to charge social media users, civil society activists and politicians for online remarks, though a sedition case against a prominent academic involving online speech was dropped. A teenage laborer was sentenced to 12 months' imprisonment for insulting a member of the Malaysian royal family on Facebook. At the same time, the government is also amending the Communications and Multimedia Act to punish social media "misuse," and threatened to require internet users to register in order to publish blogs.

Legal Environment

Malaysia's constitution provides citizens with "the right to freedom of speech and expression," but allows for limitations on that right. While some court decisions have disappointed freedom of expression advocates,[74] others show more independence. The government exercises tight control over

69 Elizabeth Zachariah, "Hundreds join Nurul Izzah for Pakatan solidarity rally in KL," *The Malaysian Insider*, February 14, 2015, http://bit.ly/1DWBe87.

70 Jonathan Head, "Malaysia election sees record turnout," *BBC News*, May 5, 2013, http://bbc.in/1JQFTxN.

71 https://www.ifex.org/malaysia/2015/08/27/protest_websites_blocked/

72 http://www.thejakartapost.com/news/2016/01/08/ngos-fume-after-malaysia-kicks-out-indonesian-activist.html

73 https://advox.globalvoices.org/2016/02/13/malaysian-police-threaten-internet-users-for-sharing-clown-memes-of-prime-minister/.

74 Reporters Without Borders, "Court's Ruling on Cartoonist's Suit Sets Disturbing Precedent for Media Freedom," July 31, 2012, http://bit.ly/1EVNG6M.

online as well as print and broadcast media through laws like the Official Sec ets Act and the Sedition Act, which dates from 1948. Violations are punishable by fines and se eral years in prison. An official moo ed increasing penalties under the Official Sec ets Act to life imprisonment and judicial caning in February 2016.[75] No formal proposal was made during the coverage period, though civil society groups were prepared to campaign against the change.[76]

In 2014, Prime Minister Najib reneged on vows made in 2013 to abolish the Sedition Act. In fact, new amendments in April 2015 widened the scope of the sedition law, allowing the government to block electronic content considered seditious.[77] Under the amended law, the penalty for sedition is now seven years in prison, up from three years previously. A new provision allows for up to 20 years for seditious activities that result in physical harm or destruction of property.[78]

In October 2015, the Malaysian Federal Court rejected a constitutional challenge to the Sedition Act filed by Dr Azmi Sha om, an academic charged under the law in September 2014 in connection with an online news article.[79] That charge was dropped in February 2016 (see "Prosecutions and Detentions for Online Activities").

Defamation is a criminal offence under Sections 499 to 520 of Malaysia's penal code. Media outlets benefit f om stronger privileges under the Defamation Act 1957 if they can prove allegedly libelous content is accurate and was published without malice;[80] lacking this protection, bloggers risk punitive damages.

In 2012, parliament passed an amendment to the 1950 Evidence Act that holds intermediaries liable for seditious content posted anonymously on their networks or websites.[81] This would include hosts of online forums, news outlets, and blogging services, as well as businesses providing Wi-Fi services.[82] The amendment also holds someone liable if their name is attributed to the content or if the computer it was sent from belongs to them, whether or not they were the author.[83] The legal change was pushed through hurriedly, but garnered significant public acklash after its passage, which failed to prevent it going into effect.[84] No implementation has been reported.

75 'Malaysia ponders stricter punishments for whistleblowers, journalists', ifex, Feb 9, 2016, http://bit.ly/28UoIhb.

76 'Groups to educate public on info rights to counter planned OSA amendments', Malay Mail Online, May 12, 2016, http://bit.ly/28TTKDa.

77 Anisah Shukry and Eileen Ng, "Sedition Act stays, says Najib," November 27, 2014, http://bit.ly/1uKsQQF; Trinna Leong and Al-Zaquan Amer Hamzah, "Malaysia toughens sedition law to include online media ban, mandatory jail," ed. Paul Tait, *Reuters*, April 10, 2015, http://reut.rs/1Ykub33, "Amendments to Sedition Act passed with several changes", *New Straits Times*, April 10, 2015, http://bit.ly/1acd664; Marie Harf, "Malaysia's Sedition Act Amendments", US Department of State, press statement, April 14, 2015, http://1.usa.gov/1OQB6ii.

78 Mong Palatino, "Malaysia strengthens Sedition Act," *The Diplomat*, April 13, 2015, http://bit.ly/1IJCBJg.

79 Human Rights Watch, "Space for public debate and free speech is rapidly narrowing in Malaysia, says new report," via IFEX, October 28, 2015, https://www.ifex.org/malaysia/2015/10/28/report_criticism_crime/ ; Article 19, "Malaysia: Sedition Act upheld in further blow to free expression," via IFEX, October 13, 2015, https://www.ifex.org/malaysia/2015/10/13/court_ruling_sedition_act/.

80 Abdul Latiff Ahmad et al., "Regulating Blogs in Malaysia," *The Innovation Journal: The Public Sector Innovation Journal* 16, no. 3 (2011) http://bit.ly/1BMUO8r.

81 Eva Galperin and Katrina Kaiser, "This Week in Internet Censorship: Points system for Weibo, Activist Released in Bahrain, Censorship in Malaysia, Ethiopia, and More," Electronic Frontier Foundation, May 31, 2012, http://bit.ly/1C8CXIG.

82 Teoh El Sen, "Pakatan seeks to halt new evidence act," *Free Malaysia Today*, June 28, 2012, http://bit.ly/1JZ9sxc.

83 Laws of Malaysia, "Evidence (Amendment) (no. 2) Act 2012," http://www.federalgazette.agc.gov.my/outputaktap/20120622_A1432_BI_Act%20A1432%20BI-evidence%20(amendment)%20(no.%202).pdf.

84 A. Asohan, "Govt Stealthily Gazettes Evidence Act Amendment, Law is Now in Operation," *Digital News Asia*, August 8, 2012, http://bit.ly/1JZ9KUF.

The government has also pursued prosecutions for online content based on the Communications and Multimedia Act 1998 (CMA). The Act's broadly worded Section 211 bans content deemed "indecent, obscene, false, threatening, or offensive;" Section 233 punishes the "improper use of network facilities or network service," when such content is shared via the internet.[85] Amendments to the CMA and the related Communications and Multimedia Commission Act (CMCA) 1998 were expected to be tabled in late 2016,[86] including measures to curb "social media misuse, that infringe, among others, on religious and racial sensitivities, or for recruitment of terrorists."[87] Critics say the intention is to stop online criticism of the government.[88] A minister said the amendments were not designed to curb free speech, but to "create a mechanism to detect irresponsible individuals who cause false news and slanderous allegations."[89]

Prosecutions and Detentions for Online Activities

In 2015 and 2016, police arrested and prosecuted internet users for remarks against the government and its policies, royalty, or Islam, continuing a trend which started in the last review period.[90] The government said it had registered 34 complaints regarding the abuse of social media between January 1 and February 4, 2016 alone, bringing at least two to court and 12 more under investigation.[91]

Several arrests were made for sedition or for violating the Communications and Multimedia Act (CMA). Police charged an activist for his social media comments;[92] arrested a woman for insulting the police on Facebook;[93] and charged a construction consultant for insulting the prime minister on Facebook.[94] Those arrested were all released on bail, but their cases were ongoing at the end of the reporting period.

One case was particularly high profile. In anuary 2016, artist and activist Fahmi Reza published a caricature of Prime Minister Najib Razak as a clown on Facebook with a comment on the use of sedition charges to suppress free expression (see Digital Activism). In March, opposition lawmaker Nurul Izzah Anwar was investigated under the CMA and Section 504 of the Penal Code for sharing the same clown caricature on Instagram, though no further action had been taken in mid-2016.[95] In June, Fahmi Reza was charged under Section 233 of the CMA for "improper use of network facilities or network service" in relation to the image. He faces a maximum fine f MYR 50,000 (US$11,900) and prison sentences up to one year.[96]

On April 28, 2016, 19-year-old laborer Muhammad Amirul Azwan Mohd Shakri was arrested for posting Facebook comments considered insulting to the crown prince of the southern state of Johor

85 OpenNet Initiative, "Malaysia," in *Country Profiles*, https://opennet.net/research/profiles/malaysi .

86 "Regulation for social media in proposed amendments to communication acts," *The Malaysian Insider*, June 8, 2015, http://bit.ly/1TsbtkR.

87 S. Neishasa, "Proposal to control social media desperate," *Berita Daily*, August 3, 2015, http://bit.ly/1Emnhyb.

88 S. Neishasa, "Proposal to register online news portals ridiculous," *Berita Daily*, August 6, 2015, http://bit.ly/1N2cCkb.

89 "We are not planning to censor free speech," *Berita Daily*, Aug 14, 2015, http://bit.ly/1TgO1fh.

90 "Malaysian government must stop ongoing crackdown and honour its pledge to repeal the Sedition Act," *Suaram*, Sept 12, 2014, http://bit.ly/1EzqaOW.

91 "Cases of social media abuse rising," *The Star Online*, Feb 23, 2016, http://bit.ly/1Rx9yNd.

92 "Malaysia: Activist charged over Facebook posts needs support," *Green Left Weekly*, October 31, 2015, http://bit.ly/1TJtzC4.

93 "Woman arrested after Facebook posting on cops' treatment of son," *The Malaysian Insider*, December 25, 2015, http://bit.ly/1QFQ0To.

94 "Malaysian consultant claims trial to insulting Najib on Facebook," Asiaone, February 19, 2016, http://bit.ly/215hZSp.

95 'Police record Nurul Izzah's statement over Instagram post,' *New Straits Times*, March 7, 2016, http://bit.ly/28QRgZW.

96 'Malaysia: Ongoing crackdown on social media;, Amnesty International, June 7, 2016, http://bit.ly/28WohB9.

(Sultans constitutionally rule nine of the country's sixteen states and federal territories).[97] He was also charged under Section 233 of the CMA. In June, outside the coverage period of this report, he was convicted on 14 counts of posting insulting comments with the intention of hurting the prince's feelings and sentenced to one year in prison, starting from the date of his arrest. News reports said he was unrepresented in court. His family filed an appeal [98] At least three others were reported to be under investigation for insulting the prince on Facebook in 2016.[99]

Two prominent politicians who oppose Prime Minister Najib Razak are also being investigated over their social media comments. Former Prime Minister Mahathir Mohamad, now a fie ce critic of the current administration, was questioned by police over a blog post accusing the attorney general of protecting the prime minister from prosecution for corruption.[100] As of mid-2016, the police were transferring the investigation to the attorney general for possible prosecution.[101] Zaid Ibrahim, a former law minister, is also being investigated for sedition over a blog post in which he criticized the judiciary.[102]

Some prominent investigations under the Sedition Act were still pending during this review period.[103] A handful of political leaders are still awaiting trial over tweets criticizing opposition leader Anwar Ibrahim's fi e year jail sentence on sodomy charges in February 2015.[104] Lawyer and activist Eric Paulsen's trial is pending following his February 2015 arrest over a tweet stating that the Malaysian Islamic Development Department (Jakim) was spreading extremism through their Friday sermons; he was released on bail.[105] Popular cartoonist Zunar was arrested and charged with sedition in early 2015 over his pro-Anwar tweet which questioned the Malaysian judiciary. He was released on bail.[106]

One trial also concluded. The Facebook user known as "Man Namblast" was found guilty of sedition for posting remarks about Hindus in June 2014,[107] and fined MYR 4,000 (US$910) by the Sessions Court in Kuala Lumpur on November 18, 2015.[108] The man, a teacher, faced a maximum fine f MYR 5,000 or a jail term of up to three years, or both.

Legal actions against digital journalists intensified during the co erage period. Police questioned *The Malaysian Insider* editors on February 26, 2016, over an article which quoted unnamed sources as saying that an independent anticorruption panel had recommended charging Prime Minister Na-

97 "Teenager gets one-year jail sentence for insulting TMJ," *Malaysiakini,* June 7, 2016, https://www.malaysiakini.com/news/344372; "Maximum jail for insult of Johor prince 'excessive', says lawyer," *Malay Mail*, June 8, 2016, http://bit.ly/28NuRKr.

98 'Family of youth appeals against jail sentence for Facebook insult', *Star Online*, June 13, 2016, http://bit.ly/28QcLvI.

99 'Malaysia: Ongoing crackdown on social media;, Amnesty International, June 7, 2016, http://bit.ly/28WohB9; 'Man held for allegedly insulting Johor Crown Prince', Star Online, June 17, 2016, http://bit.ly/28Nv0O7.

100 "Police question Mahathir again over criticism of Najib," *Straits Times*, February 25, 2016, http://bit.ly/1oROg3L

101 "Police almost done with probe into Mahathir blog post," *Free Malaysia Today*, February 27, 2016, http://bit.ly/1TJwXNh

102 "After police quizzing, Zaid expects sedition charge over article critical of judiciary," Malay Mail Online, January 12, 2016, http://bit.ly/1QmwuQ8.

103 "Unprecedented crackdown on freedom of expression a threat to democratic government," Centre for Independent Journalism, February 13, 2015, http://bit.ly/1wxanz5.

104 "Cops to quiz Rafizi, Nga in sedition p obe over Anwar verdict remarks," *The Malay Mail Online*, February 23, 2015, http://bit.ly/1BpZOhv.

105 Jennifer Gomez, "Human rights lawyer Eric Paulsen charged with sedition," *The Malaysian Insider*, February 5, 2015, http://bit.ly/1v5jNkb.

106 Diyana Ibrahim, "Cartoonist Zunar hauled up for sedition after tweet criticising Malaysian judiciary," February 11, 2015, *The Malaysian Insider*, http://bit.ly/1Bq03ZQ.

107 "FB user held over seditious remarks", *The Star Online*, February 12, 2014, http://bit.ly/1LVXjES.

108 "Teacher fined RM4,000 for seditious posting on acebook," *The Malaysian Insider*, Nov 18, 2015, http://bit.ly/1VMmWxU.

jib.[109] The government said the story was fake.[110] No court action was taken, but the MCMC blocked the website (see "Blocking and Filtering"), and it closed down in March (see "Media, Diversity, and Content Manipulation"). The same editors were previously arrested in March 2015 over a report on Islamic criminal laws,[111] which was attributed to an unnamed source.[112]

Police raided *Malaysiakini* offices on No ember 6 and November 9, questioning staff about the source of a story on political corruption, threatening defamation charges, and seizing equipment. The law minister had confi med the story. Police also raided offices belonging o *The Star* on November 6 regarding an article on the same topic.[113] Separately, Minister Abdul Rahman Dahlan also filed a defamation suit against *Malaysiankini* in December 2015 (see "Media, Diversity, and Content Manipulation").[114] In June 2014, Prime Minister Najib filed a suit against *Malaysiakini* for two allegedly defamatory articles that compiled readers' comments.[115] That case was ongoing in 2016. In 2015, Najib also filed a suit against t o other news portals, the opposition party organ *Harakah Online* and the pro-opposition *Media Rakyat*, claiming that they had defamed him. Two charges against *Media Rakyat* also name two opposition lawmakers.[116] If defeated, the websites could be required to pay significant damages

Journalist Aisyah Tajuddin and independent radio station BFM were hauled up for mocking Islam in a video posted in YouTube in March 2015. BFM Radio removed the video from its YouTube page, but Aisyah was subsequently investigated by police for blasphemy, and could face up to a year in jail if convicted. She also received death and rape threats over the video. There were no developments in the investigation in early 2016.[117]

Some outstanding investigations were discontinued. The authorities dropped a September 2014 sedition charge against academic Dr Azmi Sharom on February 12, 2016.[118] He was charged over an article in an online news portal and faced a jail term of up to seven years or a maximum fine f MYR 5,000 (US$1,040), or both if found guilty.[119] The attorney general also withdrew a May 2014 sedition charge against opposition politician Teresa Kok.[120] Kok was charged with insulting Islam and the

109 "Police probe fi e TMI editors over report on MACC," Astro Awani, February 26, 2016, http://bit.ly/1VLxXzB.

110 "MACC panel denies Malaysian Insider report," Astro Awani, February 25, 2016, http://bit.ly/1n9VqyA.

111 Austin Ramzy, "Editors and Executives of News Website Malaysian Insider Are Arrested," *The New York Times*, March 31, 2015, http://nyti.ms/1IMvYVw; and "Police arrest Edge, TMI executives for sedition," *The Malaysian Insider*, March 31, 2015, http://bit.ly/1yumAQi; 'Editors and Executives of News Website Malaysian Insider Are Arrested', *New York Times*, March 31, 2015, http://nyti.ms/1IMvYVw.

112 "Clarification and apolog ," *The Malaysian Insider*, April 4, 2015, http://bit.ly/1I7vxYQ.

113 John Berthelsen "Malaysian Police Raid Independent Website," *Asia Sentinel,* November 9, 2015, http://www.asiasentinel.com/blog/malaysian-police-raid-independent-website/.

114 "Rahman Dahlan to sue news portal," The Star Online, Dec 8, 2015, http://bit.ly/1QcUUdp; "Minister to sue Malaysiakini over 'reverse migration' report," Malaysiakini, Dec 8, 2015, http://bit.ly/1n7IDfO.

115 "Najib, Umno sue Mkini over readers' comments," *Malaysiakini,* June 3, 2014, http://bit.ly/1AUi1BP.

116 V Anbalagan, "Najib, Rosmah sue Rafizi, po tal owner over diamond ring remark," *The Malaysian Insider*, April 17, 2015, http://bit.ly/1GS1t2Q; M Mageswari, "Najib sues Tony Pua, portal owner for defamation," *The Star Online*, March 6, 2015, http://bit.ly/1E6lTy; Maizatul Nazlina, "Najib sues Harakahdaily for defamation," *The Star Online*, March 20, 2015, http://bit.ly/1OQDuWl.

117 Tse Yin Lee, "The perils of speaking out against Islamic law in Malaysia, "*BBC News*, March 29, 2015, http://bbc.in/1aaMJhU; Boo Su-Lyn, "BFM journalist gets death, rape threats over video questioning hudud," *The Malay Mail Online*, March 20, 2015,http://bit.ly/1I7udF9.

118 "Freed from sedition charge, Azmi Sharom says 'common sense' won," Malay Mail Online, Feb 12, 2016, http://bit.ly/1T3qTk1.

119 V Anbalagan, "Azmi Sharom's Sedition Act challenge referred to Federal Court," *The Malaysian Insider,* November 5, 2014, http://bit.ly/18xIADG.

120 "Sedition charge against Teresa Kok dropped," The Star Online, Nov 20, 2015, http://bit.ly/1WRTI0R.

nation's leaders four months after sharing an 11-minute video that used invented Chinese New Year predictions to satirize government policies.[121]

Surveillance, Privacy, and Anonymity

Real-name registration is not required for participation in Malaysia's blogosphere, nor is it required to use a cybercafe. Beginning in 2007, all mobile phone owners, including roughly 18 million customers using prepaid service at the time, were required to register as part of an effort to decrease rumor mongering.[122] The rule appears to have been weakly enforced.

The government, however, is revisiting an old proposal to make it compulsory for bloggers to register with the Communications and Multimedia Ministry, supposedly to curb defamatory and irresponsible writing. Nur Jazlan Mohamed, the deputy home minister, said the proposal was aimed at ensuring that articles on blogs or social networks "were accurate, valid, ethical and did not abuse the internet."[123] In mid-2016, the proposal had yet to be brought to parliament.[124]

The extent of government surveillance of ICT content is not known, but privacy protections are generally poor.[125] In 2008, the MCMC formed a panel composed of representatives from the police, the attorney general's office, and the home minist y to monitor websites and blogs. Although it still appears to be active, it has not publicly intervened in internet freedom issues. Court documents indicate that police regularly gain access to the content of text messages from telecommunications companies, sometimes without judicial oversight. The Security Offenses (Special Measures) Act (SOSMA), granted wide-ranging powers for the public prosecutor—and in emergency situations, the police—to intercept communications without the need for a court order in cases involving security offenses.[126]

The Malaysian Personal Data Protection Act 2010, which regulates the processing of personal data in commercial transactions, came into effect in November 2013. The law makes it illegal for commercial organizations to sell personal information or allow third parties to use it, with penalties up to MYR 100,000 (US$27,400) or one year imprisonment. Federal and state governments are exempted from the law, as is data processed outside Malaysia.[127] But the act requires that information about Malaysians be stored locally, and limits conditions under which the data can be transferred abroad, though it is not clear how far that requirement is enforced.[128]

In 2013, the University of Toronto-based research group Citizen Lab reported detecting software known as FinFisher, described by its distributor Gamma International as "governmental IT intrusion and remote monitoring solutions," on 36 servers worldwide, including one in Malaysia.[129] The soft-

121 P. Ramani, "Teresa Kok charged with sedition over CNY video," *Free Malaysia Today,* May 6, 2014, http://bit.ly/188NUMT.

122 "Dec 15 Registration Deadline Stays: MCMC," Bernama, August 18, 2006, http://bit.ly/1zq73QJ.

123 "Bloggers registration can prevent defamation, disunity – experts," Bernama, Feb 22, 2016, http://bit.ly/1WFGPHj.

124 "Registration of blogs, a draconian move," The Malaysian Insider, February 23, 2016, http://bit.ly/1WRTirg.

125 Privacy International, *Final Report for "Privacy in Asia" Scoping Project,* November 2009, https://idl-bnc.idrc.ca/dspace/handle/10625/40000.

126 Mickey Spiegel, "Smoke and Mirrors: Malaysia's "New" Internal Security Act," *Asia Pacific Bulletin,* no. 167, (June 2012), http://bit.ly/1Amz9N8.

127 Barry Ooi, "How the Personal Data Protection Act Impacts the Market Research Industry," December 29, 2012.

128 Anupam Chander and Uyen P. Le, "Breaking the Web: Data Localization vs. the Global Internet,"(UC Davis Legal Studies Research Paper No. 378, *Emory Law Journal*, April 2014) http://bit.ly/1Bq2KuA.

129 Morgan Marquis-Boire et al., "You Only Click Twice: FinFisher's Global Proliferation," Citizen Lab, March 13, 2013, http://bit.ly/1grgVFd.

ware potentially allows the server to steal passwords, tap Skype calls, or record audio and video without permission from other computers, according to Citizen Lab. *The Malaysian Insider* subsequently documented FinFisher's presence in Malaysia based on a *New York Times* report.[130] The MCMC threatened *The Malaysian Insider* with criminal charges, though none were filed However, Citizen Lab later reported they had further identified "a Malaysian election- elated document" they characterized as a "booby-trapped candidate list" containing surveillance spyware.[131] Because the spyware is only marketed to governments, "it is reasonable to assume that some government actor is responsible," the group concluded. A separate Citizen Lab report published in 2014 said a Malaysian government agency was a "current or former user" of Remote Control System spyware marketed by the Milan-based Hacking Team.[132]

During this review period, the Prime Minister's Office again denied having pu chased spyware to surveil citizens. On January 1, 2016, Minister Azalina Othman Said disputed a fresh claim by a technology blogger that such purchases were made in September 2013 and July 2014, based on internal Hacking Team documents leaked by hackers in 2015. The minister could not confi m if other government agencies had made such purchases.[133]

Intimidation and Violence

Physical violence sporadically affects traditional and online journalists in Malaysia.[134] On July 12, 2015, two photographers and a reporter were assaulted while covering a racially-motivated fracas at a shopping mall.[135] Government officials esponded to the assault by calling for deeper regulation of social media, on the grounds that digital platforms were responsible for inflaming ensions around the incident.[136] No similar incidents affecting digital media practitioners were reported.

Technical Attacks

In the past, independent online news outlets and some opposition-related websites have faced intense distributed denial-of-service (DDoS) attacks, often at moments of political importance. The attacks force sites to crash by overloading the host server with requests for content. Some observers believe such attacks are either sponsored or condoned by Malaysian security agencies, since they often align with government priorities. *Malaysiakini* was one of many sites reporting on the opposition which were subjected to an apparently coordinated assault before the 2013 elections.[137] No severe or crippling incidents were reported by news portals or opposition websites during this review period.

130 Boo Su-Lyn, "Malaysia uses spyware against own citizens, NYT reports," *The Malaysian Insider,* March 14, 2013,http://bit.ly/1E52SSf. The original *New York Times* article: Nicole Perlroth, "Researchers Find 25 Countries Using Surveillance Software," *The Business of Technology* (blog), *The New York Times* March 13, 2013, http://nyti.ms/1G2XSOv.

131 "Short Background: Citizen Lab Research on FinFisher Presence in Malaysia," Citizen Lab, May 2013, http://bit.ly/1zNT7Bo.

132 Bill Marczak et al, "Mapping Hacking Team's "Untraceable" Spyware," Citizen Lab, February 17, 2014, http://bit.ly/1kPDo0Y.

133 "No, PMO did not buy spyware, reiterates Azalina," Berita Daily, January 1, 2016, http://bit.ly/1Qd9ceg.

134 Committee to Protect Journalists, "Journalists assaulted, detained during rally in Malaysia," April 30, 2012, http://cpj.org/x-/4b4a.

135 "NUJ condemns assault on journalists at Low Yat Plaza," FreeMalaysiaToday, July 13, 2015, http://bit.ly/215q5uf.

136 Center for Independent Journalism, "Regulating social media not the answer to recent violence in Malaysia," via IFEX, July 16, 2015, https://www.ifex.org/malaysia/2015/07/16/social_media_violence/.

137 Human Rights Watch, "Malaysia: Violence, Cyber Attacks Threaten Elections," May 1, 2013, http://bit.ly/1Ezugqi; Shawn Crispin, "In Asia, Three Nations Clip Once-Budding Online Freedom," in *Attacks on the Press*, Committee to Protect Journalists (New York: Wiley, February 2013), http://bit.ly/1wxdabx.

Freedom House

Mexico

	2015	2016
Internet Freedom Status	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	9	8
Limits on Content (0-35)	10	10
Violations of User Rights (0-40)	20	20
TOTAL* (0-100)	**39**	**38**

* 0=most free, 100=least free

Population:	**127 million**
Internet Penetration 2015 (ITU):	**57 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- Mexico's internet penetration improved in 2015, reaching more than 57 percent of the population, although regional disparities in access persist (see **Availability and Ease of Access**).
- At least three reporters who covered sensitive stories online and seven other journalists were killed during the coverage period. Mexico continued to be one of the most hostile environments for reporters in the world (see **Intimidation and Violence**).
- The Supreme Court upheld new data retention requirements and real-time geolocation provisions passed in 2014 despite civil society pressure, although it did confi m the need for authorities to obtain a judicial warrant to access users' metadata (see **Surveillance, Privacy, and Anonymity**).
- At least three news sites were hit with cyberattacks on election day in Puebla, disrupting voters' access to information at a critical time. Other sites were targeted throughout the year (see **Technical Attacks**).

Introduction

While internet access and quality have improved, high levels of physical and technical violence against online media continued to impact Mexico's internet environment over the past year.

Recent telecommunications reforms have begun to induce changes in Mexico's ICT market by increasing competition and slashing prices for some telecommunication services. Nevertheless, Mexico still faces challenges in its quest to extend internet access to all citizens, as regional disparities create a stark digital divide.

High levels of violence against journalists continue to severely limit internet freedom and fuel a climate of self-censorship. But online journalists, bloggers, and social media activists still risk their safety to report on local crime and corruption. During this period, online publications suffered cyberattacks, journalists received death threats, and at least two online journalists, and another print journalist who used social media to report on violence, were killed. Although the June 2012 Law to Protect Human Right Defenders and Journalists created a protection mechanism to support at-risk journalists and human rights defenders, it has suffered from inadequate enforcement and delays in responding to requests.[1]

Using the tense security situation and the war on drugs as justification, the go ernment has also increased its surveillance powers. In May 2016, the Supreme Court ruled that data retention requirements and real-time geolocation included in the 2014 Telecommunications Law were constitutional. Under that law, internet service providers (ISPs) and mobile providers must store their customers' metadata for at least two years and provide detailed communication records to police. In a positive move, the ruling did establish the need for a judicial warrant to access users' metadata. Meanwhile, reports concerning a vast state surveillance apparatus have continued to call into question the adequacy of privacy protections and the scope of government surveillance activities. The Hacking Team leak in July 2015 revealed that Mexico was the company's biggest client worldwide and that the company had signed more than 14 contracts with various state and federal agencies.

Obstacles to Access

The implementation of the 2014 Telecommunications Law has opened the ICT market to greater competition. While new legislation and government initiatives have the potential to increase availability and ease of access, the real-world impact of these changes in some parts of the country remains to be seen, as the country still suffers from a wide digital divide between the north and south.

Availability and Ease of Access

Internet penetration in Mexico has increased significantly o er the past years. According to data

1 Washington Office on Latin America and eace Brigades International, "El Mecanismo de Protección para Personas Defensoras de Derechos Humanos y Periodistas en México: desafíos y oportunidades," [The Mechanism for the Protection of Human Rights Defenders and Journalists in Mexico: Challenges and Opportunities], February 3, 2015, http://bit.ly/1zPQbtg; See also: Edgar Cortez, "Sólo en el discurso, la protección a periodistas y defensores de ddhh" [Only discourse, the protection of journalists and human rights defenders], *Animal Político,* July 4, 2016, http://bit.ly/29k9H7D.

from the International Telecommunications Union (ITU), internet penetration reached 57.43 percent in Mexico in 2015, compared to 44.39 percent in 2014 and just 26.34 percent in 2009.[2]

Telecommunications reforms promoted by President Enrique Peña-Nieto in 2013 may substantially reshape the telecommunications industry and increase access. The government has already noted some key improvements, including the elimination of national roaming fees, lower mobile telephony rates and an increase in foreign investment.[3] The reform package also seeks to develop a Shared Network (Red Compartida) and Backbone Network (Red Troncal) to improve quality, affordability and coverage of telecommunication services across the country.[4] Aiming to expand mobile broadband service at more affordable prices, the Red Compartida project would create a shared wholesale network, notably using 90 MHz of the 700 MHz band.[5] The government began the bidding process for this network in January 2016.[6] State-owned company Telecomm (Telecommunications of Mexico) would also use and develop the national infrastructure of the Federal Electricity Commission (CFE) to expand the fibe -optic cable network across the country.[7] As a fi st step in September 2015, CFE announced the concession of three fibe -optic strands to Telecomm, one of which is intended for the Red Compartida.[8]

However, the real-world impact of these changes remains to be seen in some parts of the country.[9] Mexico continued to suffer from limited access and the digital divide between the north and south is still wide. While 39.2 percent of homes had internet connections in 2015, the proportion of homes with internet connections in some of the poorest states has only improved slightly.[10] In 2015, Quintana Roo and Sonora entered the group of states with more than half of homes with access to the internet, along with Nuevo Leon, Mexico City, and Baja California. At the same time, only 1 in 10 had access to the internet in Chiapas and 2 in 10 in Oaxaca.[11]

Such limited and disparate connectivity rates are also evident in the relatively small percentage of internet users with broadband access. Although the number of Mexicans with broadband subscriptions has increased over the past decade, growing from 0.4 percent in 2003 to 11.16 percent in

2 International Telecommunications Union, "Percentage of Individuals Using the Internet," accessed September 20, 2016, http://bit.ly/1FDwW9w.

3 Secretaría de Comunicaciones y Transportes [Secretariat of Communications and Transportation], "Regulación Mexicana de Telecomunicaciones, de las menos restrictivas del mundo: OCDE" [Mexican Telecommunications Regulation, one of the least restrictive in the world: OECD], June 23, 2016, http://bit.ly/2e8ODXp; See also: Federal Telecommunications Institute, Three Years After the Constitutional Reform, June 2016, http://bit.ly/29zZ5zh.

4 Secretaría de Comunicaciones y Transportes, "The SCT and the IFT sign agreements for a "shared network" in the 700 mhz band," Press release, October 9, 2014, http://bit.ly/2felUMY.

5 Secretaría de Comunicaciones y Transportes, "Red Compartida: general criteria" July 17, 2015, http://bit.ly/2edjz80.

6 Anthony Harrup, "Mexico Launches Bidding Process for Shared Mobile Network," *The Wall Street Journal,* January 29, 2016, http://on.wsj.com/2fv48nN.

7 Claudia Juarez Escalona, "Telecomm controlará fibra óptica de la CFE" [elecomm will control the CFE's fiber optic net ork], *El Economista*, May 27, 2014, http://bit.ly/1NXBVmF.

8 Miriam Posada García, "Cederá CFE hilos de fibra óptica a elecomm" [CFE will concede fiber optic strands o Telecomm], *La Jornada,* October 1, 2015, http://bit.ly/1VsJT7U; See also: José Guadarrama, "La red de fibra óptica de la CFE, a elecomm este mes" [The fiber optic net ork: to Telecomm this month], Excelsior, January 2, 2016, http://bit.ly/2fv3WVz.

9 Christine Murray, "As Mexico lauds telecom reform, rural poor search for connection," *Reuters,* October 27, 2016, http://reut.rs/2f5JiP4.

10 Instituto Nacional de Estadística y Geografía, "Módulo sobre disponibilidad y uso de las tecnologías de la información en los hogares, 2015," [Module on availability and usage of technology at home, 2015], accessed October 13, 2016, http://bit.ly/1MmCHGH.

11 Instituto Nacional de Estadística y Geografía, "Módulo sobre disponibilidad y uso de las tecnologías de la información en los hogares, 2015."

2015,[12] Mexico still falls significantly below the b oadband penetration rates of other OECD countries, which have an average rate of approximately 29 percent.[13] In Mexico where the minimum wage is approximately US$120 a month,[14] the high price of broadband service, which can range from US$26 to US$100 per month,[15] is a significant fac or in the country's low broadband penetration rate.

Internet cafes and the availability of internet at the workplace and schools have partially improved disparities in internet use between socioeconomic groups, but mobile devices are increasingly becoming a popular means for accessing the internet. About 87 percent of internet users access the internet from home, 38 percent from work, 28 percent from school, and 25 percent from public places. The number of users accessing the internet from mobile devices increased by 17 percentage points since 2014, representing 52 percent, while those using cybercafes is decreasing, representing 14 percent.[16]

In 2015, mobile broadband subscriptions reached a penetration rate of roughly 52.1 percent, overwhelmingly surpassing the penetration rate of fi ed broadband subscriptions, at 12.1 percent.[17] Mobile phone access is significantly mo e widespread in Mexico than internet use, with the ITU reporting a mobile penetration rate of 85.3 percent (about 107 million subscriptions) as of 2015.[18] This rate still puts the country behind other countries in the region. However, the number of smartphone users in Mexico is increasing rapidly as new companies are entering the mobile phone market. An eMarketer study estimated that the number of smartphone users rose by 41.4 percent in the second quarter of 2015 when compared with the same period a year earlier, with a total of 62.5 million, or 59.8 percent of all mobile connections in Mexico.[19] The prevalence of smartphones is due in part to a drop in prices for mobile phone use,[20] the increasing availability of smartphones, and promotions that narrow the price gap between basic phones and smartphones.

Restrictions on Connectivity

There were no recorded activities or public incidents related to government imposed restrictions on ICT connectivity during this coverage period. Article 190 in the 2014 Telecommunications Law, however, authorizes the "appropriate authority" within the Mexican government to request the suspension of telephone service in order to "halt the commission of crimes."[21]

12 OECD, "Historical penetration rates, fi ed and wireless broadband," *OECD Broadband Portal,* updated February 2016, http://bit.ly/1Brdh9K; See also: Patricia Rey, "Mexico, second worst OCDE country for broadbrand penetration," *BNAmericas*, February 27, 2015, http://bit.ly/1KG2NVZ.

13 OECD, Fixed Broadband Subscriptions, Q2 2015, accessed October 14, 2016, http://bit.ly/2dSRRhI.

14 Comisión Nacional de Salarios Mínimos [National Commission on Minimum Salaries], Press Release, December 11, 2015, http://bit.ly/1YaiLkQ.

15 Danielle Kell et al, "The Cost of Connectivity 2014: Data and Analysis on Broadband offerings in 24 cities across the world," Policy Paper, Open Technology Institute, October 30, 2014, http://bit.ly/1L0Cco0.

16 Asociación Mexicana de Internet (AMIPCI), "12º Estudio sobre los Hábitos de los Usuarios de Internet, Mexico 2016" [12th Study on Internet User Habits, Mexico 2016], accessed October 14, 2016, http://bit.ly/29SY60u.

17 OECD, Total fi ed and wireless broadband subscriptions by country, December 2015, accessed September 21, 2016, http://bit.ly/25NH4GL; See also: PwMexico, Overview of the telecommunication Sector in Mexico, February 2015, http://pwc.to/1ST6Sdc.

18 International Telecommunications Union, "Mobile-cellular telephone subscriptions, 2000-2015," accessed September 21, 2016, http://bit.ly/1FDwW9w.

19 eMarketer, Mexico's smartphone User Base Reaches 62.5 Million, October 16, 2015, http://bit.ly/1LUQPMP.

20 "Precios de telefonía móvil, de los más bajos en 1T16" [Mobile telephone prices, the lowest in Q1 2016], *El Financiero,* April 14, 2016, http://bit.ly/1NjfRpc.

21 Artículo 189-190 de Ley Federal de Telecomunicaciones y Radiodifusión" [Art. 189-190 o Federal Telecommunications and Radio Law], http://bit.ly/1zCzcYq.

Civil society groups successfully rallied to remove wording from earlier drafts of the Telecommunications Law that would have allowed the government to temporarily block telecommunications signals "in events and places critical to the public and national security."[22] Although the version of the law that was approved narrowed the parameters for blocking telecommunications signals in comparison with the proposed draft of the law, there were still concerns that authorities could abuse these provisions to limit expression in critical moments.

Although the majority of the backbone infrastructure in Mexico is privately owned, the state-owned company Telecomm has taken on greater control of the infrastructure, after taking over fibe -optic infrastructure from the Federal Electricity Commission.[23] Mexico has only one internet exchange point (IXP), set up by KIO Networks in April 2014. Experts say that this IXP may increase efficiency and reduce costs for Mexican ISPs by helping to manage traffic ac oss networks.[24]

ICT Market

Under constitutional reforms to the telecommunications sector signed in 2013,[25] companies are prohibited from controlling more than 50 percent of the market share. In March 2014, the recently created Federal Institute for Telecommunications (IFETEL) declared América Móvil a dominant company, indicating that it violated antitrust standards under the law. In response, América Móvil preemptively started selling assets to comply with the new regulations.[26] The new Telecommunications Law published in July 2014 allowed IFETEL to take measures to reduce the market dominance of América Móvil's holdings in the mobile (Telcel) and fi ed-line (Telmex) market.

In an important step that has the potential to reduce costs and obstacles to calling between phone networks, IFETEL determined that the company must eliminate mobile roaming charges and fees for receiving incoming calls from rival providers on Telcel's network. Under new regulations, América Móvil also initiated steps to allow other telecommunications providers to use its infrastructure, and after a long legal dispute, América Móvil and Axtel reached an agreement for the latter to offer mobile phone services on América Móvil's network.[27]

Despite the regulatory actions, as of 2015 América Móvil's Telmex and Telcel still dominate the ICT landscape with 60.7 percent of landline subscriptions (a 2 percent decrease from 2014) and 70.7 percent of the wireless market (a 4.3 percent decrease from 2014), respectively. The top competitor in fi ed-line subscriptions, Grupo Televisa, accounted for 20.1 percent, followed by Megacable

22 Rafael Cabrera, "Bloqueo, censura… ¿Qué propone Peña Nieto para internet?" [Blocking, Censorship… What is Peña Nieto proposing for internet], *Animal Político*, March 29, 2014, http://bit.ly/1KOyri1.

23 Peralta, "Telecomm venderá conectividad de fibra óptica en 2015" [elecomm will sell fiber optic connectivity in 2015], *Expansión*, December 11, 2014, http://bit.ly/2deO119.

24 Julio Sánchez Onofre, "Primer IXP in Mexico, una realidad," *El Economista*, April 30, 2014, http://bit.ly/1h3UAQG. See also: "Inauguración del primer IXP mexicano," [Inauguration of the fi st IXP] April 30, 2014, http://bit.ly/1ULslbw.

25 "Mexican Senate approves telecoms-reform bill," *Al Jazeera*, May 1, 2013 http://bit.ly/1KOyU3J; See also: Dolia Estevez, "Mexico's Congress Passes Monopoly-Busting Telecom Bill, Threatening Tycoon Carlos Slim's Empire," *Forbes*, May 1, 2013, http://onforb.es/1iFp4cQ.

26 Dolia Estevez, "In A Surprising Move, Mexican Billionaire Carlos Slim To Sell Telecom Assets In Compliance With New Anti-Trust Rules," *Forbes*, July 9, 2014, http://onforb.es/1iFpLDh.

27 Anthony Harrup, "Mexico's América Móvil, Axtel Settle Disputes," *The Wall Street Journal*, March 18, 2015, http://on.wsj.com/1RbVesD.

with 11.9 percent, and Axtel with 3.2 percent. The top competitor in wireless connections, Telefónica, claimed 18.5 percent of wireless subscriptions, and AT&T 9.9 percent.[28]

Although it is still early to fully assess the impact of the Telecommunications Law on market concentration, competition, and prices, the initial developments seem to bode well for ICT competition in Mexico. In January 2015, U.S.-based carrier AT&T closed a $2.5 billion deal with Grupo Salinas for the purchase of Iusacell, the third largest Mexican carrier.[29] The move marked the entrance of U.S. companies into the Mexican market and increasing competition for América Móvil. AT&T also purchased Nextel Mexico in a 1.8 billion deal.[30] After the deals, AT&T started to offer plans to Mexican users, including one of 9 GB at a monthly rate of US$100.

Regulatory Bodies

In 2013, the government established a new autonomous regulatory apparatus known as the Federal Telecommunications Institute (IFETEL) as part of a constitutional reform, in order to increase transparency of media regulation.[31] IFETEL has the legal mandate to act as an antitrust body, protecting the industry against monopolistic practices.

After secondary legislation was approved in July 2014, IFETEL began acting on its mandate to unilaterally punish non-competitive practices through the withdrawal of corporations' licenses, the application of asymmetric regulation, and the unbundling of media services.[32] The most notable step taken by IFETEL was the declaration that América Móvil and Televisa were dominant companies. This action indicates positive changes in Mexico's telecommunications market, especially if IFETEL can continue to remain independent from political and corporate interests.

Limits on Content

While harassment and physical violence has encouraged a climate of self-censorship among journalists and online activists, many have continued to risk physical danger in order to write about crime and corruption. In some cases, public officials and private actors have also been accused of exerting pressure to manipulate the media environment, and in March 2016 members of Milenio *newspaper's data unit resigned over allegations of censorship. Meanwhile, the "right to be forgotten" has continued to stir debate following a January 2015 ruling to request the removal of three links from Google's search results, which contained sensitive information about a businessman.*

Blocking and Filtering

No evidence has been documented that the government or other actors blocked or fil ered internet

28 Federal Telecommunications Institute (IFETEL), Cuarto Informe Trimestral Estadístico 2015 [Fourth quarterly statistical report 2015], March 2016, http://bit.ly/2e0q6A8.

29 Roger Cheng, "Done deal: AT&T closes $2.5 billion purchase of Mexico's Iusacell," January 16, 2015, http://cnet.co/1sHfJp3.

30 Noticias Iusacell, AT&T acuerda la compra de Nextel Mexico, January 26, 2015, http://bit.ly/1RH6SOH.

31 Juan Montes, "Mexico Telecoms Reform Bill Advances," *The Wall Street Journal,* March 22, 2013, http://on.wsj.com/1LXSc6E

32 Víctor Pavón-Villamayor, "Ifetel, la mayor apuesta en telecomunicaciones," [Ifetel, The Biggest Bet in Telecommunications] *Forbes México*, April 25, 2013, http://bit.ly/1JyL0Mr; See also: Juan Montes, "Mexico Telecoms Reform Bill Advances," *The Wall Street Journal,* March 22, 2013, http://on.wsj.com/1LXSc6E/.

and other ICT content. Facebook, Twitter, YouTube, and international blog-hosting services are freely available in Mexico and have enjoyed steady growth in recent years.

Content Removal

The Mexican government does not systematically request the removal of online content from intermediaries, news sites, and hosting services. Facebook did not register any content removal requests for 2015,[33] and Twitter registered two removal requests in the first half of 2016, but no requests in the second half of 2015.[34] Although there is no strong legislative framework on intermediary liability, existing legislation offers some protections from liability for ISPs in cases of copyright infringement.[35] A crucial ruling from the Federal Institute of Access to Information and Personal Data Protection (IFAI) in January 2015,[36] however, threatened to introduce greater liability for search engines if they did not comply with requests to remove sensitive personal information from their search results.

Digital rights advocates have challenged the data protection authority's decision, which ruled in favor of a request to remove links from Google search results under threat of sanction.[37] Carlos Sánchez de la Peña, a businessman whose family had extensive dealings in the transport sector, had requested the removal of three links which included criticisms of his family's business dealings, on the grounds that they constituted an affront to his honor and privacy.[38] After Google Mexico dismissed the request on jurisdictional grounds, Sánchez petitioned IFAI to force Google Mexico to remove the links. Following in the footsteps of several so-called "right to be forgotten" cases, IFAI's decision argued that individuals had the right to demand that the search engine remove search results that might violate their privacy.

Civil society groups expressed serious concern that the ruling could set a precedent for intermediary liability and censorship. Although Sánchez characterized the links as defamatory and a violation of his personal privacy, civil society groups have argued that the links—which included a journalistic investigation in the media outlet *Revista Fortuna* about fraud—had public interest value.[39] Both Google Mexico and *Revista Fortuna*—the latter represented by the digital rights group R3D (Digital Rights Defense Network)—have challenged the resolution. While a district court denied R3D's request in February 2016, a tribunal later overturned this decision in August in favor of *Revista Fortuna's* right to be heard.[40] This latest ruling rescinded the 2015 ruling and discontinued Google Mexico's case against INAI, opening way for a new procedure on the matter.[41]

33 Facebook, "Mexico," *Government Request Report,* accessed September 2016, http://bit.ly/2ddCj4e.

34 Twitter, "Mexico," *Transparency Report*, accessed September 2016, http://bit.ly/2dAvaNI.

35 Jose Camarena, "WILMAP: MEXICO," The Center for Internet and Society, Stanford Law School, http://stanford.io/1MV98kd.

36 This was the name of the institute at the time of the ruling. However, in May 2015, the institute changed its name to the National Institute of Transparency, Access to Information, and Personal Data Protection (INAI).

37 La Razón, "Google litiga contra el IFAI por el derecho al olvido" [Google challenges IFAI over right to be forgotten], March 21, 2015, http://bit.ly/1JOkoJz

38 Lauren Iliff, "Google Wages Free-Speech Fight in Mexico, *The Wall Street Journal*, May 27, 2015, http://on.wsj.com/1J0MdS1.

39 Animal Político, "Fallo del IFAI contra Google abre puerta para que cualquiera censure contenidos en Internet," *Vanguardia*, January 30, 2015, http://bit.ly/1PJNUDi.

40 This decision occurred outside the period covered by this report. See: "¡Ganamos! Tribunal anula resolución del INAI sobre el falso «derecho al olvido»" [We won! Tribunal annuls INAI resolution on false "right to be forgotten"], August 24, 2016, http://bit.ly/2ekBFpe; and Manu Ureste, "Derecho al olvido en internet: ¿un derecho, censura o un redituable negocio en México?" [Right to be forgotten on the Internet: a right, censorship, or a profitable business in Mexico?], *Animal Político,* September 13, 2016, http://bit.ly/2cT4QPA.

41 José Soto Galindo, "Fortuna obliga al INAI a discutir sobre Google y los datos personales otra vez," [Fortuna forces INAI to discuss Google and personal data again], *El Economista,* August 25, 2016, http://bit.ly/2dn6F5v.

Media, Diversity, and Content Manipulation

Local officials ha e often been accused of manipulating online content in their favor, or of harassing or otherwise attempting to intimidate journalists to keep them from writing about issues of local corruption and crime.

The climate of violence and harassment towards the media contributes to significant sel -censorship. In some states heavily afflic ed by violence, the local media will simply not report stories about drug trafficking or drug- elated violence. A survey by the MEPI Foundation, a Mexican nonprofit focused on promoting investigative journalism, found that 8 out of 10 respondents residing in high-crime cities said that they knew that local media would not report on crime in their area.[42]

Several cases suggest that public officials also at empted to manipulate media content by exerting pressure on media outlets critical of the government. In March 2016, a reporter at the national newspaper *Milenio* resigned over allegations of government censorship of an investigative piece criticizing the misallocation of resources to fight hunger in ce tain municipalities.[43] Shortly after the article was published online, Rosario Flores Berlanga, secretary of Rural, Urban and Territorial Development (Sedatu), visited *Milenio*'s newsroom to complain about the piece. The article, headlined "The (false) success of the crusade against hunger," was temporarily taken down from the website, and then republished with a new headline that omitted the word "false."[44]

In an earlier case in March 2015, independent radio station MVS terminated a contract with a group of investigative journalists from Aristegui Noticias, ostensibly due to their involvement with the whistleblower website Méxicoleaks.[45] Many critics believe that the real reason for the termination was a reaction to a controversial report Aristegui Noticias published online investigating a luxurious residence in Mexico City owned by President Enrique Peña Nieto's family.[46]

Online trolls have targeted both online and print journalists through Twitter and other social media, and some reports suggest that some government officials or po erful figu es regularly employ commentators or bots to manipulate online debate.[47] Following the disappearance of 43 students from Ayotzinapa in September 2014, spam bots reportedly flooded witter hashtags used by activists to share information and mobilize. The bots also created fake hashtags in attempts to manipulate trending topics linked to critical protests.[48]

Economic constraints influence the di ersity of media in Mexico. Scarce funding and a lack of interest in online advertising create challenges for individuals and nonprofits seeking o establish sustainable online outlets in Mexico. Reliance on public advertising renders independent media vulnerable

42 Fundación MEPI, "Se autocensuran por crimen organizado" [Organized Crime is self-censored] February 3, 2015, http://bit.ly/1iWTqbA.

43 "Renuncia Karen Cota, autora del reportaje de Milenio DataLab censurado por la Sedatu," [Karen Cota, author of Milenio DataLab's report censored by Sedatu, resigns] *Emeequis*, March 16, 2016, http://bit.ly/1MWspTi.

44 "Los números de la cruzada contra el hambre," [The numbers of the crusade against hunger], *Milenio DataLab,* March 7, 2016, accessed on March 21, 2016, http://bit.ly/1R29a67.

45 Elisabeth Malkin, "In Mexico, Firing of Carmen Aristegui Highlights Rising Pressures on News Media," The New York Times, March 27, 2015, http://nyti.ms/1FDE7yz.

46 "La casa blanca de Enrique Peña Nieto (investigación especial)," [The white house of Enrique Peña Nieto (special investigation)] *Aristegui Noticias,* November 9, 2014, http://bit.ly/1xc1FVN.

47 Rise of the Peñabots," *Data & Society: Points*, February 26, 2016, http://bit.ly/2dxA5w8; Alberto Nájar, "¿Cuánto poder tienen los Peñabots, los tuiteros que combaten la crítica en México?," *BBC Mundo*, March 7, 2015, http://bbc.in/1KG9qHX; Erin Gallagher, "Tracking The Mexican Botnet: Connecting the Twitterbots," *Revolution News*, March 18, 2015, http://bit.ly/1FS4CxF.

48 "Pro-Government Twitter Bots Try to Hush Mexican Activists," *Wired,* August 23, 2015, http://bit.ly/2d1IBUV.

to manipulation of content or closure due to lack of funding,[49] although it is the former that appears to be the more pernicious of the two trends. In Puebla, for example, independent media organizations say the state government uses a combination of state, municipal, and university advertising as a way to control the editorial independence of local media.[50]

Despite such challenges, however, financially independent digital media outlets a e appearing in Mexico, creating a new ecosystem of news options. These independent outlets, such as *Paralelo*, an outlet created by freelance and local journalists in Chiapas, bring new voices to the public debate. Another new digital media venture, *Animal Político*, a popular site that claims more than one million followers on Facebook, is successfully experimenting with alternate forms of financing. In o der to raise revenue for the site without compromising content based on advertisers' political leanings, *Animal Político* is practicing brand journalism, offering social media consulting and digital content to private companies. Additional financing is deri ed from syndicated content, private sponsorships, and event organizing.[51] Other digital media outlets have emerged in Mexico City, Puebla, and Oaxaca.[52]

The social media landscape in Mexico is also vibrant. Mexico has the second largest community of Facebook users in Latin America after Brazil—and the fi th largest in the world—with an estimated 45.5 million users, which represents over 95 percent of Mexico's internet users.[53] The number of Twitter users in Mexico has ballooned in recent years, reaching an estimated 21.3 million in 2015.[54]

Articles 145 and 146 of the Telecommunications Law establish protections for net neutrality. However, net neutrality reemerged as a contentious issue ahead of the launch in December 2015 of Free Basics, Facebook's zero-rating platform, on the Virgin Mobile network in Mexico.[55] Zero-rating programs, which are operated by most of the major mobile providers, have generated significant debate.[56] While supporters note that the Free Basics program will introduce provide millions of users with access to important social, health, and political resources on the internet, critics have contended that the program, along with other zero-rating programs, violates net neutrality provisions and fails to provide users with proper data security.[57] According to the Network of Defense of Digital Rights (R3D), Mexican telecommunications companies have started to offer zero-rating programs: Telcel offers free access to Facebook and Twitter. Iusacell and Movistar have similar plans. IFETEL has yet to issue rules on net neutrality and traffic management [58]

49 "México," in *Article VIII, Control estatal de los medios de comunicación* [State control of media], Fundar Centro Análisis e Investigación, on Scribd, May 3, 2015, 57-60, http://bit.ly/1GcRe4F.

50 "México," in *Article VIII, Control estatal de los medios de comunicación*," 60.

51 Tania Lara, "Popular Mexican news site *Animal Politico* seeks to eliminate dependence on government advertising," *Journalism in the Americas Blog*, Knight Center at the University of Texas Austin, April 30, 2013, http://bit.ly/1h44YYW.

52 There are other promising examples of new online news outlets such as: http://www.sinembargo.mx, based in Mexico City; http://ladobe.com.mx, based in Puebla, http://pagina3.mx, based in Oaxaca; http://nodonoticias.com, in Morelos; http://diarioactivo.mx, and http://www.artificialradio.m .

53 "Facebook Dominates the Social Media Market in Mexico," *EMarketer,* April 14, 2016, http://bit.ly/2dpGMV2.

54 "Twitter's User Base in Latin America Continues to Grow," *EMarketer,* May 6, 2016, http://bit.ly/2dxKWpU.

55 Jair López, "Llega a México el internet gratuito de Facebook y Virgin Mobile" [Facebook and Virgin Mobile free internet arrives in Mexico], *El Financiero*, December 10, 2015, http://bit.ly/1Y2raH5.

56 Red en Defensa de los Derechos Digitales, "Neutralidad de la Red en México: Del Dicho Al Hecho" [Net Neutrality in Mexico: From Talk to Deed], accessed October 14, 2016, http://bit.ly/1GQtvre.

57 Milenio Digital, "Internet.org pondría en riesgo la neutralidad de la red, advierten organizaciones," *Tendencia,* May 19, 2015, http://bit.ly/1Kjxqm2.

58 Red en Defensa de los Derechos Digitales, "Neutralidad de la Red en México: Del Dicho Al Hecho" [Net Neutrality in Mexico: From Talk to Deed], accessed October 14, 2016, http://bit.ly/1GQtvre.

Digital Activism

Social media has continued to serve as an important forum for internet users in Mexico. Even in the face of cyberattacks, harassment, and physical violence, users make regular use of social media to provide critical warnings to local communities about dangerous cartel-related situations and to protest instances of corruption and violence by authorities and drug cartels.[59]

In 2016, social media channels were central to raising awareness and mobilizing protests in 27 cities against gender violence, under the umbrella movement #VivasNosQueremos ("We Want to Stay Alive"). More than 6,000 people took to the streets in Mexico City in April 2016 to ask for an end to femicide and gender violence.[60] The hashtag #TodosSomosAyotzinapa continues to be used to criticize the ongoing impunity for human rights violators and the apparent collusion of the state in violence against Mexicans. The hashtag was launched to organize protests against the kidnapping and murder of 43 students from a teaching college in Ayotzinapa, Guerrero on September 26, 2014.[61]

Social media activism succeeded in forcing the government to amend several articles in a draft version of the Telecommunications Law before it was passed in 2014.[62] In 2013, a coalition of NGOs working on the project "Internet Para Todos" (Internet for All) turned to the internet to gather signatures for a petition to lobby the government to recognize internet access as a fundamental right. Due in large part to the success of the coalition, Congress included internet access as a civil right in its 2013 reform of the Mexican Constitution.

Violations of User Rights

Mexico continued to be one of the most hostile environments in the world for online journalists and bloggers, resulting in at least three murders of journalists reporting news online between June 2015 and May 2016. The government has used insecurity as an excuse to increase surveillance. In May 2016, the Supreme Court ruled to uphold data retention mandates and real-time location of mobile devices as outlined in the 2014 Telecommunications Law, after a legal challenge by civil society. The ruling confirmed the need for a judicial warrant to access historical metadata, but not for real-time geolocation.

Legal Environment

The Mexican Constitution guarantees freedom of speech, freedom of the press, and privacy of personal communications. A constitutional reform in 2013 granted the government expanded powers to curtail monopolies in the telecommunications sector (see ICT Market), established internet access

59 Damien Cave, "Mexico Turns to Twitter and Facebook for Information and Survival," *The New York Times*, September 24, 2011, http://nyti.ms/1JySbEA; Miguel Castillo, "Mexico: Citizen Journalism in the Middle of Drug Trafficking Violence" *Global Voices*, May 5, 2010, http://bit.ly/1WtYP8i.

60 "Miles de mujeres protagonizan la mayor marcha por la violencia machista en México," *El País,* April 25, 2016, http://bit.ly/1WlPq3V; See also: "La marcha Vivas Nos Queremos contra las violencia machista en fotos y videos," *Animal Político,* April 24, 2016, http://bit.ly/1XPT2tI.

61 "Protests Mark Seven months Since Ayotzinapa Kidnappings," *PanAm Post*, April 27, 2015, http://bit.ly/1JNis3V.

62 Elizabeth, "#EPNvsInternet: Mass Campaign against Mexican Communications Bill," *Global Voices,* April 21, 2014, http://bit.ly/1P29ODI; William M. Turner, "#EPNvsInternet y el regreso de los jóvenes al activismo en redes sociales," *CNN México,* April 23, 2014, http://cnn.it/1kpJzaa; Mauricio Torres, "10 claves para desenredar el debate sobre la ley de telecomunicaciones," *CNN México,* April 25, 2014, http://cnn.it/1i0C7yM.

as a human right, and guaranteed net neutrality. A Telecommunications Law was subsequently approved in July 2014, but controversial provisions that pose a risk to privacy were largely upheld by the Supreme Court in May 2016 (see Surveillance, Privacy, and Anonymity).[63]

Although defamation was decriminalized at the federal level in 2007, criminal defamation statutes continue to exist in some of Mexico's 32 states.[64] The penal code in Tabasco, for example, establishes penalties ranging from six months to three years of prison for libel. Some halting progress has been made in decriminalizing defamation. In July 2015, the governor of Tlaxcala submitted to the state congress an initiative that would decriminalize defamation.[65] Other provisions at the local level may be equally problematic for journalists, such as Article 333 of the Penal Code in Chihuahua, which criminalizes those who, "for a profit or o cause injury, improperly produce or edit, by any technical means, images, texts or audio, which are totally or partially false or true."[66]

The Law for the Protection of Human Rights Defenders and Journalists was passed in June 2012, establishing the Governmental Mechanism of Protection, an institutional body of government officials and civil society members charged with providing protection for threatened human rights workers and journalists.[67] Among the law's provisions is a requirement that state governments work in conjunction with federal authorities to ensure that protection is effectively extended to those under threat; as of August 2015, 31 states and Mexico City had signed agreements to this effect.[68] While the legislation is promising in that it establishes a legal basis for protection and suggests an end to impunity for attackers, to date, capacity to implement the law has been lacking. In April 2014, the mechanism came under criticism due to delays in processing approximately 57 percent of the 152 time-sensitive requests for protection.[69] A second evaluation made by civil society organizations in July 2015 came the same conclusions, pointing to a lack of funding, lack of coordination between federal and state authorities, and prevalence of impunity in most cases of aggression against a journalist or a human rights defender.[70]

Despite legislation intended to increase the security of journalists and human rights defenders, the government has had little success in deterring attacks on journalists, bloggers, and activists, which are rarely punished in a country that ranks near the top in global surveys on impunity.[71] While the

63 "El Supremo mexicano avala la retención de datos de los usuarios" [Supreme Court ratifies etention of user data], *El País,* May 6, 2016, http://bit.ly/1ryeEk4.

64 Commission on Human Rights, Congress General of the United States of Mexico, *Gaceta Parlamentaria, Número 3757-VIII*, [Parliamentary Gazette, No. 3757-VIII], Thursday April 25, 2013, http://bit.ly/1NXOcYf; See also: Committee to Protect Journalists, Thomson Reuters Foundation and Debevoise & Plimpton LLP, "Mexico" in Critics Are Not Criminals: Comparative Study of Criminal Defamation Laws in the Americas, March 2016, http://tmsnrt.rs/2eAZQiu.

65 Lucía Pérez, "Propone MGZ despenalizar delitos contra el honor," *E-Consulta.com Tlaxcala*, July 19, 2015, http://bit.ly/1h4cCm1.

66 Código Penal del Estado de Chihuahua [Penal Code of the State of Chihuahua], updated June 13, 2016, http://bit.ly/2dcyGhq; See also: Gerardo Cortinas Murra, "Artículo 133," *El Diario*, May 2, 2016, http://bit.ly/2dlFVz6.

67 Leah Danze, "Mexico's Law to Protect Journalists and Human Rights Activists Remains Ineffective," Latin America Working Group, June 30, 2013, http://bit.ly/1LY0MlV.

68 PIB and WOLA, "El mecanismo de protección para personas defensoras de derechos humanos y periodistas en México: desafíos y oportunidades," http://bit.ly/1DNcNwK; See also: Peace Brigades International, "Qué Hacemos," [What we do], April 15, 2015, http://bit.ly/1KOE1kC.

69 Tania L. Montalvo, "Sin atender, 57% de casos del Mecanismo para la Protección de Periodistas," [57 Percent of Cases of Mechanism for the Protection of Journalists Unprocessed] *Animal Político*, March 25, 2014, http://bit.ly/1kpqebA.

70 Espacio de OSC, "Mecanismo Federal de Protección a DDHH y periodistas sin respaldo financie o ni voluntad política," propuestacivica.org, July 28, 2015, http://bit.ly/2e7rAIN.

71 Committee to Protect Journalists, "Getting Away with Murder: CPJ's 2015 Global Impunity Index spotlights countries where journalists are slain and killers go free," October 8, 2015, http://bit.ly/1G1HEGQ.

upper echelons of the judiciary are viewed as independent, state-level legal bodies have frequently been accused of ineffectual conduct, biased behavior, and even harassment of online journalists.

Prosecutions and Detentions for Online Activities

There have been few documented cases of individuals detained, prosecuted, or sanctioned by law enforcement agencies on charges related to disseminating or accessing information on the internet. On April 30, 2016, however, an online journalist in Chihuahua State was arrested and spent one night in jail. Gabriel Ortega was accused of publishing false information online with the intention of damaging the public image of Chihuahua's health secretary for an article about how the state's health secretary transferred millions of Mexican pesos to the wife of the current governor.[72] Journalists in Chihuahua have heavily criticized Article 333 of the Penal Code, which criminalizes the publication of "fully or partially false or true" information (See Legal Environment).

Online reporters have also faced harassment and arrest while covering demonstrations and police action, or political events such as electoral processes. More recently during elections in Chihuahua on June 5, 2016, for example, two online reporters were arrested along with a print journalist while they investigated a complaint about vote buying.[73]

Surveillance, Privacy, and Anonymity

In April 2016, a group of 17 national and international organizations called on the Supreme Court to review the constitutionality of articles 189 and 190 of the 2014 Telecommunications Law.[74] One month later, the court ruled largely in favor of the law, upholding data retention mandates and real-time geolocation. On a positive note, it did establish the need for a judicial warrant to access historical metadata, though not for real-time geolocation data.[75] Mexico's constitution requires that any interception of personal communications be accompanied by a judicial warrant.[76] Activists have announced that they will challenge the ruling before the Inter-American System for the protection of human rights, arguing that such provisions contradict international human rights standards, in particular the right to privacy.[77]

The Supreme Court ruling provided some clarification as o which authorities can access said user data, notably the Federal Prosecutor, Federal Police, and the authority directly in charge of applying and coordinating the National Security Law. Civil society groups had argued that vague language

72 Article 19, "Gobierno de Chihuahua utiliza sistema penal para criminalizar a periodista" [Government of Chihuahua uses penal system to criminalize journalist], May 9, 2016, http://bit.ly/2dQ5MSf; "Captura de Gabriel Ortega por denuncia de Pedro Hernández: TSJE" [Gabriel Ortega captured after complaint by Pedro Hernández], *Tiempo,* April 29, 2016, http://bit.ly/2eBhTVu.

73 Periodistas en Riesgo, "Detienen a reporteros que cubrían elecciones," [Journalists covering elections arrested], June 5, 2016, http://bit.ly/2epuhbQ.

74 R3D, "La SCJN debe proteger el derecho a la privacidad ante retención de datos y vigilancia sin controles en #LeyTelecom," [SCJN must protect the right to privacy facing uncontrolled data retention and surveillance in Telecom Law], April 14, 2016, http://bit.ly/26b90ED.

75 Supreme Court of Justice of the Nation (SCJN), "inviolabilidad del contenido de las comunicaciones y de los datos que permitan identificarlas: segunda sala" May 4, 2016, http://bit.ly/23TtOfR.

76 Jeremy Mittman, "Mexico Passes Sweeping New Law on Data Protection," *Privacy Law Blog,* Proskauer Rose LLP, May 11, 2010, http://bit.ly/1FxvTs0.

77 Global Voices, "Suprema Corte en México valida retención de metadatos y geolocalización de Ley Telecom," [Supreme Court of Mexico validates data retention and geolocation of the Telecom Law], May 6, 2016, http://bit.ly/2d8sicb; R3D, "La SCJN y la #LeyTelecom: Lo malo, lo bueno, lo absurdo y lo que sigue" [The SCJN and Telecom Law: the bad, the good, the absurd, and what comes next], May 5, 2016, http://bit.ly/2fsPDm0.

allowing for data requests by the "appropriate authority" did little to establish parameters for who this authority might be, opening the door for abuse by law enforcements agencies that have been infiltra ed by organized crime.

Article 189 of the law forces telecommunication companies to provide users' geolocation data to police, military, or intelligence agencies in real time. Article 190 similarly forces providers to maintain records of their users' metadata for a period of two years, and grant security agencies access to metadata at any time.[78] For the fi st year, ISPs and mobile providers must save the relevant data in a system that allows the competent authorities to consult the data electronically in real-time, or what some have called "back-door access"; for the following year, the data must be stored in such a way that telecommunications companies can retrieve the data within 48 hours of being notified by authorities.[79]

The Telecommunications Law expanded on and partially replaced previous legislation that increased surveillance and allowed for real-time geolocation. In 2012, Congress passed a bill, known as the "Geolocation Law," which amended existing legislation to allow the Federal Prosecutor (PGR) to obtain the real-time location of a mobile device for a limited list of criminal investigations (for example, kidnapping, extortion, or organized crime). Of the two laws that were amended by the Geolocation Law, one was replaced by the 2014 Telecommunications Law, while the other (the Federal Code on Criminal Procedure), was replaced by the new National Code on Criminal Procedure, which entered into force at the federal level by June 2016. According to the reformed version published on June 17, 2016, the code includes a possibility to retain data in networks, computers or other devices, with a judicial order. Article 303 of that law authorizes geolocation of mobile devices, and expands its application to any investigation. In the reformed version, geolocation would also require a judicial warrant, except for exceptional cases, such as kidnapping investigations, when a person's life or physical integrity is in danger.[80]

Recent reports concerning a vast state surveillance apparatus have further called into question the adequacy of privacy protections. In July 2015, a leak of internal documents from the surveillance company Hacking Team revealed that Mexico was the company's biggest client worldwide, having signed more than 14 contracts with various state and federal agencies. Civil society organizations have argued that these contracts are illegal because many of the agencies involved in the contract lack constitutional or legal authority to conduct surveillance or espionage.[81] The media outlet *Animal Politico* has also accused the state government of Puebla of using Hacking Team products to target the political opposition and journalists, based on the fact that several leaked emails show that the company produced exploits that had subject lines or attachments directly addressed to political figu es.[82]

The leaked information from Hacking Team is only the latest in a series of scandals involving Mexi-

78 Artículo 189-190 de Ley Federal de Telecomunicaciones y Radiodifusión.

79 Artículo 189-190 de Ley Federal de Telecomunicaciones y Radiodifusión.

80 Código Nacional de Procedimientos Penales [National Code on Criminal Procedure], updated June 17, 2016, http://bit.ly/2deCKxz; See also: Luis Fernando Garcia and Jesus Robles Maloof, "La vigilancia y su impacto en el derecho a la privacidad en México," Internet en México, derechos humanos en el entorno digital, Derechos Digitales, March 2016, http://bit.ly/29VzALs.

81 For more information about the revelations of Hacking Team's operations in Mexico see Julio Sánchez Onofre, "Vulneración a Hacking Team confi ma abuso de espionaje en México," [Breach of Hacking Team confi ms abuse of espionage in Mexico] *El Economista,* July 6, 2015, http://bit.ly/1JRDTlA; See also: Daniel Hernandez and Gabriela Gorbea, "Mexico is Hacking Team's Biggest Paying Client -- By Far," *Vice News*, July 7, 2015, http://bit.ly/1LWGbmO.

82 Ernesto Aroche, "El gobierno de Puebla usó el software de Hacking Team para espionaje político," *Animal Politico*, July 22, 2015, http://bit.ly/1TQO7rh.

co's surveillance apparatus. In July 2012, military sources leaked evidence, which was later confi med by the Mexican army, pertaining to the Mexican army's secret purchase of more than MXN 4 billion (more than US $300 million) of spyware engineered to intercept online and mobile phone communications.[83] In addition to recording conversations and gathering text messages, email, internet navigation history, contact lists, and background sound, the surveillance software is also capable of activating the microphone on a user's cell phone in order to eavesdrop on the surrounding environment. In 2013, reports also surfaced that FinFisher software is being used for surveillance in Mexico. Although a group of human rights organizations has called for a federal investigation into the use of espionage and intelligence tools, the government has yet to conduct or submit to any such investigation.[84] In 2006, reports alleged that the United States provided equipment allowing the Mexican government to "intercept, analyze and use intercepted information from all types of communication systems operating in Mexico."[85]

Government requests to social media companies for information regarding users have increased significantly o er the past year. Between January and December 2015, Facebook received 724 requests from the Mexican government for information related to 1,296 users, an increase of 141 percent compared to 2014. In 65 percent of the cases, Facebook released some information.[86] Facebook did not reveal the type of information requested by the government. Between July and December 2015, Google received 159 requests from the Mexican government for user data of 212 users or accounts. The company produced information in 53 percent of such cases.[87]

After a 2008 requirement that cell phone users register with the government was revoked in 2012, there are no longer any official p ovisions regarding anonymity.

Intimidation and Violence

Threats and violence from drug cartels—and occasionally members of local government—have continued to plague online reporters. In 2015, Reporters Without Borders listed Mexico as one of the most dangerous countries in the world for media personnel.[88] According to Periodistas en Riesgo, between June 2015 and May 2016, at least 10 journalists were murdered. Two of these journalists worked exclusively online to report crimes and a third used his Twitter account to report on violence.

On July 2, 2015, authorities found the body of Juan Mendoza Delgado, the director and founder of the local news website *Escribiendo la Verdad* (which translates to "Writing the Truth"). Although authorities claimed that Mendoza had been run over by a car, human rights organizations are investigating to see whether Mendoza's death was related to his writing, which was often highly critical of

83 Ryan Gallagher, "Mexico Turns to Surveillance Technology to Fight Drug War," *Future Tense* (blog), *Slate*, August 3, 2012, http://slate.me/1MBOliq; "Paga Sedena 5 mmdp por equipo para espiar," *El Universal*, July 16, 2012, http://eluni.mx/1L0Otcd.

84 Tania Molina Ramirez, "Sigue activo el programa de espionaje cibernético Finfisher en México: Citizen Lab " [FinFisher Cyber Espionage Program Kept Active in Mexico] *WikiLeaks en La Jornada*, October 7, 2013, http://bit.ly/1MBOzWN.

85 See Beckusen, "U.S. Looks to Re-Up its Mexican Surveillance System," *Wired,* May 1, 2013, http://bit.ly/2deKWhA, Robert Beckhusen, "U.S. Looks to Re-Up its Mexican Surveillance System," *Wired* online, May 1, 2013, http://wrd.cm/1L0OxIM and Katitza Rodriguez and Gabriela Manuli, "Mexicans Need Transparency on Secret Surveillance," Electronic Frontier Foundation, July 24, 2012, http://bit.ly/1YKIttU/.

86 Facebook, "Mexico," in Global Government Requests Report, January-June 2014, http://on.fb.me/18CxvzL; Facebook, "Mexico," in Global Government Requests Report, July-December 2014, http://on.fb.me/18CxvzL. "Mexico," in Global Government Requests Report, January-June 2015, http://bit.ly/2egCAmR; "Mexico," in Global Government Requests Report, July-December 2015, accessed May 17, 2016, http://bit.ly/2ddCj4e.

87 Google, "User Data Requests – Mexico," *Transparency Report,* accessed October 14, 2016, http://bit.ly/2dQwj1I.

88 Reporters Without Borders, *World Press Freedom Index: 2016*, accessed October 14, 2016, https://rsf.org/en/mexico.

local politicians and organized crime.[89] Francisco Pacheco, a print reporter, was also killed on April 24, 2016, after he posted information on Twitter about an armed confrontation of federal police officers with members of a criminal group.[90] On May 14, 2016, Manuel Torres was assassinated with a bullet in his head while he was returning home in Poza Rica, Veracruz. He had a 20-year career as a journalist, and had recently launched his online news outlet, Noticias MT.[91]

2015 was also the first year since 1984 that a murder of an active journalist (photojournalist Rubén Espinosa) took place in Mexico's capital.[92] In August, one week after the killing, Mexico City enacted a law to protect journalists at risk in the city. Organizations such as Reporters without Borders have reacted positively to this move, yet urged the government to allocate the necessary resources to effectively implement it.[93]

Although threats, verbal attacks, and physical attacks that do not lead to death are less likely to make the news, these aggressions are pervasive. Jorge Martínez Castañeda, director of *Rotativo Digital*, an online news organization based in Michoacán, was physically attacked on January 6, 2016 by Manuel García, son of the mayor of Tacambaro. Martínez had published a story about the mayor's involvement in a corruption case. In February 2016, reporters for the weekly political magazine *Proceso* received death threats from online trolls after they criticized the lack of attention of the Mexican government to the murder of Anabel Flores, a female journalist who was kidnapped and assassinated in Veracruz.[94] Lucero Aguilar, a reporter for the weekly magazine *Expresión San Luis*, said she received more than 500 death threats from false Twitter accounts, most of them showing the picture of the elected San Luis Potosi mayor. "Shut your mouth or we are going to dismember you," read one of the threats against Aguilar.[95] More recently, online trolls sent death threats to a journalist after he ran a column on crime and violence in a trendy neighborhood in Mexico City.[96]

This coverage period also saw at least eight incidents of police officers confiscating or destroying cameras or cell phones of reporters covering protests. Karlo Reyes Luna, a photojournalist for *AVC Noticias* and *VozAlterna*, two online news portals in Veracruz, reported aggressions and destruction of equipment by state police officers on September 15, 2015.[97] Reporters who cover human rights abuses are also the victims of robbery or destruction of professional equipment. In early September 2015, unknown people broke into the home of Flor Goche, a reporter for *Desinformemonos*, an independent online news organization, and Elva Mendoza, a *Contralinea* magazine reporter. Aggressors stole computers and documents.

89 Committee to Protect Journalists, "Juan Mendoza Delgado," *Journalists Killed,* June-July 2015, http://bit.ly/1LY3Hek.

90 Periodistas en Riesgo, "Asesinan a reportero en Taxco" [Reporter assassinated in Taxco], April 24, 2016, http://bit.ly/2ehkVKB.

91 Periodistas en Riesgo, "Matan a periodista en Poza Rica, Veracruz" [Journalist killed in Poza Rica, Veracruz], May 16, 2016, http://bit.ly/2deJbAP.

92 Committee to Protect Journalists, "Mexican Journalist who Fled Violent Veracruz State Murdered in Capital," August 3, 2015, https://cpj.org/x/6522.

93 Reporters Without Borders, "DF de Mexico, ¿una ley para proteger periodistas?" [Mexico DF, a law to protect journalists?], August 14, 2015, http://bit.ly/2cD1b2O.

94 Journalists at Risk, "Amenazan por Twitter a reportero de Proceso" [Threats via Twitter to Proceso reporter], February 9, 2016, http://bit.ly/2dm83Gh.

95 Journalists at Risk, "Denuncia periodista amenaza de alcalde electo de SLP" [Journalist denounces threat by SLP mayor], June 8, 2015, http://bit.ly/2cDnDNV.

96 "El Periodista Hector de Mauleon recibe amenazas tras denunciar violencia en la colonia Condesa" [Journalist Hector de Mauleon receives threats after denouncing violence in Condesa], Sin Embargo, September 22, 2016, http://bit.ly/2cVK52d.

97 Journalists at Risk, "Fotoperiodista reporta agresión de policías de Veracruz" [Photojournalist reports police aggression in Veracruz], September 15, 2015, http://bit.ly/2dsSNsN.

Mexican journalists have also suffered aggressions while covering electoral processes. A coalition of civil society organizations working to monitor the federal and local election on June 7, 2015 reported 58 aggressions directly associated with the electoral context. Most of them were threats and six were technical attacks, including four cases of cyberattacks, one hacking of an account, and one alteration of a website.[98] (See "Technical Attacks" for more information)

Spotlight on Marginalized Communities

Freedom on the Net 2016 **asked researchers from India, Indonesia, Kenya, Kyrgyzstan, Jordan, Mexico, Nigeria, and Tunisia to examine threats marginalized groups face online in their countries. Based on their expertize, each researcher highlighted one community suffering discrimination, whether as a result of their religion, gender, sexuality, or disability, that prevents them using the internet freely.**

In Mexico, Oliver Trejo examined online threats against women who use digital media to document sexual harassment.[1] The study found:

- In April 2016, hashtags such as *#NoEsNo* ("no means no") and *#MiPrimerAcoso* ("my fi st harassment") were shared on social networks to protest violence against women. Activists hope that the internet can serve as a tool for reporting incidents of gender-based sexual violence in a country where many victims distrust government institutions. Yet as technological advances have increased internet access and affordability in Mexico, a culture of gender-based discrimination has migrated from the streets to online environments. Derogatory and discriminatory remarks about women are disseminated on news portals, blogs and social networks.
- In a disturbing trend, women who use the internet to publicize offline harassment ha e become the targets of sexualized abuse on social media in ways that could further deter victims from reporting crimes of assault and sexual violence.

1 Oliver Trejo, "*'Viral Hate:' Trolling Victims of Sexual Assault in Mexico,*" research paper, August 2016, on file with F eedom House.

Technical Attacks

Technical attacks are now a central tactic in attempts to suppress freedom of expression, and entities that commit cyberattacks do so with relative impunity. Recently, the ongoing threat of Distributed Denial of Service (DDoS) attacks has led outlets to enlist the help of companies like Deflect, a C - nadian nonprofit o ganization protecting websites of human rights organizations and independent media publications.[99]

Several major cyberattacks against news websites were reported between June 2015 and May 2016. For example, the digital outlet *Letra Roja* was forced offline for se eral hours on March 3, 2016, after it published a report linking government officials in Durango with o ganized crime.[100] More recently, the independent online TV portal Rompevientotv.com was also victim of a DDoS attack that affected the website for several days on July 3, 2016.[101]

98 "Elecciones 2015 y agresiones contra periodistas y el derecho a la libertad de expresión, primeros resultados 7 de Julio de 2015" [2015 elections and aggressions against journalists and the right to freedom of expression. First results, July 7, 2015], Elecciones y agresiones, http://bit.ly/2cDmdDp.

99 Jorge Luis Sierra, "How Technology Keeps Journalists Safe in Latin America," *Media Shift*, May 20, 2015, http://bit.ly/1YKJCIm.

100 Article 19, "Inhabilitan portal de medio tras publicación de reportaje sobre autoridades de Durango" [Media portal disabled after publishing a report], March 8, 2016, http://bit.ly/1P2wE9V.

101 "Rompeviento Tv reanuda transmisiones" [Rompeviento TV renews broadcasting], *Rompeviento Tv,* July 5, 2016, http://bit.ly/2eEcY6o.

Spiking at politically sensitive times, at least three attacks took place on election day in Puebla, which has become a major hub for cyberattacks against independent online media organizations:

- Centronline.mx, based in Puebla, reported at least one major cyberattack on June 7, 2015.[102]
- AVC Noticias, also based in Puebla, reported on its Twitter account a cyberattack against its website on June 7, 2015.[103]
- Diario Cambio de Puebla reported a DDoS attack against its website on June 7, 2015.[104]

102 Journalists at Risk, "Ataque cibernetico a sitio de noticias en Puebla" [Cyberattack against news site in Puebla], June 7, 2015, http://bit.ly/2cD1DOq.

103 Journalists at Risk, "Reportan hackeo al portal de noticias de AVC Noticias" [Hack against news portal of AVC Noticias reported] June 7, 2015, http://bit.ly/2d6m61d.

104 Journalists at Risk, "Diario Cambio denuncia ataque cibernético" [Diario Cambio denounces cyberattack], June 7, 2015, http://bit.ly/2e7rykb.

Freedom House

Morocco

	2015	2016
Internet Freedom Status	Partly Free	Partly Free
Obstacles to Access (0-25)	11	12
Limits on Content (0-35)	9	9
Violations of User Rights (0-40)	23	23
TOTAL* (0-100)	**43**	**44**

* 0=most free, 100=least free

Population:	**34.4 million**
Internet Penetration 2015 (ITU):	**57 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- In January, unlicensed VoIP services were blocked on mobile devices after a decision by the regulator. Some speculated that the actions were motivated by financial conce ns over competition between telecommunications companies and voice-calling services provided by the likes of WhatsApp and Skype (see **Restrictions on Connectivity**).
- Provisions in the new press code—proposed during the coverage period and passed in June 2016—remove jail sentences for journalistic crimes, except in cases when journalists fail to pay fines, which emain steep. The code also mandates the registration of online journalists in a move that may bring them further stifle f ee reporting (see **Legal Environment**).
- News site *Badil* was repeatedly targeted on spurious charges of defaming public officials and publishing false information. El Mehdaoui, its editor, was given a four-month suspended sentence and ordered to pay a hefty fine in June f last year, while in August a court ordered the news site to be shut down for three months, subject to an appeal (see **Prosecutions and Detentions for Online Activities**).
- In June 2015, a court ordered the news site *Goud* to pay over US$ 51,000 in damages to the king's private secretary over an article deemed defamatory. The heavy fine may ankrupt the independent news site (see **Prosecutions and Detentions for Online Activities**).
- Five prominent activists and online journalists face up to fi e years in prison for "threatening the security of the state," while two additional journalists could be fined for eceiving foreign funding without permission. All seven individuals are implicated in a troubling court case that has been repeatedly postponed (see **Prosecutions and Detentions for Online Activities**).
- YouTube footage of a young Moroccan man lifting asphalt barehanded from a local road led to his arrest for allegedly defaming the official esponsible for the poor construction. He was eventually released and acquitted of all charges after a large public outcry (see **Prosecutions and Detentions for Online Activities**).

Introduction

Internet freedom declined in Morocco over the past year due to new restrictions on Voice-over-IP (VoIP), while legal harassment of prominent activists and online journalists continued.

In a new obstacle to greater internet access, Morocco's regulator blocked free voice-calling features provided by apps like WhatsApp, Skype, and Viber, seemingly under pressure from telecommunications providers. Restrictions on VoIP impact the country's entrepreneurs, who depend on VoIP when interacting with clients overseas. Millions of Moroccans will be unable to make cheap or free calls to relatives in the diaspora, many of whom regularly send remittances back home.

Moroccan authorities use nuanced means to limit online content and violate users' rights. For example, while websites are rarely blocked, problematic press and antiterrorism laws place heavy burdens on intermediaries and allow for the shutting down of news sites. The unfair disbursement of advertising money, strict self-censorship, and ongoing trials of prominent journalists have prevented the emergence of a vibrant online media sphere. Nonetheless, digital media remains freer than local television or newspapers, and the government has taken several positive steps in recent years, such as passing a new press code in June 2016—after the coverage period of this report.

But barring reform to other problematic laws, journalists will still find themsel es punished for "defaming" prominent officials by calling out corruption or criticizing go ernment policies. Hamid El Mehdaoui, editor of *Badil*, was involved in three separate court cases for his site's investigative reporting, while the news site *Goud* was ordered to pay over US$ 51,000 for an article on the king's private secretary. In one disturbing case, seven prominent digital activists and online journalists face up to fi e years in prison for peaceful efforts to improve human rights and further public discourse in the country. Their trial has been postponed at least three times, a tactic regularly used by the authorities to avoid international condemnation, while engendering self-censorship at home. This situation is reinforced by the state's use of surveillance technology to further strengthen the atmosphere of fear among online journalists and activists.

Obstacles to Access

While access continues to increase, Morocco's regulator announced a restriction on VoIP services, a decision interpreted as an attempt to protect telecoms companies from competition from voice-calling apps such as WhatsApp, Skype, and Viber. The move will disproportionately impact the country's entrepreneurs and those with family in the diaspora, who rely on these services to avoid the high cost of long-distance calls.

Availability and Ease of Access

Internet access in Morocco has increased steadily in recent years, although obstacles remain in place in certain areas of the country. The internet penetration rate grew from 52 percent in 2010 to 57 percent in 2015, according to the International Telecommunication Union (ITU).[1] Meanwhile, there are 1.27 mobile subscriptions for every individual, indicating high mobile penetration.

1 International Telecommunication Union, "Statistics," 2015, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

Network coverage is highly uneven between urban and rural areas. Telecommunications companies do not abide by the ITU principle of telecommunications as a public service, instead preferring to invest in more lucrative urban areas. According to Morocco's regulator, urban dwellers are more likely to have internet access than rural inhabitants, with penetration at 67 percent versus 43 percent, respectively. Some 55 percent of individuals possessed a smartphone by the end of 2015, up from 38 percent in 2014. Smartphone uptake in rural areas almost doubled from 2014 to 2015, reaching 43 percent of individuals aged of 12-65.[2] Rural inhabitants constitute 39.7 percent of the overall population,[3] and while many have access to electricity, television, and radio, most do not have access to phone lines and high speed internet. The high rate of illiteracy is another obstacle to internet access (43 percent of Moroccans aged 10 and above are illiterate).

The Moroccan government has undertaken several programs over the years aimed at improving the country's ICT sector. Most recently, the *Note d'Orientations Générales 2014-2018* (Guidelines for the Development of the Telecoms Sector 2014-2018) provides the framework for the development of ICTs in the next four years.[4] The program aims to provide fibe -optic and other high speed connections throughout the country, to reinforce the existing regulatory framework and provide universal access.

As a result of previous government efforts, internet use remains relatively affordable. For a 3G or 4G prepaid connection of up to 225 Mbps, customers pay MAD 129 (US$13.2) for initial connectivity fees for the fi st month, and then MAD 5 per day (US$0.51). Internet users pay on average MAD 3 (US$0.31) for one hour of connection in cybercafes.

Restrictions on Connectivity

On January 7, 2016, Morocco's telecommunications regulator, the ANRT, announced the suspension of all Voice-over-Internet-Protocol (VoIP) services over mobile phones.[5] A press release cited Article 2 of the Law n°24-96 governing the post and telecommunications, which stipulates that only licensed telecom operators may offer telephone services to the public. The ANRT also cited a previously unenforced 2004 regulatory decision on VoIP. Many observers indicated the move was intended to protect the revenues of Morocco's telecom companies from competition from apps like WhatsApp, Viber, FaceTime, Facebook Messenger, Skype, and others that provide users with free voice calls.[6] The ban on VoIP will likely have a costly impact on entrepreneurs dealing with overseas clients and Moroccans with family members in the diaspora, who may be forced to turn to costlier services. The blocks may be easily bypassed using virtual private networks (VPNs).[7] Some traced the move back to Emirati carrier Etisalat, which owns a majority stake in Maroc Telecom.[8] VoIP services are also restrict-

2 ANRT Information Technology Observatory, "Survey on ICT access and usage by households and individuals in Morocco, 2015," April 2016, http://bit.ly/2fpGfhB.

3 General Population and Housing Census, "Note sur les premiers résultats du Recensement Général de la Population et de l'Habitat 2014" [News Release on the fi st results of the General Population and Housing Census 2014], news release, accessed February 18, 2016, http://bit.ly/1P9z0pG.

4 ANRT, *Rapport Annuel 2013*.

5 ANRT Press release, accessed 9 February 2016, http://www.anrt.ma/sites/default/files/CP- elephonie-IP-fr.pdf.

6 See "Morocco Blocks VoIP Services to Shore Up Telecom Companies: Oxford Business Group," Moroccan World News, March 4, 2016, http://bit.ly/2fkKUow, and Emmanuel Samoglou, "UAE telecoms companies told to free up internet calling," The National, April 18, 2016, http://bit.ly/22PtSwt.

7 Aline Mayard, "Impact of the VoIP ban in Morocco on the economy and entrepreneurship," January 12, 2016, http://www.wamda.com/2016/01/impact-voip-ban-morocco-on-the-economy-and-entrepreneurship.

8 Stefania Bianchi and Sarmad Khan, "Etisalat Moves West Africa Units to Maroc Telecom It's Acquiring," Bloomberg, May 5, 2014, http://bloom.bg/2eHGwfA.

ed in two of Etisalat's key markets, Egypt and the UAE.[9]

Beyond VoIP, authorities did not impose large scale restrictions on connectivity over the past year. However, the centralization of Morocco's internet backbone facilitates the potential control of content and surveillance. Maroc Telecom owns and controls a fibe -optic backbone of more than 10,000 kilometers (km) covering the country. The national railroad company, Office Nationale des Chemins de Fer (ONCF), and the national electricity and water utility, Office National de l'Electrici é et de l'Eau Potable (ONEE), have also built 2,000 km and 4,000 km fibe -optic infrastructures, respectively. The state owns 30 percent of the shares of Maroc Telecom and controls both the ONCF and ONEE, hence providing it with strong control of the entire internet backbone. Morocco's national and international connectivity has a combined capacity exceeding 10 terabits per second.[10] The three telecom operators (Maroc Telecom, Medi Telecom, and INWI) all have varying access to international connectivity.

ICT Market

Maroc Telecom, Medi Telecom, and INWI are the three internet service providers (ISPs) and mobile phone companies in Morocco. Maroc Telecom (*Ittissalat Al Maghrib*, IAM) is a former state company that held a monopoly over the telecoms sector until 1999.[11] That year, the National Agency for the Regulation of Telecommunications (ANRT) granted licenses for Medi Telecom and INWI. In 2014, Emirati carrier Etisalat purchased a 53 percent stake in Maroc Telecom from Vivendi.[12] Medi Telecom is a private consortium led by Spain's Telefónica, while INWI (formerly WANA, Maroc Connect) is a subsidiary of Ominum North Africa (ONA), the leading Moroccan industrial conglomerate also owned by the royal family. All three companies have submitted applications for 4G mobile phone licenses, following a call for tenders from the ANRT.[13]

Regulatory Bodies

Service providers such as ISPs, cybercafes, and mobile phone companies do not face any major legal, regulatory, or economic obstacles.[14] The ANRT is a government body created in 1998 to regulate and liberalize the telecommunications sector. Its board of directors is made up of government ministers and its head is appointed by the king. The founding law of the ANRT extols the telecommunications sector as a driving force for Morocco's social and economic development, and the agency is meant to create an efficient and trans arent regulatory framework that favors competition among operators.[15] A liberalization of the telecoms sector aims to achieve the long-term goals of increasing GDP, creating jobs, supporting the private sector, and encouraging internet-based businesses,

9 Peter Micek, Deji Olukotun, Al Walid Chennoufi, "Etisalat shuts ff internet services in Egypt and Morocco," Access Now, January 6, 2016, https://www.accessnow.org/etisalat-shuts-off-services-in-egypt-and-morocco/.

10 Natalija Gelvanovska, Michel Rogy, and Carlo Maria Rossotto, *Broadband Networks in the Middle East and North Africa: Accelerating High-Speed Internet Access,* (Washington, D.C.: World Bank, January, 29, 2014), 129, https://openknowledge.worldbank.org/handle/10986/16680.

11 The State owns 30% of Maroc Telecom shares, 53% owned by the Emirate telecoms company Etisalat, and 17% is public. See Maroc Telecom, "Répartition du Capital," accessed February 18, 2016, http://bit.ly/1L9tjET.

12 Stefania Bianchi and Sarmad Khan, "Etisalat Moves West Africa Units to Maroc Telecom It's Acquiring," Bloomberg, May 5, 2014, http://bloom.bg/2eHGwfA.

13 ANRT, "Licences 4G : Dépôt de dossiers de candidature relatifs à l'appel à concurrence," [in French] news release, March 12, 2015, accessed February 18, 2016, http://bit.ly/1YlCHPf.

14 Interviews with Dr. Hamid Harroud and Dr. Tajjedine Rachdi, director and former director of Information Technologies services of Al Akhawayn University in Ifrane, conducted on March 20 and 22, 2015.

15 ANRT, Loi No. 24-96, [in French, Trans.: Laws governing the post and telecommunications] http://bit.ly/1JTMCp6.

among others. While Maroc Telecom, the oldest telecoms provider, effectively controls the telephone cable infrastructure, the ANRT is tasked with settling the prices at which the company's rivals (such as Medi-Telecom and INWI) can access those cables. Thus the ANRT makes sure competition in the telecoms market is fair and leads to affordable services for Moroccan consumers.[16] Some journalists argue that the ANRT is a politicized body lacking independence, due to the fact that its director and administrative board are appointed by a *Dahir* (Royal Decree). However, international organizations such as the World Bank and the ITU have not expressed any major criticism about the ANRT's neutrality.[17]

The allocation of digital resources, such as domain names or IP addresses, is carried out by organizations in a non-discriminatory manner.[18] According to the Network Information Centre, which manages the ".ma" domain, there were 60,060 registered Moroccan domain names in February 2016.[19]

Limits on Content

While websites are rarely blocked, authorities limit online content through a variety of nuanced mechanisms. Problematic press and antiterrorism laws place high burdens on intermediaries and allow for the shutting down of online news sites. In addition, discriminatory allocation of advertising and the repeated prosecution of online news editors impedes the diversification of Morocco's digital landscape.

Blocking and Filtering

The government did not block or fil er any websites over the coverage period. Social media and communication services such as YouTube, Facebook, or Twitter and international blog-hosting services are available in the country. Websites are available which discuss controversial views or minority causes, such as the disputed territory of Western Sahara, the Amazigh minority, or Islamist groups.

The last instance of government blocking of online content dates back to October 2013, when the Attorney General ordered the ANRT to block the Arabic and French-language websites of the investigative news site, *Lakome*. Its Arabic-language editor-in-chief, Ali Anouzla, was arrested one month earlier for citing an article in the Spanish newspaper *El País*, which contained an embedded YouTube video attributed to Al Qaeda in the Islamic Maghreb (AQIM).[20] Activists and observers believe *Lakome* was blocked for its critical stance towards the monarchy. An Arabic-language version of the site has been relaunched using the address lakome2.com.

Content Removal

16 ANRT, Loi No. 24-96, [in French, Trans.: Laws governing the post and telecommunications] http://bit.ly/1JTMCp6.

17 Caroline Simard, "Morocco's ANRT Guidelines Project Related to Fundamental Regulatory Aspects," accessed 18 February 2016, http://bit.ly/1LDbxtG; Björn Wellenius and Carlo Maria Rossotto, "Introducing Telecommunications Competition through a Wireless License: Lessons from Morocco," *Public Policy for the Private Sector,* (1999), accessed February 18, 2016, http://bit.ly/1KvpIq8.

18 Network Information Centre, the service that manages the domain .ma, is owned by Maroc Telecom. There are calls for domain.ma to be managed by an independent entity, not a commercial telecoms company.

19 This service is owned by Maroc Telecom. Network Information Centre, accessed February 18, 2016, http://www.registre.ma/?page_id=71.

20 The video entitled, "Morocco: Kingdom of Corruption and Despotism," incites viewers to commit terrorism acts against the country: Amnesty International, "Morocco/Western Sahara," *Amnesty International Report 2014/15,* http://bit.ly/1EFAvfa.

While the government does not block online content, it maintains control over the information landscape through a series of restrictive laws that can require the shutting down of publications and removal of online content. For example, a court ordered the news site Badil to be shut down in August 2015, although the decision was appealed (see "Prosecutions and Detentions for Online Activities"). Under the press law, the government has the right to shut down any publication "prejudicial to Islam, the monarchy, territorial integrity, or public order," and it maintains prison sentences and heavy fines for the publication of offensive content (see "Legal Environment").

In addition, the antiterrorism law[21] gives the government sweeping legal powers to fil er and delete content that is deemed to "disrupt public order by intimidation, force, violence, fear or terror."[22] Article 218-6 assigns legal liability to the author and anybody who in any way helps the author to disseminate an apology for acts of terrorism, a provision which would include site owners and ISPs. Intermediaries must block or delete infringing content when made aware of it or upon receipt of a court order.[23] While the law was ostensibly designed to combat terrorism, authorities retain the right to define ague terms such as "national security" and "public order" as they please, thus opening the door for abuse. Many opposition news websites are hosted on servers outside of the country to avoid being shut down by the authorities.

The government also resorts to more ad hoc, extralegal means to remove content deemed controversial or undesirable. For example, *Hespress*, which in the past featured content both supportive and critical of the government, has deleted videos of street protests and interviews with opposition figu es from the site out of fear or pressure from authorities.[24]

Media, Diversity, and Content Manipulation

Due to self-censorship on key political topics, the Moroccan online media landscape lacks diversity and investigative journalism. In the words of Aboubakr Jamai, "the carrot in Morocco is bigger than the stick, the state would rather reward you for obedience than punish you for dissent. So many otherwise good journalists prefer the financial ewards than the risky duties of watchdogs."[25] Online news outlets receive unofficial di ectives not to report on controversial issues, or not to allow certain voices to be heard. In a state that punishes investigative reporting and whistleblowing, people with sensitive information tend to stay quiet to avoid possible retribution. Debates on issues related to the monarchy do not make news, both in traditional and online media. For example, the release of Prince Hicham's "explosive"[26] book, *Journal d'un Prince Banni* [Diary of a Banished Prince] in April

21 The Anti-Terrorism law, passed in 2003 after the 2003 terrorist attacks in Casablanca. On 16 May 2003, Morocco was subject to the deadliest terrorist attacks in the country's history. Five explosions occurred within thirty minutes of each other, killing 43 people and injuring more than 100 in suicide bomb attacks in Morocco's largest city, Casablanca. Morocco has been a staunch ally of the U.S. The 14 suicide bombers all originated from a poor suburban neighborhood in the outskirts of Casablanca.

22 OpenNet Initiative, *Internet Filtering in Morocco*, (2009) http://bit.ly/18GiHgW.

23 Loi nº 03-03, Anti-terrorism law, available at, https://www.unodc.org/tldb/showDocument.do?lng=fr&documentUid=1840&country=MOR, accessed February 18, 2016.

24 Interviews with Driss Ksikess, a well-known journalist and former editor in chief of Nichane and Reda Benotmane, a prominent activist and founding member of Freedom Now, conducted on April 2-3 2015.

25 Interview with Aboubakr Jamai, conducted on February 19 2016.

26 Sara Daniel, "INFO OBS. Maroc : les mémoires du 'prince rouge, " *L'OBS/Monde*, December 10, 2013, accessed April 3, 2015, http://bit.ly/1JTBiZV.

2014[27] surprisingly did not trigger any discussion or reaction in the country, which many observers link to self-censorship and fear of reprisals.[28]

The existing atmosphere of fear among journalists online was strengthened with the arrest of Anouzla and the ensuing blocking of *Lakome*.[29] Given Anouzla's reputation for independence, nonviolence, and pushing boundaries, many saw the charges of "advocacy of acts amounting to terrorism offenses" and "providing assistance to perpetrators or accomplices of acts of terrorism" as a clear attempt to silence a dissenting voice.[30] Many online and offline news outlets loo ed up to *Lakome* for maintaining a high ceiling for freedom of expression, especially in matters related to the monarchy, wherein most political power is concentrated.[31]

Compounding self-censorship and fear are the personal attacks and derogatory comments received by activists and opinion makers online for openly criticizing government policies.[32] Numerous accounts are created on Twitter and Facebook with the sole purpose of harassing, intimidating, and threatening activists. Activists believe that these progovernment commentators are also equipped with direct or indirect access to surveillance tools, since they have often obtained private and personal information on other users.[33] There is no clear indication regarding the identity behind the accounts and whether they are state-sponsored or simply overzealous private individuals. However, due to the amount of time and energy needed to engage in such activity, and the access they have to private information, there are serious doubts that these are private citizens acting on the basis of their own personal resolve.

The government also uses financial p essure to push the most outspoken print media publications into closure or bankruptcy. Advertising revenue provided by the government or government-linked companies is not split fairly between independent and progovernment publications.[34] In addition to state-run and opposition news outlets, the Moroccan media contains a variety of "shadow publications," nominally independent but editorially supportive of the state.[35] The news outlets exist primarily to divert airtime from more serious and engaging news portals and to compete over online advertising money and audience share. There is no evidence linking these publications to a larger state strategy to counter the growth of voices of dissent. However, these shadow publications receive large amounts of advertising, possibly in return for their progovernment bias. Powerful business entities, such as the three telecommunication companies, are known to adhere to state pressure to withdraw advertising money from news outlets that run counter to the state-owned media narra-

27 First cousin of King Mohammed VI and third in the line of succession to the throne, Prince Moulay Hicham gained the nickname "Red Prince" because of his pro-democracy positions and his calls for reforms of the monarchy. The book is an account of a member of the royal family who expressed his views on the political system in Morocco, and called for the reform of the Mekhzen and the institution of the monarchy.

28 Interviews with digital activists and online journalists.

29 Interviews with digital activists and online journalists.

30 Interview with Aboubakr Jamai.

31 Interview with Ali Anouzla.

32 Interview with Ali Anouzla.

33 Interview with Zineb Belmkaddem.

34 Interview with Driss Ksikess.

35 Interview with Driss Ksikess.

tive.[36] In a recent example of this, the Office Chérifien des Phosph es (OCP) and Caisse de Dépôt et de Gestion (CDG),[37] two state-owned companies that do not offer any particular products to Moroccan consumers, are now buying advertising time and space. This move is meant to obtain positive media coverage, avoid negative publicity, and secure media outlets for their press releases.

The state, however, does not limit the ability of online media to accept advertising or investment from foreign sources, which is crucial for maintaining a profitable business and ensuring that citizens can access a range of different opinions and news sources. In addition, webhosting and free blogging services are freely accessible. ISPs are not known to limit bandwidth availability to discriminate on the basis of content.

The most remarkable change in internet use among Moroccans continues to be the growing interest in social media and user-generated content, as well as domestic news portals. In 2010, the top ten most visited websites did not include any Moroccan news websites.[38] By 2015, three online news portals made it to top 10 most visited site, with *Hespress* remaining as the most popular website in Morocco with an estimated 600,000 unique visitors per day. It is ranked fourth after Google, Facebook, and YouTube. *Chouftv*, and *Hibapress* are now ranked sixth and seventh, respectively. The Moroccan classified ads si e *avito.ma*, is ranked fi th and Moroccan sports site *Elbotola* is ranked 11th, bypassing the pan-Arabic sports website Kooora which ranked top ten in previous years.[39]

Digital Activism

Internet users take advantage of various social media tools to educate, organize, and mobilize people around a wide variety of issues. One recent instance of online activism consisted of a campaign to criticize the country's three telecommunication companies after ANRT blocked VoIP from mobile devices. Starting in February, campaigners used hashtags like #OpeUnlike, #OpUnlike, and #voileip to call on users to unlike the social media pages of the three companies.[40] The campaign estimated that each unlike equates to a loss of 3 MAD (0.30 USD) for the companies. According to Hamza Badih, a digital activist, the campaign started off as a grassroots movement within a small community of technology activists, whose leadership was instrumental in engaging a large number of internet users. He added that a monitoring website was created to track the number "unlikes," updated every 10 seconds.[41] The site went viral. According to the website, the "unlike" campaign resulted in the loss of 550,000 likes for the three telecom operators in just over a week. However, according to Badih, the telecoms managed to limit the damage by purchasing "likes" from e-marketing companies.[42] Users also used satire to mock the company slogans of the three telecoms. Nonetheless, the campaign

36 According to *The Report: Emerging Morocco 2013* by Oxford Business Group, Maroc Telecom, Medi Telecom, and Inwi (formerly WANA Corporate) spent three times more the amount of the second sector in terms of advertising with 1.3 bn MAD (£115.6 M). In 2011, according to l'Economiste.ma, telecommunications advertising spending represents 23% of the total advertising market share. See:
"Investissements publicitaires la télé en perte de marché," *L'Economiste,* November 30, 2011, accessed February 18, 2016, http://bit.ly/1KvtrE9.

37 The OCP is the world's largest exporter of phosphate and its derivatives. The CDG is a state institution in charge of collecting and managing specific sta e funds and savings.

38 Bouziane Zaid and Mohamed Ibahrine, *Mapping Digital Media: Morocco*, Open Society Foundations, June 2011, accessed February 18, 2016, http://osf.to/1VCMRJ5.

39 Google, Facebook, YouTube, Hespress, and Google Morocco were the fi e most visited sites in 2014. See, Alexa, "Top Sites in Morocco," accessed February 18, 2016, http://www.alexa.com/topsites/countries/MA.

40 http://unlikes.oudy.works/?ref=red

41 http://unlikes.oudy.works/?ref=red

42 Interview with Badih conducted on 3 March 2016.

was ultimately unsuccessful as the minister of industry, commerce, investment and digital economy endorsed the decision to block VoIP by issuing decree N° 2.16.347. The decree framed the issue around the question of fair competition and endowed ANRT with the prerogative to put an end to all unfair competition practices.[43]

Violations of User Rights

Moroccan laws on criminal defamation and antiterrorism continue to pose a threat to free speech. A new press code containing several positive elements under consideration during the coverage period and eventually passed in June. While the law eliminates jail time for the press, it includes steep fines and mandates the registration of online journalists, in a move that could bring them further under the authorities' control. Furthermore, well known activists and journalists face intimidation through repeated prosecutions and never-ending trials.

Legal Environment

The Moroccan constitution contains provisions designed to protect freedom of expression, but in practice these principles are not defended by the judiciary. According to the 2011 constitution, passed by referendum to curtail public protests at the onset of the Arab Spring, all Moroccan citizens are equals before the law and Article 25 guarantees all citizens "freedom of opinion and expression in all its forms."[44] Although the constitution strengthened the judiciary as a separate branch of government, the judicial system in Morocco is far from independent. The king chairs the High Council of Judicial Power and appoints its members. As such, the courts often fail to produce fair and balanced rulings, frequently basing their decisions on recommendations from security forces.[45]

Moroccan users may be punished for their online activities under the penal code, the antiterrorism law, and the press code. Article 218-2 of the antiterrorism law proscribes prison terms of two to six years and fines f MAD 10,000 to 200,000 (US$ 1,000 to 20,000) for those convicted of condoning acts of terrorism, through offline as ell as online speech.[46]

A new press code passed in June 2016 received mixed reactions among free speech activists.[47] Unlike the previous press code from 2002, the new code contains provisions that specifically apply o online media.[48] Most significantl , the code eliminated jail sentences for journalists and replaced penalties with steep fines. A ticles 76 and 77 of the new code put forward fines f up to MAD 200,000 (US$20,000) for publication of what can be seen as offensive content about the monarchy, Islam, and territorial integrity. These fines a e largely unaffordable for Moroccan journalists, who may be impris-

43 Reda Zaireg, "Blocking of VoIP in Morocco," *Huffington Post*, June 7, 2016, http://www.huffpostmaghreb.com/2016/06/07/blocage-voip-maroc-decret_n_10332766.html.

44 Constitution of Morocco, Art. 25, adopted in 1962, reformed in 2011, accessed January 18, 2014, http://bit.ly/1M04kt8.

45 Mohamed Madani, Driss Maghraoui, and Saloua Serhouni, *The 2011 Moroccan Constitution: A Critical Analysis*, (Stockholm, Sweden: International Institute for Democracy and Electoral Assistance, 2012).

46 Loi n° 03-03, Anti-terrorism law, available at, https://www.unodc.org/tldb/showDocument.do?lng=fr&documentUid=1840&country=MOR, accessed October 6, 2015.

47 Yasmine el-Rifae, "Mission Journal: Morocco's new press law undermined by draft penal code," Committee to Protect Journalists, July 29, 2016, https://www.cpj.org/blog/2016/07/mission-journal-moroccos-new-press-law-undermined-.php.

48 Approbation à l'unanimité par la Chambre des représentants du projet de loi n° 88-13 relatif à la presse et à l'édition , accessed 8 August 2016, http://mincom.gov.ma/media/k2/attachments/ApprobationZZl.pdf.

oned for failure to pay.[49] Most importantly, pending reform of the penal code, journalists may still be jailed for offences against the monarchy or threats to national security, which has occurred in the past.

In a move likely to stifle online media, A ticles 34 and 35 stipulate that online news portals must register their domain names in Morocco to be able to obtain press cards and benefit f om state support. News portals must also obtain three types of authorizations from three different bodies, valid for one year at a time: from the High Authority of Audiovisual Communication (HACA)[50] to post online videos, from the Moroccan Cinema Center (CCM)[51] to shoot film, and f om the ANRT to host domain names under press.ma.[52] These organizations are state-controlled and can easily be influenced o deny authorizations or reject renewals for political purposes. These measures will likely maintain the culture of prior restraint and fortify self-censorship among media workers.

Prosecutions and Detentions for Online Activities

Moroccans continue to face the possibility of unjust arrest and prosecution for their online activities, particularly for material that is seen as critical of state officials. Cou t cases against journalists are often postponed so that the government can avoid international condemnation while maintaining the threat of prosecution.

Over the coverage period, a group of seven prominent online journalists and activists were pursued on serious charges. Maria Moukrim (editor-in-chief of Febrayer.com) and Rachid Tarik (member of the Moroccan Association of Investigative Journalism, AMJI) face fines for " eceiving foreign funding without notifying the General Secretariat of the government," while following fi e individuals face a possible fi e-year prison term for "threatening the internal security of the state."[53] They are:

- Maati Monjib (university professor and president of Freedom Now),
- Samad Ayach (online journalist and member of Freedom Now),
- Hicham El Mansouri (AMJI member),
- Hicham Al Miraat (former advocacy director for Global Voices and former head of the Digital Rights Association, ADN), and
- Mohamed Essabeur (head of the Moroccan Education and Youth Association, AMEJ).[54]

49 Interview with Reda Benotmane, a prominent activist and founding member of Freedom Now, conducted on April 2-3 2015.

50 The High Authority for Audiovisual Communication (*Haut Autorité de la Communication Audiovisuelle*, HACA) was created in 2002 and mandated to establish the legal framework for liberalizing the audiovisual sector, and to oversee a public service broadcasting (PSB) sector.

51 *Le Centre Cinématographique Marocain* (CCM) is in charge of the organization and promotion of the film indust y in Morocco and it oversees the application of the legislation and regulation of the sector.

52 Bouziane Zaid, New press code in morocco to still send journalists behind bars, available at, http://www.mediapowermonitor.com/content/new-press-code-morocco-still-send-journalists-behind-bars, (accessed 3 March 2016).

53 Reporters without Borders, "RSF urges authorities to abandon trial against fi e journalists", available online at: http://en.rsf.org/maroc-rsf-urges-authorities-to-abandon-26-01-2016,48772.html, (accessed 16 February 2016).

54 Editorial board, "Free speech goes on trial in Morocco," *the Washington Post, November 20, 2015,* http://wapo.st/1MZNUvT.

After an initial court date was set for November 19, 2015 in Rabat, it has been repeatedly postponed to March 29, June 29, and as of the time of writing, October 26, 2016.[55]

The charges seem related to a June 2015 training session run by Dutch nongovernmental organization Free Press Unlimited and AMEJ in the city of Marrakesh.[56] According to Free Press Unlimited, plain-clothed police office s raided the session and confisca ed all participants' smartphones, later transferring them to a police office in Casablanca. As f mid-2016 they had not been returned to their owners.[57]

Hamid El Mehdaoui, editor of the news website *Badil*, has faced repeated prosecution over the coverage period for his site's reporting:

- El Mehdaoui was convicted in June 2015 of criminal defamation after a complaint by the general directorate of national security over a story on the 2014 death of activist Karim Lachqar while in police custody. He was given a four-month suspended sentence and, together with the source of the story, ordered to pay a combined fine f MAD 100,000 (US $10,000) by a Casablanca court.[58]

- In August 2015, a court in the city of Meknes ordered *Badil* to be shut down for three months and sentenced El Mehdaoui to a fine f 30,000 MAD (US$ 3,000) over criminal defamation charges related to a story about a car bombing in the city. The judicial proceedings were initiated by the regional governor, who claimed that the story was factually false and that no car bombing occurred or was attempted.[59] El Mehdaoui's lawyer appealed the decision and a new court hearing had not yet been determined. The website remained operational despite the initial court decision.[60]

- In yet another court case, on June 20, 2016, a district court in Casablanca convicted El Mehdaoui of criminal defamation over a report on the minister of justice's travel expenses. He was given a four month suspended sentence and a fine f MAD 10,000 (US$ 1,000).[61]

Journalist Ali Anouzla is once again facing prosecution after an interview he gave to German newspaper *Bild* in November 2015. Due to an apparent mistake in translation, which the newspaper corrected, Anouzla was charged with "endangering the Kingdom's territorial integrity," a severe charge that may result in fi e years in jail. Anouzla's reference to the "Sahara" was translated as "occupied Western Sahara."[62] He was eventually acquitted of charges on May 24, 2016 after repeated post-

55 Telquel, "Un député français juge « inquiétant » le procès de Mâati Monjib et de six activists," June 30, 2016, http://bit.ly/2ewqvf9.

56 "Smart phones confisca ed. Moroccan authorities remain silent," Free Press Unlimited, July 9, 2015, https://freepressunlimited.org/en/news/smart-phones-confisca ed-moroccan-authorities-remain-silent.

57 "Ruth Kronenburg, "Freedom of expression should not be on trial," Free Press Unlimited, June 23, 2016, https://freepressunlimited.org/en/news/freedom-of-expression-should-not-be-on-trial.

58 Committee to Protect Journalists, "Morocco editor, source convicted in defamation case," June 30, 2015, https://cpj.org/x/64c3.

59 Soufiane Sbiti, "La justice fe me le site électronique Badil.info pour trois mois," Telquel, August 11, 2015, http://telquel.ma/2015/08/11/justice-ferme-site-electronique-trois-mois_1459204.

60 Interview with Hamid El Mehdaoui

61 "Le journaliste Hamid El Mahdaoui condamné à 4 mois de prison avec sursis," *Telquel, June 21, 2016,* http://telquel.ma/2016/06/21/le-journaliste-hamid-el-mahdaoui-condamne-a-4-mois-de-prison-avec-sursis_1503008.

62 Reporters Without Borders, "RSF demands immediate withdrawal of new charges against editor", available online at, https://en.rsf.org/morocco-rsf-demands-immediate-withdrawal-09-02-2016,48823.html, (accessed 16 February 2016).

ponements of court hearings.[63] Anouzla continues to face charges of "advocacy of acts amounting to terrorism offenses" and "providing assistance to perpetrators or accomplices of acts of terrorism" after his arrest in September 2013. Anouzla is the editor-in-chief of the Arabic-language version of *Lakome*, a news site, who was targeted for an article he had written on jihadist threats to Morocco in which he provided a link to a Spanish site, which in turn had embedded a jihadist video. He was released on bail on October 25, 2013 and his trial has been continually postponed.[64]

In June 2015, a Casablanca court ordered the news site *Goud* to pay MAD 500,000 (US$52,000) for civil defamation charges, a steep fine which may ankrupt the independent news site.[65] *Goud* was targeted for an article that accused the king's private secretary, Mounir El-Majidi, of corruption. As of July 2016, the ruling was under appeal by the site's managers.[66]

Abderrahman El Makraoui, a young man from the municipality of Jemaat Sehim near the coastal city of Safi, was ar ested over a YouTube video[67] uploaded on January 18, 2016, in which he denounced the shoddy conditions of a newly paved road and removed chunks of pavement with his bare hands.[68] The president of the municipality sued him for defamation, resulting in a public outcry by Moroccans and a solidarity campaign using the hashtag #Iam_Abderhmane. The justice minister subsequently sent a letter to the public prosecutor to release him on bail, and Makraoui was released on February 8. A Safi district cou t acquitted him of all charges on March 9, 2016.[69]

Authorities have also used trumped up charges of drug possession, adultery, and other crimes to intimidate well known activists and journalists and to tarnish their public image. Hicham El Mansouri, a journalist and a member of the Moroccan Association of Investigative Journalism, served a 10-month jail sentence from March 2015 to January 2016 on a trumped-up adultery charge.[70] Many international human rights organizations called for his release in a statement on April 2015 and condemned the trial's irregularities.[71]

Surveillance, Privacy, and Anonymity

Given the absence of blocking and fil ering, Moroccan activists identified su veillance as the most dangerous instrument in the hands the regime.[72] The awareness of being systematically monitored impacts the way activists perceive the risks they take and the margin of freedom they have. Hisham Almiraat, co-founder of the website Mamfakinch and one of the leaders of the February 20th

63 "Ali Anouzla innocenté dans l'affaire des déclarations sur le Sahara," *Telquel, May 26, 2016,* http://telquel.ma/2016/05/26/ali-anouzla-innocente-affaire-declarations-sahara_1498856.

64 Reporters Without Borders, "Human rights organizations call for charges against journalist Ali Anouzla to be dropped," February 18, 2014, accessed March 23, 2015, http://en.rsf.org/morocco-human-rights-organizations-call-18-02-2014,45889.html.

65 Committee to Protect Journalists, "Moroccan editor, source convicted in defamation case," June 30, 2015, accessed August 5, 2015, https://cpj.org/x/64c3.

66 Yasmin El Rifae, "Mission Journal: Morocco's new press law undermined by draft penal code," Committee to Protect Journalists, July 29, 2016, https://www.cpj.org/blog/2016/07/mission-journal-moroccos-new-press-law-undermined-.php.

67 See https://www.youtube.com/watch?v=rzFGM4pZbBQ.

68 Huffpostmaghreb, Libéré, « Abderrahman accueilli en héros après avoir dénoncé le mauvais état des routes, http://www.huffpostmaghreb.com/2016/02/09/abderrahman-el-makraoui-safi-ma oc_n_9195154.html, (accessed 16 Feb 2016).

69 "Moroccan man arrested after denouncing corruption released," Moroccan World News, March 10, 2016, https://www.moroccoworldnews.com/2016/03/181787/moroccan-man-arrested-for-denouncing-corruption-released/.

70 http://www.huffing onpost.com/entry/moroccan-journalist-is-released-after-10-months-in-prison_us_569d03a9e4b0b4eb759f1682

71 Committee to Protect Journalists, "Morocco jails press freedom advocate Hicham Mansour, April 7, 2015, https://cpj.org/2015/04/morocco-jails-press-freedom-advocate-hicham-mansou.php.

72 Interview with Zineb Belmkaddem.

Movement, explained that the state's capacity to own and reconstruct one's personal story, based on surveillance and monitoring, allows authorities to "assassinate your character and use your own information to hurt you."[73] According to Zineb Belmkaddem, "surveillance entails the stealing of data and data is private property… it's like the state coming to my home every day to steal my belongings." Reports and interviews have revealed the use of malware products from Italian company Hacking Team to target activists.[74] Activists have demanded that the state be more transparent about who conducts surveillance, who is targeted, and to what end.[75] Instead, authorities have responded by targeting those same activists who voice their concerns. After the publication of interviews and investigations into surveillance practices in Morocco by Privacy International and Morocco's Digital Rights Association (ADN), the interior ministry announced that a criminal complaint had been filed against "persons who distributed a report containing grave accusations about spying practices." [76]

Beyond these concerns, online anonymity is broadly respected. Internet users do not need to register or provide any kind of identification at cybe cafes. There are no indications that the purchase and use of encryption software by private citizens or companies is restricted.[77] However, free access to the technology is starting to change. In the past, pre-paid SIM cards were purchased anonymously and citizens could get them from the three telecom companies' retail stores without having to show identification. oday, customers are asked for a copy of their ID. However, street vendors and other non-affilia ed sales outlets continue to provide SIM cards without IDs.

Intimidation and Violence

There were no incidents of violence against users for their online activities, but harassment and extralegal intimidation remain a high concern in the country. Ali Lmrabet was denied paperwork necessary to renew his passport, residency, and work papers in mid-2015. In April 2015, with the expiration of a ten-year ban from publishing, he unsuccessfully attempted to restart his satirical news site *DemainOnline*. He subsequently went on hunger strike in front of the United Nations building in Geneva until the interior minister indicated he could receive his new passport.[78] On September 2015, Lmrabet received his passport and residency papers at the Moroccan general consulate in Barcelona.[79]

Technical Attacks

In addition to surveillance and malware attacks, online news portals that express dissenting voices are subject to continuous cyberattacks.[80] Reports and interviews[81] with prominent activists reveal an ongoing campaign by anonymous hacking groups to target outspoken voices. Groups such as the

73 Interview with Hisham Almiraat, conducted January 13, 2014.

74 Privacy International, *Their Eyes On Me: Stories of surveillance in Morocco*, (April 7, 2015) http://bit.ly/1JTHBZ4.

75 Interviews with digital activists and online journalists.

76 Reporters Without Borders, "RSF Backs Moroccan NGO Targeted by Interior Ministry," June 4, 2015, http://en.rsf.org/maroc-rsf-backs-moroccan-ngo-targeted-by-04-06-2015,47969.html.

77 Interviews with Dr. Fouad Abbou, professor of computer Science and Telecommunications and Dr. Hamid Harroud, director of the Information Technologies Services of Al Akhawayn University in Ifrane, conducted on 29 March 2015.

78 Paul Schemm, "Moroccan journalist ends hunger strike on passport promise," Associated Press, July 28, 2015, http://bigstory.ap.org/urn:publicid:ap.org:9188413890354165a7199406e84a6b58.

79 "Ali Lmrabet a pu récupérer ses pièces d'identité," *Telquel, April 9, 2015,* http://telquel.ma/2015/09/04/ali-lmrabet-pu-recuperer-ses-papiers-didentite_1461925.

80 Interview with Hisham Almiraat.

81 Interviews with Hishaam Almiraat, Samia Errazzouki, Yassir Kazar, and Ali Anouzla.

Monarchist Youth, the Moroccan Repression Force, the Moroccan Nationalist Group, and the Royal Brigade of Dissuasion have hacked into activists' email and social media accounts, often publishing offensive content in a bid to harm their reputation.[82]

82 Privacy International, *Their Eyes On Me: Stories of surveillance in Morocco*.

Freedom House

Myanmar

	2015	2016
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	18	17
Limits on Content (0-35)	17	17
Violations of User Rights (0-40)	28	27
TOTAL* (0-100)	**63**	**61**

* 0=most free, 100=least free

Population:	**53.9 million**
Internet Penetration 2015 (ITU):	**22 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- Internet penetration topped 20 percent in 2015, up from less than 2 percent in 2013 (see **Availability and Ease of Access**).
- Hackers targeted *The Irrawaddy* magazine's Burmese-language website in the lead-up to the November 2015 elections, publishing a fake report about Aung San Suu Kyi's health, though her National League for Democracy party won a parliamentary majority (see **Technical Attacks**).
- Five people were detained for at least six months each under the 2013 Telecommunications Law in reprisal for online speech criticizing military or government officials; at least one trial was still pending under the new administration (see **Prosecutions and Detentions for Online Activities**).
- Outgoing officials app oved Vietnamese military-linked Viettel's bid to enter the mobile telecommunications market in a joint venture with local fi ms and a subsidiary of military conglomerate Myanmar Economic Corporation (see **Availability and Ease of Access**).
- Campaigners used social media to advance causes including constitutional reform, election monitoring, and humanitarian assistance to flood victims and efugees (see **Digital Activism**).

Introduction

Higher rates of internet access and digital advocacy improved internet freedom, though the year also saw the highest number of prosecutions documented since liberalization began in 2011.[1]

Myanmar went through its second phase of political transition, shifting power from the military-backed government to the National League for Democracy (NLD) party chaired by Nobel Peace Prize laureate Aung San Suu Kyi in April 2016.[2] Troublingly, internet users were tentative in their discussion about the new government, and continued to practice self-censorship after the November elections, fearing harassment and censure from the still-powerful military, and even supporters of the democratically elected leadership.

The unprecedented political dynamism of the general elections in November 2015 was marred by intimidation of internet users by supporters on both sides of the political divide. With the new NLD administration sworn in on March 30, 2016, rights groups expect reform. Dozens of political prisoners were pardoned and released in April.[3] Another early step was to streamline bureaucracy with the creation of a new Ministry of Transport and Communications.

The government of former military leader President Thein Sein officially ended media censo ship in 2012. Norway's Telenor Group established the country's fi st independent connection to the international internet, and Qatar's Ooredoo launched mobile phone service across large parts of the country in 2014. The government passed a Telecommunications Law to facilitate this opening of the market.[4] However, it was the basis of several arrests for online speech in 2015 and 2016. And the outgoing communications ministry issued its last mobile telecommunication operator license to a newly-formed consortium in a move that observers said advantaged the military's financial in erests.

Online mobilization was particularly dynamic. All major political parties engaged on social media, which was an influential platfo m in major cities, and internet usage nationwide was 12 percent higher than usual on election day, according to one report.[5] However, intolerance is also rampant online, aggravated by discriminatory policies against ethnic minorities like the Muslim Rohingya,[6] who are denied citizenship under Myanmar's laws. Religious nationalist movements negatively influenced public discou se on the internet, especially in the run-up to the elections and immediately after the new government took office. In a new de elopment, some NLD supporters are showing intolerance for criticism of Aung San Suu Kyi.

1 Earlier Freedom House publications referred to Myanmar as Burma. The military-led government changed the country's name from Union of Burma to the Republic of the Union of Myanmar without a referendum in 1989, a decision the opposition rejected as politicized. Myanmar became increasingly common, particularly after the regime adopted a more civilian form of government.

2 Although the NLD won 79 percent of seats in parliament, Aung San Suu Kyi is barred from running for president under a clause in the constitution which excludes her for having a spouse or children who are foreign nationals (her sons are British citizens). Parliament elected her ally Htin Kway to the presidency and appointed Aung San Suu Kyi to the newly-created position of state counselor. See: BBC News, "Myanmar elects Htin Kyaw as fi st civilian president in decades," March 15, 2016, http://www.bbc.com/news/world-asia-35808921; Euan McKirdy, New government role created for Myanmar's Aung San Suu Kyi," April 7, 2016, http://www.cnn.com/2016/04/06/asia/aung-san-suu-kyi-state-counsellor-role-created/.

3 AAPP-B, "AAPP-B monthly Chronology of April 2016 and Current Political Prisoners list," May 20, 2016, http://aappb.org/2016/05/aapp-b-monthly-chronology-of-april-2016/.

4 Shibani Mahtani, "Myanmar's Telecom Revolution Bogs Down," The Wall Street Journal, October 25, 2013. http://on.wsj.com/1w4lTPD.

5 *Internet Journal,* November 13, 2015, http://internetjournal.media/news/4772

6 Human Rights Watch, "Myanmar: Rohingya Muslims Face Humanitarian Crisis," March 26, 2013, http://bit.ly/1HSsJdA.

Obstacles to Access

Internet access is improving in Myanmar, as increasing numbers of users go online via cell phones, which are becoming more affordable. Yet internet penetration still ranks among the world's lowest. The quality of service remains poor because of inadequate infrastructure, and poverty continues to limit citizens' internet usage. Military conglomerates are still positioned to benefit from the system and manipulate the telecommunications market.

Availability and Ease of Access

The number of internet users has notably increased over the past two years. The International Telecommunication Union estimated internet penetration at 22 percent in 2015, revising its 2014 estimate from 2 to 12 percent; it was less than 2 percent in 2013.[7] Users in most provincial towns have much poorer quality connections in comparison with the few urban cities, let alone those in rural villages. Chronic power outages, service interruptions, and insufficient transmission owers continue to impede efficient in ernet usage.

Private fi ed-line internet connections are prohibitively expensive, though there is significant e-gional variation. While prices are trending downwards, the cost of service during the coverage period remained comparable to the previous year. The one-time installation cost for a home broadband connection from MPT, the dominant state-owned provider, was US$50, plus an annual fee of US$50, with monthly rates from US$17 to US$80 for speeds from 512 Kpbs to 2.5 Mbps. For faster fiber connections, setup costs range f om US$200 to US$1,000; in addition to an annual US$60 fee, monthly service, starting at US$100, can run to thousands of dollars per month for speeds up to 100 Mbps.[8] Redlink, a private company run by the son of a former military general-turned-house speaker, charges even more: a fiber connection f 2 Mbps cost US$500 to set up, then US$125 per month plus a US$60 annual fee. Since Myanmar's gross domestic product was just US$980 per capita in 2014, these costs keep personal internet access far out of reach for the majority.[9]

Mobile penetration in the country reached 65 percent in December 2015, an increase from 30 percent in 2014. This calculation was based on the number of active SIM cards, which totaled 36 million by January 2016. Ericsson's Q3 2015 Mobility Report names Myanmar as the fourth-fastest growing market in the world.[10]

MPT has offered mobile phones since the 1990s, but charged from US$2,000 to US$5,000. The price dropped to US$200 in 2012 after the political and economic liberalization in 2011. In 2013 the military-owned MEC and MPT distributed a fini e number of SIM cards per month for about US$1.5 each under a state-run lottery. Telenor and Ooredoo introduced competition to the market in 2014 (see ICT Market). However, since they lack infrastructure compared to MPT, their underperforming services are often the impetus for users to subscribe to multiple providers and switch SIM cards to overcome connection issues.

7 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1cblxxY.

8 Based on an exchange rate of MMK 1,000 to $1, fiber se vice for 100mbps was listed at MMK 7,000,000 in 2015. See, http://www.mpt.com.mm/en/product-services/fi ed-line-internet/.

9 International Monetary Fund, "World Economic Outlook Database," October 2013, http://bit.ly/1DvPAd4.

10 Catherine Trautwein, "Myanmar named fourth-fastest-growing mobile market in the world by Ericsson," *Myanmar Times,* November 20, 2015, http://www.mmtimes.com/index.php/business/technology/17727-myanmar-named-fourth-fastest-growing-mobile-market-in-the-world-by-ericsson.html.

MPT offers this more reliable service and coverage at a premium, in violation of the state's own pricing regulation. According to an MCIT directive, operators should not charge more than MMK 20 (US$0.01) per minute for voice calls during peak hours and MMK 15 per minute off-peak, but MPT charged MMK 50 per minute in 2015, reduced to MMK 25 per minute in 2016. Ooredoo and Telenor also charged MMK 25 per minute, according to local news reports. MPT's prepaid service cost MMK 2 per minute for users on the GSM wireless network, and MMK 4 per minute for users of CDMA 800 and WCDMA networks. All operators offer promotional plans costing MMK 6 to 8 per 1MB of data and voice calls at MMK 20 per minute.

At these rates, mobile internet service is more accessible than ever before. In September 2015, operators described the prices as among the lowest in the world given Myanmar's recent entry into the telecommunications market.[11] Senior figu es within the sector accused their counterparts of sparking a price war by lowering their prices, threatening the investment still needed to ensure quality of service for consumers unsustainable.[12]

However, a regular mobile internet user might still expect to spend MMK 10,000 to 20,000 (US$10 to US$20) per month in 2016, while those who rely on the connection for business could spend MMK 30,000 to 50,000 (US$30 to US$50). This represents little change from last year and limits connectivity for a large percentage of the population, one quarter of which lives below poverty line.[13]

Restrictions on Connectivity

Until 2014, the Ministry of Communications and Information Technology (MCIT) essentially controlled the country's infrastructure via the state-owned Myanmar Post Telecommunication (MPT), which covers over 90 percent of the country.

Major operators and infrastructure investors have said that building infrastructure in Myanmar is the greatest challenge of the sector.[14] International financial institutions such as the Asia De elopment Bank and Europe's Infrastructure Development Fund have provided operators with loans and support to develop cable, bandwidth, and transmission towers.[15]

Myanmar is connected to the international internet via the SEA-ME-WE 3 submarine cable, and satellite and cross-border cable links with China and Thailand. Connections were formerly controlled by MPT, giving it a monopoly over international bandwidth, but Telenor and Ooredoo each reported having constructed three international connections to Thailand and China in 2016; Telenor said it is working on a fourth, to India.[16] A spokesperson for the company rated its dependence on MPT

11 *Internet Journal,* September 30, 2015, http://internetjournal.media/news/4307 .

12 Telegeography, "Price war, what is it good for? Absolutely nothing, say Myanmar cellcos," September 28, 2015, https://www.telegeography.com/products/commsupdate/articles/2015/09/28/price-war-what-is-it-good-for-absolutely-nothing-say-myanmar-cellcos/ .

13 Asian Development Bank, "Asian Development Bank & Myanmar: Fact Sheet," December 31, 2014, http://bit.ly/1RU97j7.

14 *Internet Journal,* September 16, 2015, http://internetjournal.media/news/4123 .

15 *7 Day Daily,* February 9, 2016, http://7daydaily.com/story/57611 and Telegeography, "IGT secures USD122m loan for Myanmar tower rollout," January 11, 2016, https://www.telegeography.com/products/commsupdate/articles/2016/01/11/igt-secures-usd122m-loan-for-myanmar-tower-rollout/ .

16 "Myanmar's connectivity catch-up," *Frontier Myanmar,* February 1, 2016, http://frontiermyanmar.net/en/news/myanmars-connectivity-catch-up.

at 10 percent in an interview with *Frontier Myanmar,* though Ooredoo declined to make a similar estimate.[17]

In early 2016, the Singapore-based cable company Campana Group announced plans to develop the Myanmar-Malaysia-Thailand-International Connection (MYTHIC) cable, Myanmar's first private undersea internet cable, which it said would provide an extra 300 Gigabits a second of bandwidth once it becomes operational in 2017.[18] As part of a first 100-Day Plan, the new Ministry of Transport and Communications also announced construction of onshore link to the undersea cable SEA-ME-WE 5 to be operational by early 2017.[19]

Since the two foreign telecom firms started to develop their own fiber networks in March 2015, capacity has increased. Low bandwidth continues to cause congestion, however, and power outages also frequently disrupt access.[20] Heavy flooding in several regions of the country, bureaucratic processes, and corruption often impede construction.

ICT Market

Despite diversification, state-owned conglomerates continue to skew the telecommunications playing field through the state-owned Myanmar Post Telecommunication (MPT), and a new military-linked joint venture. Long-promised plans to privatize MPT have not materialized since the government announced them in 2012.

In 2013, the government awarded international licenses to Norway's Telenor and Qatar's Ooredoo, allowing them to offer services and infrastructure alongside MPT.[21] Military-linked Yatanarpon Teleport (YTP) was also allowed to run as a local operator.

Between June 2015 and April 2016, in a maneuver that allegedly advantaged the military's financial interests, the outgoing ministry selected the Vietnamese company Viettel,[22] which is run by the Vietnamese military,[23] to operate a 49 percent stake in a fourth mobile telecommunication operator as part of a joint venture with a consortium of 11 local firms and a government shareholder.[24] The consortium and the government shareholder, Star High Public Company under the supervision of the Ministry of Defense, will control 51 percent of the operation, which was expected to apply for a license in late 2016 and begin providing service in 2017.[25]

17 "Myanmar's connectivity catch-up," *Frontier Myanmar,* February 1, 2016, http://frontiermyanmar.net/en/news/myanmars-connectivity-catch-up.

18 "Myanmar's connectivity catch-up," *Frontier Myanmar,* February 1, 2016, http://frontiermyanmar.net/en/news/myanmars-connectivity-catch-up .

19 *Internet Journal,* May 31, 2016, http://internetjournal.media/news/6511 .

20 Kyaw Hsu Mon, "Power Chief Pledges End to Rangoon Outages," *The Irrawaddy,* April 8, 2015, http://www.irrawaddy.org/burma/power-chief-pledges-end-to-rangoon-outages.html.

21 Shibani Mahtani and Chun Han Wong, "Norway's Telenor, Qatar Telecom Get Myanmar Telecom Licenses," *Wall Street Journal*, June 27, 2013.

22 Telegeography, "Myanmar selects Viettel to partner for fourth licence,"March 29, 2016, https://www.telegeography.com/products/commsupdate/articles/2016/03/29/myanmar-selects-viettel-to-partner-for-fourth-licence/ ;

23 Reuters, "Viettel plans $1.5 billion Myanmar telecoms investment with local firms," April 18, 2016, http://www.reuters.com/article/viettel-myanmar-telecoms-idUSL3N17L3DR .

24 Republic of the Union of Myanmar, "Results of the Request for Proposal for Partnership with local Consortium willing to apply for Fourth Telecom Operator Licence in the Republic of the Union of Myanmar," press release, March 25, 2016, http://bit.ly/2fBTGju.

25 Aung Kyaw Nyunt and Steve Gilmore, "Fourth telco licence just weeks away," *Myanmar Times,* October 4, 2016, http://www.mmtimes.com/index.php/business/technology/22882-fourth-telco-licence-just-weeks-away.html .

Star High Public Company is operated by the military-run conglomerate Myanmar Economic Corporation, which since 2008 is subject to financial sanctions by Uni ed States Treasury for its role in supporting repression by the military junta.[26] Officials said the com any was chosen because it could offer capital, access to 1,000 towers and more than 13,000 kilometers of fibe , among other telecoms assets. However, the license fee for the fourth operator, at US$300 million, was significantly lo er than payments made by the other two foreign fi ms, creating the appearance of an uneven playing field. elenor paid US$500 million and local news reports said Qatar's Ooredoo spent more than US$1 billion for their respective licenses.[27]

Regulatory Bodies

The Posts and Telecommunications Department regulates Myanmar's telecommunications industry under the MCIT. Under the junta, the MCIT and intelligence agencies implemented arbitrary and ad hoc censorship decisions. Upon taking power in 2016, the new NLD administration merged the MCIT with the Ministry of Rail Transport and Ministry of Transport to create a new Ministry of Transport and Communications.[28]

Other state institutions tasked with information and communications technology (ICT) development and management have been largely inactive.[29] The Myanmar Computer Federation, formed under the 1996 Computer Science Development Law and comprised of industry professionals, is the designated focal point for coordination with the ITU. Critics say it failed to take advantage of the 2011 political change to play a more active role in the ICT sector.

Clause 86 of the Telecommunications Law established an independent commission to take over regulatory functions within two years. The business community also welcomed the law's creation of an appeal tribunal mechanism to adjudicate over administrative issues in the telecommunications industry. The MCIT subsequently released two regulatory laws, License Provision in October 2014 and Networking and Linking in January 2015.

Three more regulatory laws followed: Rules on Competition in June 2015, Rules on Numbering in December, and Frequency Spectrum in March 2016. The MCIT released a draft by-law on Gateway Regulation to regulate international gateway services in January, developed in consultation with the World Bank. The enactment of the by-laws and regulations is a good indication of the government's willingness to further liberalize the country's telecoms sector.

26 U.S. Department of the Treasury, "Treasury Designates Burmese State-Owned Enterprises," press release, July 29, 2008, https://www.treasury.gov/press-center/press-releases/Pages/hp1105.aspx; Shibani Mahtani and Richard C. Paddock "'Cronies' of Former Myanmar Regime Thrive Despite U.S. Blacklist," *Wall Street Journal,* August 12, 2015, http://www.wsj.com/articles/cronies-of-former-myanmar-regime-thrive-despite-u-s-blacklist-1439433052 .

27 Clare Hammond and Catherine Trautwein, "Viettel picked for fourth telecoms tie-up with military partner," *Myanmar Times,* March 25, 2016, http://www.mmtimes.com/index.php/business/technology/19662-viettel-nears-contract-for-fourth-telecoms-operator.html; Catherine Trautwein, "Telcos lobby govt over fourth operator," *Myanmar Times,* February 19, 2016, http://www.mmtimes.com/index.php/business/technology/19088-telcos-lobby-govt-over-fourth-operator.html.

28 Aye Thidar Kyaw and Catherine Trautwein, Chan Mya Htwe, "NLD proposes merging economic ministries into powerhouses," March 18, 2016, http://www.mmtimes.com/index.php/business/19540-nld-proposes-merging-economic-ministries-into-powerhouses.html.

29 These include the Myanmar Computer Science Development Council, the e-National Task Force, the Myanmar Computer Federation, the Myanmar Computer Professionals' Association, the Myanmar Computer Industry Association, and the Myanmar Computer Enthusiasts' Association.

Limits on Content

During the coverage period, both military and self-styled pro-democracy activists actively pressured online media practitioners and outlets they perceived as critical, keeping levels of self-censorship high. Tactics included reporting rival Facebook users for violating the site's community standards, resulting in their accounts being temporarily disabled, and manipulative political commentary. While digital content was not subject to censorship, sensitive political and social topics were nevertheless underrepresented online.

Blocking and Filtering

The government lifted systematic state censorship of traditional and electronic media in 2012. Since then, political content appeared to be almost universally available, and even social content, such as pornography, was not blocked as of mid-2016.

Content Removal

While new readers are more likely to encounter a range of content than they were in the past, authorities have made a concerted effort to exclude certain topics from mainstream discourse in ways that lack transparency and due process. Notably, since censorship was officially li ted the military has pressured individuals and media outlets to remove posts or images perceived to hurt the public image of the armed forces. Content subject to prosecution is also generally removed (see "Prosecutions and Detentions for Online Activities").

In a phenomenon seen for the fi st time during the coverage period, Facebook users misused the mechanism for reporting offensive content in order to disable rival pages. Activists with different political agendas organized to report their opponents for violating Facebook's community standards, resulting in specific accounts or ages being temporarily removed while the owner appealed to have them reinstated.

Some prominent examples were apparently carried out by NLD supporters. A cartoonist who uses the penname Maung Maung Fountain had his account briefly shut down in anuary 2016 after he shared a cartoon that made fun of Aung San Suu Kyi's inconsistencies. Unknown people had reported him to Facebook for violating a requirement that users identify themselves by name they use in everyday life.[30] Dr. Than Htut Aung, CEO of the Eleven Media Group, said that his Facebook account was temporarily disabled in January using the same process after he criticized a top NLD leader's handling of the media.[31] The Eleven Media Group had generally advocated for the NLD when it was in the opposition.

Media, Diversity, and Content Manipulation

Self-censorship with regard to military and related issues is common online, especially after military officials issued wa nings in response to news articles and cartoons they said harmed the dignity and

30 Nyan Lynn Aung, "Facebook unblocks cartoonist's page," *Myanmar Times,* January 14, 2016, http://www.mmtimes.com/index.php/national-news/yangon/18473-facebook-unblocks-cartoonist-s-page.html.

31 Interview with Dr. Than Htut Aung, March 30, 2016

spirit of the military during the Kokang conflict in 2015. t the same time, journalists are becoming more cautious when reporting on the NLD government. Although the media was relieved from "government censorship" in 2012, they increasingly fear "public censorship" in the form of social media abuse, according to one of the country's largest weeklies.[32] In June 2015, one local reporter told *The Irrawaddy* she had changed her online behavior and "acted more cautiously when covering controversial subjects" from fear of online harassment.[33]

Social media and communication apps including Viber, Line, Friendfinde , and Google+ are freely available. Facebook is the most popular, since many users developed the habit of using the platform to share information, initiate collective action on social and political issues, or follow exile media outlets when website blocking was still pervasive. According to one estimate, there were about seven million Facebook users in October 2015, up from three million in January.[34] For some users frustrated at the challenge of navigating between sites on poor connections, Facebook is the sole source of online news, potentially depriving local outlets of the advertising revenue.

Facebook was also an effective instrument for urban politicians in the run-up to the November elections, though its impact is limited in rural areas. One-third of Myanmar's 91 political parties have an active Facebook presence.[35] Young, digitally-savvy candidates used Facebook to mobilize volunteers and communicate with voters, including Nay Phone Latt, the blogger and former political prisoner who directs the advocacy group Myanmar ICT for Development Organization (MIDO). During a purge inside the then-ruling USDP party in August, House Speaker Thura U Shwe Mann, who was removed from the party's chairmanship, took to Facebook after several hours incommunicado, generating thousands of "likes." Aung San Suu Kyi, whose official age has been "liked" by over 1.3 million people, received the most online support. Along with content from the campaign trail, the politician many call "The Lady" posted a video on how to cast a ballot.[36]

Some progovernment Facebook pages, such as Myanmar Express, and blogs like *OppositEye,* actively manipulate online commentary to conduct smear campaigns against Muslims or the political opposition. Ethnic Burman internet users also spread racially-charged comments across social media platforms throughout the coverage period.[37] *Mabatha,* the radical group of Buddhist monks, intensified its anti-Muslim and anti-NLD campaigns in the run-up to the elections.

Digital Activism

Online activism increased during the coverage period thanks to the 2015 elections and humanitarian relief campaigns online. One of the most effective online campaigns urged people to verify their names in the electoral register in September, after the Union Election Commission announced irregularities in the existing voter lists.

From July through September 2015, severe flooding hit 12 f the country's 14 states resulting in over 100 deaths and affecting up to one million people. Local charity associations effectively used social

32 *7 Day Daily,* March 30, 2016, http://www.7daydaily.com/story/61577 .

33 Sean Gleeson, "For Burma's Journalists, a Bumpy Road to 'Discipline-Flourishing Democracy'," *Irrawaddy,* June 17, 2015, http://www.irrawaddy.com/burma/for-burmas-journalists-a-bumpy-road-to-discipline-flourishing-democrac .html .

34 *Internet Journal,* October 23, 2016, http://internetjournal.media/news/4582 .

35 Catherine Trautwein, Wa Lone, "The Facebook election? Not quite yet," *Myanmar Times,* October 7, 2015, http://www.mmtimes.com/index.php/business/technology/16877-the-facebook-election-not-quite-yet.html .

36 Catherine Trautwein, Wa Lone, "The Facebook election? Not quite yet."

37 Sait Latt, "Intolerance, Islam and the Internet in Myanmar today," New Mandala, June 10, 2012, http://bit.ly/1g6ktQr.

media to spread news and mobilize resources. Via the three mobile operators, people could make donation to flood victims via SMS. MP , which has 13 million mobile subscribers, reported receiving US$200,000 of donations within four days.[38] Facebook also partnered with Save the Children International to fundraise for children affected by the disaster. In August, a new button appeared atop cluttered newsfeeds across the globe offering users the chance to donate US$10 or more to the cause; Facebook pledged to match donations up to a total of US$500,000.[39]

Online advocacy also had a positive effect after a video clip depicting abuse in a military academy circulated widely on social media. The public response forced the military to launch a high-level investigation team and pledge action against abusive officials [40] an unprecedented gesture towards accountability from the country's virtual power holder.

A fi e percent tax on mobile phone top up cards was the subject of a huge online campaign, causing the previous parliament to suspend it in May 2015. The tax took effect on April 1, 2016, but media outlets and social media users who had been vocal against the levy appeared to concede, particularly since the revenue generated was now supporting the new government, which said the fi st month's earnings went to support education.[41]

Violations of User Rights

The 2013 Telecommunications Law transformed the industry, but introduced a defamation provision which was used to jail internet users for political speech during the coverage period of this report. Other harsh punishments for political dissent on electronic media remain on the books. Hackers targeted private media outlets and also high-level, newly-elected officials.

Legal Environment

The current constitution, drafted by the military-led government and approved in a fla ed 2008 referendum, does not guarantee internet freedom. It states that every citizen may exercise the right to "express and publish their convictions and opinions," if "not contrary to the laws enacted for Union [of Myanmar] security, prevalence of law and order, community peace and tranquility or public order and morality."[42]

Parliament enacted the long-pending Telecommunications Law, drafted with the help of international experts including the World Bank, in October 2013.[43] Domestic and international investors applauded the consultative drafting process, along with the guidelines for the industry which pro-

38 *Internet Journal,* August 11, 2015, http://internetjournal.media/news/3696 .

39 Yen Saning, "Facebook Will Match Your Flood Relief Donations," *Irrawaddy,* August 10, 2015, http://www.irrawaddy.com/burma/facebook-will-match-your-flood- elief-donations.html .

40 https://www.facebook.com/XinhuaMyanmar/photos/a.423782941124025.1073741827.422671591235160/565720306930287/?type=3&theater.

41 *Internet Journal,* May 27, 2016, http://internetjournal.media/news/6484 and "Tax paid on cell phone top-ups to be spent on education," *Coconuts Yangon,* May 27, 2016, http://yangon.coconuts.co/2016/05/27/tax-paid-cell-phone-top-ups-be-spent-education .

42 Republic of the Union of Myanmar Constitution, Ch. VII, Defense Services, art. 354 sec. b. http://www.Myanmarlibrary.org/show.php?cat=1140.

43 The Pyidaungsu Hluttaw passage of The Telecommunication Law, No. 31, October 8, 2013, http://bit.ly/1g8hlU5.

vided the foundation for improving access.[44] However, the law includes broadly-worded clauses that subject internet activity to criminal punishment. Clause 66(d) prohibits "extortion…coercion, unlawful restriction, defamation, interfering, undue influence, or intimidation using a elecommunication network," with penalties up to three years of imprisonment. Clause 68 punishes "communication, reception, sending, distribution or sharing of incorrect information with dishonest intention" with imprisonment for up to a year, an unspecified fine, or both. The law was epeatedly implemented to punish speech during the coverage period of this report, though no by-laws have been enacted detailing procedures for its enforcement.[45]

The government also failed to repeal the notorious 2004 Electronic Transaction Law (ETL) in 2013, which has routinely been used to criminalize internet activism. Instead, parliament amended the ETL, reducing but not eliminating possible jail sentences for ill-defined online actions. Under the newly-amended law, "any act detrimental to" state security, law and order, community peace and tranquility, national solidarity, the national economy, or national culture—including "receiving or sending" related information—is punishable by three to seven years imprisonment, down from seven to fi teen years.

In 2014, Thaung Tin, an MCIT deputy, acknowledged the need to fix epressive laws like the ETL and the Computer Science and Development Law, which criminalizes unauthorized use of a computer with a "fax-modem card."[46] In 2014 the MCIT announced plans to revise the ETL and clarify confusing language, but no developments had been reported in mid-2016.[47] During the coverage period, officials also said a dra t law to punish cybercrime was being drawn up, but none had been submitted to the new parliament by mid-year.[48]

Prosecutions and Detentions for Online Activities

Prior to the leadership change, at least six internet users were charged and four subsequently sentenced under the 2013 Telecommunications Law for sharing social and political content on Facebook, marking the highest number of prosecutions for online speech since the political opening.[49] One of those charges was brought by NLD supporters in response to images of Aung San Suu Kyi doctored to make her appear naked.

- In September 2015, Zaw Myo Nyunt was arrested for sharing an illustration showing feet stamping on Myanmar's army chief on Facebook. In January 2016 he was given a one-year prison sentence with labor under the telecommunication law. Patrick Kum Jaa Lee, an NGO worker, was also arrested for allegedly sharing Zaw Myo Nyunt's post. He served a six-

44 Shibani Mahtani, "Myanmar's Telecom Revolution Bogs Down," The Wall Street Journal, October 25, 2013. http://on.wsj.com/1w4lTPD.

45 Lun Min Mang, "Kachin activist convicted in Facebook defamation case," *Myanmar Times,* January 25, 2016, http://www.mmtimes.com/index.php/national-news/18631-kachin-activist-convicted-in-facebook-defamation-case.html .

46 The State Law and order Restoration Council passage of The Computer Science Development Law, No. 10/96, September 20, 1996, http://bit.ly/1CXw1zk.

47 "A newly designed Electronic Contact Cooperation Law may be released soon," 7Day Daily, December 14, 2014. http://7daydaily.com/story/26977.

48 "Task force set up to tackle cyber crime," *Eleven Myanmar,* May 30, 2015, http://elevenmyanmar.com/local/task-force-set-tackle-cyber-crime .

49 Dozens of political prisoners formerly jailed for electronic activities remained free after they were released en masse in January 2012.

month sentence for violating Article 66(d) of the Telecommunication Law and was released in April 2016.[50]

- In November 2015, poet Maung Saung Kha was detained under Article 505 of the penal code, which criminalizes insult, and Article 66(d) of the Telecommunication Law for posting a poem on Facebook that implied a tattoo of the president on his penis disappointed his wife.[51] He was given six month prison sentence and released in May 2016 because he had already served the time.[52]

- In December 2015, a court jailed NLD party member Chaw Sandi Tun for six months under Article 66(d) of the Telecommunication Law for a Facebook post perceived as mocking the army chief and a new military uniform. Her post compared the light green office 's uniform with that of a *longyi*, or traditional Myanmar skirt, worn by Aung San Suu Kyi. She was arrested in October 2015 and released on March 30, 2016, after serving her sentence.[53]

- In February 2016, sailor Hla Phone was detained under Article 66(d) of the Telecommunications Law over a series of posts "defaming the army chief, the military and the president by posting photoshopped pictures and text," made by the well-known Facebook account Kyat Pha Gyi. He denied operating the account, which remained active after his arrest and denied any connection with Hla Phone.[54] Another charge under Article 505 of the penal code was added later,[55] and he was officially indic ed in August, after more than six months in detention.[56]

- In March 2016, Facebook user Than Tun, a local USDP official, was sen enced to six months in prison with labor after NLD supporters charged him under Article 66(d) of the Telecommunication Law for sharing an image of Aung San Suu Kyi altered to make her appear naked, along with sexually explicit language.[57]

Moreover, at least one arrest took place after the new government came to power. On May 4, 2016, police arrested Nay Myo Wai, a prominent anti-Muslim activist, after an NLD supporter filed suit against him under Article 66(d) of the Telecommunications Law. News reports said he was charged based on a Facebook post claiming that army chief Min Aung Hliang had not seized power because

50 Esther Hitusan, "Prominent Political Prisoner Freed in Myanmar, Many Remain," The Associated Press, April 1, 2016, http://www.usnews.com/news/world/articles/2016-04-01/prominent-political-prisoner-freed-in-myanmar-many-remain and Lun Min Mang, "Kachin activist convicted in Facebook defamation case," *Myanmar Times,* January 25, 2016, http://www.mmtimes.com/index.php/national-news/19805-kachin-activist-released-after-imprisonment-for-facebook-post.html .

51 *Eleven Media,* Facebook, http://bit.ly/2eGUvCu; Su Myat Mon, "Kachin Aid Worker Jailed for Defamatory Facebook Post Walks Free," *Irrawaddy,* April 1, 2016, http://www.irrawaddy.com/burma/kachin-aid-worker-jailed-for-defamatory-facebook-post-walks-free.html and PEN International, "Myanmar: Poet on trial for defamation," May 30, 2016, http://www.pen-international.org/newsitems/myanmar-poet-on-trial-for-defamation/ .

52 ABC News "Myanmar's 'penis poet' Maung Saungkha freed after six months in jail for defamation," May 24, 2016, http://www.abc.net.au/news/2016-05-24/myanmars-penis-poet-freed-after-six-months-in-jail/7442908 .

53 Su Myat Mon, "Chaw Sandi Tun, Famed Facebook Antagonizer, Released From Prison," *Irrawaddy,* March 30, 2016, http://www.irrawaddy.com/burma/chaw-sandi-tun-famed-facebook-antagonizer-released-from-prison.html .

54 *Irrawaddy,* "Arrest over Facebook Post a Case of Mistaken Identity, Defendant Says," February 16, 2016, http://www.irrawaddy.com/burma/arrest-over-facebook-post-a-case-of-mistaken-identity-defendant-says.html .

55 "Accused "Kyat Pha Gyi" account owner face another charge," *Eleven Media,* October 3, 2016, http://www.elevenmyanmar.com/local/accused-kyat-pha-gyi-account-owner-face-another-charge .

56 Reuters, "Man Indicted for Insulting Military Chief, Former President on Facebook," via *Irrawaddy,* August 23, 2016, http://www.irrawaddy.com/burma/man-indicted-for-insulting-military-chief-former-president-on-facebook.html .

57 *7 Day Daily,* March 28, 2016, http://www.7daydaily.com/story/61497; Salai Thant Zin, "USDP Official Sued o er Fake Suu Kyi Nude Shared on Facebook," *Irrawaddy,* October 19, 2015, http://www.irrawaddy.com/election/news/usdp-official-sued-o er-fake-suu-kyi-nude-shared-on-facebook.

he wanted to marry Suu Kyi.[58] The regional court denied his bail request in June;[59] he was found not guilty in July.[60]

However, the NLD did not press charges against an individual using the Facebook account name Ye Lwin Myint who threatened to kill Aung San Suu Kyi, after the user issued an apology. On February 3, the Ye Lwin Myint account posted a threat to shoot Suu Kyi if Article 59(f) of the constitution, which bars her from the presidency, was suspended.[61]

Surveillance, Privacy, and Anonymity

State surveillance, historically pervasive and politicized, abated after the political opening but has intensified somewhat since 2013 due o religious unrest and the opposition-led constitutional reform movement, among other issues. Regrettably, the Telecommunications Law introduced scope for abuse. Clause 75 grants unspecified go ernment agents the authority "to direct the organization concerned as necessary to intercept, irrespective of the means of communication, any information that affects the national security or rule of law." The clause added that the government would do so without affecting the fundamental rights of the citizens, but included no privacy protections. Clause 76 allows the government to inspect or seize this information on the premises of private telecommunications enterprises.

In March 2016, Telenor and Ooredoo told journalists that authorities have asked them to provide private customer information 85 times in total under an interim agreement with the regulator while a framework establishing procedures for compliance with the Telecommunications law remains pending. Telenor reported complying with 11 out of 58 requests, and Ooredoo with nine out of 27. Both companies said that requests have been so far limited to historical data or call records.[62] MPT refused to supply the media with any information about such requests. Several international and local civil society representatives and some diplomats believe that the military has stepped up surveillance by means of wiretapping, hacking and even intercepting Voice over Internet Protocol (VoIP) calls amid the intensifying social protests and political rivalries developing during the coverage period.[63]

Intimidation and Violence

No incident of violence was reported during this coverage period, though journalists operating on and offline eported receiving death threats. In just one example, an anti-Muslim extremist threatened journalists in June 2015 following the Democratic Voice of Burma's coverage of Rohingya

58 The Associated Press, "Myanmar Anti-Muslim Activist Arrested for Post About Suu Kyi," via Voice of America, May 5, 2016, http://www.voanews.com/content/myanmar-anti-muslim-activist-arrested-for-post-about-suu-kyi/3316586.html .

59 Salai Thant Zin, "The Irrawaddy: Court denies bail to ultra-nationalist politician charged with defamation," Burma Net, June 21, 2016, http://www.burmanet.org/news/2016/06/21/the-irrawaddy-court-denies-bail-to-ultra-nationalist-politician-charged-with-defamation-salai-thant-zin/ .

60 Salai Thant Zin, "Nationalist Provocateur Let Free in Defamation Case," *Irrawaddy,* July 15, 2016, http://www.irrawaddy.com/burma/nationalist-provocateur-let-free-defamation-case.html .

61 Toe Wai Aung, "NLD accepts apology from Facebook user," *Myanmar Times,* February 10, 2016, http://www.mmtimes.com/index.php/national-news/18895-nld-accepts-apology-from-facebook-user.html .

62 Catherine Trautwein, "Mobile operators comply with one in four data requests," *Myanmar Times,* March 30, 2016, http://www.mmtimes.com/index.php/business/technology/19721-mobile-operators-comply-with-one-in-four-data-requests.html .

63 Interviews with a family member of Thura Shwe Mann, who was purged in August 2015 from the ruling party's chairmanship, and one senior diplomat" December 2015.

migrants stranded in the Andaman Sea and the Malacca Straits.[64] The internet was also a medium for intimidation and harassment. Ye Lwin Myint threatened to kill Aung San Suu Kyi on Facebook in February 2016 (see "Prosecutions and Detentions for Online Activities").

Technical Attacks

Research published during the coverage period identified attacks esulting in a string of media website defacements dating back to 2012 as having been initiated on military premises.

In October 2015, hackers attacked *The Irrawaddy* magazine's Burmese-language website twice within a few days. The hackers posted a fabricated story saying then-opposition leader Aung San Suu Kyi was suffering from ovarian cancer. In a separate attack, the site was hacked and left inaccessible for several hours.[65]

In November, the Sweden-based cyber security fi m Unleash Research Labs released the results of a three-year investigation identifying the group behind the attack, and others timed to coincide with the lead-up to the November 2015 elections, as the "Union of Hacktivists." The fi m said it had traced the group's activities to a secretive, military-operated network hidden behind two fi ewall proxies. The attackers compromised the target sites weeks or months ahead of publicly defacing them, and worked to obtain passwords to staff email accounts, according to the report.

The fi m's report also detailed the activities of the prominent hacktivist network Blink Hacker Group (BHG), which has claimed responsibility for numerous distributed denial-of-service (DDoS) attacks on Democratic Voice of Burma over its coverage of the persecuted Rohingya minority in western Myanmar.[66]

Targeted hacks remained widespread in 2016. High profile public fig es were subject to attacks, including top NLD leader Win Htein and the newly elected Yangon Chief Minister Phyo Min Thein.[67]

64 Kyi Naing, "Politician directs death threats at Myanmar journalists," *The Nation,* June 2, 2015, http://www.nationmultimedia.com/asean&beyon/Politician-directs-death-threats-at-Myanmar-journa-30261260.html .

65 "Hackers Hit The Irrawaddy's Burmese Website with False News Story," *Irrawaddy,* October 12, 2015, http://www.irrawaddy.com/burma/hackers-hit-the-irrawaddys-burmese-website-with-false-news-story.html .

66 Unleashed Research Labs, "Fighting Cyber Attacks during the Burmese Elections, November 2015, http://unleashed.blinkhackergroup.org/release/ .

67 *7 Day Daily,* April 20, 2016, http://www.7daydaily.com/story/62602 .

Freedom House

Nigeria

	2015	2016
Internet Freedom Status	Partly Free	Partly Free
Obstacles to Access (0-25)	10	10
Limits on Content (0-35)	8	7
Violations of User Rights (0-40)	15	17
TOTAL* (0-100)	**33**	**34**

* 0=most free, 100=least free

Population:	**182.2 million**
Internet Penetration 2015 (ITU):	**47 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Partly Free**

Key Developments: June 2015 – May 2016

- The Frivolous Petitions Prohibition Bill 2015 threatened to restrict social media, but it was withdrawn in May 2016 following significant digital activism (see **Digital Activism**).
- The Digital Rights and Freedom Bill 2016, drafted by civil society organizations to codify internet freedom protections, passed its second reading in the House of Representatives (see **Legal Environment**).
- Numerous bloggers and online journalists were arrested for their online activities, many under the May 2015 cybercrime law (see **Prosecutions and Detentions for Online Activities**).

Introduction

Internet freedom in Nigeria declined due to an unprecedented pattern of arrests and prosecutions against bloggers that followed the passage of the Cybercrime Act in 2015.

Nigeria has a vibrant, savvy, and growing internet user population, enabled by a strong and innovative technology sector. Compared to the environment for traditional news media in Nigeria, online media is relatively free from restrictions, with no blocking or fil ering of online content reported during the coverage period.

A robust civil society has helped protect and enhance internet freedom for Nigerians, as demonstrated by the successful social media movement against the Frivolous Petitions Prohibition Bill 2015. Activists called it the "Social Media Bill" because it threatened to constrain critical expression on social networks. The bill was withdrawn on May 17, 2016, following statements by senators that reflec ed civil society's concerns. To codify protections for Nigeria's internet freedom, civil society groups drafted the Digital Rights and Freedom Bill 2016, which underwent parliamentary review in 2016.

Despite the progress observed, a cybercrime law passed at the end of former President Goodluck Jonathan's tenure in May 2015 led to the arrest of several bloggers and online journalists on charges of "cyberstalking" for online writings that criticized government officials and po erful bankers. Four prosecutions were documented during this report's coverage period, and arrests continued to be reported in late 2016, marking a significant jump o er the number of incidents reported in previous years. Intimidation and harassment for online expression also became more common, and self-censorship noticeably increased.

Obstacles to Access

Access to information and communications technologies (ICTs) continued to grow, despite high costs and frequent power cuts that disrupt network services. The Communication Service Tax Bill 2015, introduced in March 2016, threatens to jeopardize the affordability of internet access by imposing a 9 percent tax on communications services.

Availability and Ease of Access

With over 86 million users, Nigeria has one of the largest internet user populations in sub-Saharan Africa. The internet penetration rate was 47 percent in 2015, up from 43 percent in 2013 according to the International Telecommunications Union (ITU).[1] Rapid growth in internet use can largely be attributed to the proliferation of mobile phone and Fixed Wireless Access (FWA) services.[2] According to the Nigerian Communications Commission (NCC), the sector regulator, mobile phone teledensity in Nigeria stood at 108 percent, while there were almost 96 million active mobile internet subscriptions on GSM and CDMA networks as of January 2016.[3] The ITU documented a lower mobile phone penetration rate of 82 percent in 2015, up from 78 percent in 2014.[4]

1 International Telecommunication Union, "Percentage of Individuals Using the Internet," 2000-2013, http://bit.ly/1cblxxY.

2 Fixed Wire Access (FWA) is a type of high-speed internet access that uses radio signals as a connection to service providers instead of cables, enabling areas that lack fiber optic cables or DSL o access broadband internet.

3 Nigerian Communications Commission, "Active Internet Subscriptions (GSM) and (CDMA)," http://bit.ly/1kAqyVk.

4 International Telecommunication Union, "Mobile-cellular subscriptions," 2000-2013, http://bit.ly/1cblxxY.

Increasing access to the internet is driven by affordable data services for mobile subscribers. The Alliance for an Affordable Internet ranked Nigeria the 12th most affordable internet environment among 51 developing and emerging countries assessed in its 2015 Affordability Drivers Index.[5] As of March 2016, BlackBerry service packages cost as low as US$7.50 a month, an option that attracts many young Nigerians. Android data services have also been become popular, with 1 gigabyte of data available for US$5. As technologies improve, prices have continued to decrease; in 2016, for example, the average cost of a GSM plan was US$0.05 per megabyte of data, compared to US$0.26 per megabyte in 2015 and US$1 per megabyte in 2011.

Nevertheless, costs are still a major impediment to internet access for many Nigerians, particularly those in rural areas, and speeds are still slow, averaging 3.3 Mbps (compared to a global average of 6.3 Mbps), according to Akamai's "State of the Internet" report.[6] Nigeria's internet user landscape is also characterized by a significant digital gender divide: Oc ober 2015 research by the Web Foundation found that poor women in Nigeria's largest city, Lagos, were 50 percent less likely to have access to the internet than men of the same age, education, and income level.[7]

In March 2016, the government introduced the Communication Service Tax Bill 2015 which, if passed, threatens to jeopardize the affordability of internet access by imposing a 9 percent tax for communications services, such as SMS, data, and voice services, payable by consumers.[8]

Power cuts frequently disrupt service and access, despite Nigeria's status as an oil-rich country. Nigerian households reportedly received an average of less than six hours cumulative power supply per day in August 2015, and over 77 percent of Nigerians rely on alternative electricity sources.[9] Those who can turn to private generators and standby battery-powered inverter systems to stay online during outages. In a March 2016 apology, the government said "sabotage, gas shortage and vandalism of power infrastructure" were responsible for the power supply problems.[10]

Shortfalls in power supply undermine the quality of internet service offered by providers. Telecommunications base stations in Nigeria are typically powered by diesel generators, which reportedly account for 80 percent of their operating expenses.[11] Separately, the need to pay for expensive backup power generators has accelerated the closure of cybercafés that were already struggling with competition against the growing popularity of internet access on mobile devices.

Another major obstacle to internet access in Nigeria is language literacy. Home to over 500 local languages,[12] most internet content is in English, and local language content is vastly underrepresented. For example, the Wikipedia pages in the three major Nigerian languages of Yoruba, Hausa and Igbo are sparsely developed, and in many instances, Wikipedia entries on Nigerian topics are edited by

5 Alliance for Affordable Internet, The Affordability Report, 2015, http://a4ai.org/2015-16-a4ai-affordability-report-out-today/

6 Akamai, "Average Connection Speed," map visualization, *The State of the Internet*, Q1 2016, accessed August 1, 2016, http://akamai.me/1LiS6KD

7 Web Foundation, "Women's Rights Online: translating access into empowerment," October 20, 2015, http://bit.ly/1MTh70d

8 Communication Services Tax Bill, 2015, http://bit.ly/29HIOth; "Nigeria's onerous new Communication Service Tax Bill, by Tomiwa Ilori," Premium Times, June 6, 2016, http://opinion.premiumtimesng.com/2016/06/06/a-stitch-in-time-saves-nine-a-review-of-the-communication-service-tax-bill-by-tomiwa-ilori/

9 NOI Polls, "Average Cumulative Power Supply Still Deplorable as Nigerians Receive Less Than 6 Hours Per Day," August 18, 2015, http://bit.ly/29HHtlZ.

10 "Power failure: Nigerian govt apologizes, blames sabotage," Premium Times, March 11, 2016, http://bit.ly/1Ux1fo1

11 Compared to a mere 5% in Malawi where power from the grid is stable. See, Association of Telecommunication Companies of Nigeria: http://bit.ly/1Uc58Pb

12 Nigerian languages, http://www.onlinenigeria.com/languages/languages.asp

editors not residing in Africa.[13] Local language resources, such as audio and video health and educational material, come with higher data requirements, potentially limiting access for users who can afford less data yet who stand to benefit the most f om educational materials online.

Spotlight on Marginalized Communities

Freedom on the Net 2016 **asked researchers from India, Indonesia, Kenya, Kyrgyzstan, Jordan, Mexico, Nigeria, and Tunisia to examine threats marginalized groups face online in their countries. Based on their expertize, each researcher highlighted one community suffering discrimination, whether as a result of their religion, gender, sexuality, or disability, that prevents them using the internet freely.**

In Nigeria, Olutosin Adebowale, conducted a survey of 25 women and 25 girls in rural areas across Nigeria's six geopolitical zones, who described the challenges they face accessing the internet in interviews conducted by research assistants in person or by telephone.[1] The study found:

- The lack of internet facilities in rural communities in Nigeria is depriving women and girls of education and employment opportunities. Ninety-eight percent of survey respondents said there was no public internet access where they live; thirty-four percent said the nearest internet access point was over 40 km from home.
- The high cost of home internet service keeps women offline, e en if they own a computer and a modem. Yet the Communication Service Tax bill introduced in May 2016 would raise costs further, adding a nine percent tax on electronic communication services payable by the end user.
- Cybercafés are dominated by men and subject to raids by police targeting pornography and scams, making them ill-suited to advance the needs of women and girls. Yet mobile internet service is too slow to find information or complete forms. Sixty-seven percent of women and forty-eight percent of girls reported missing out on economic and professional opportunities because they lack quality internet service.

1 Olutosin Adebowale, "A Bridge to the World:" Internet Access for Rural Women and Girls in Nigeria," research paper, September 2016, on file with F eedom House.

Restrictions on Connectivity

There were no restrictions on connectivity to the internet or mobile networks during the coverage period.

The backbone connection to the international internet is decentralized, resulting in a climate of healthy competition with little government interference. The backbone infrastructure has improved significantly o er the last decade, with multiple players, including Phase 3, Glo 1, Suburban Telecom, Multilink and MTN, building fiber net orks that crisscross the country. There are three active Internet Exchange Points (IXPs), although only 37 ISPs, academic institutions, and telecommunications companies are connected to them, due to poor quality of service.[14]

13 Alex Hern, "Wikipedia's view of the World is written by the West," The Guardian, September 15, 2015, http://bit.ly/1KkakXs

14 Adeyemi Adepetun, "Why Internet exchange points suffer low patronage in Nigeria," The Guardian, February 10, 2015, http://bit.ly/1WlK7PX

ICT Market

The ICT market in Nigeria has expanded considerably over the past decade, with the number of licensed internet service providers (ISPs) rising from 18 in 2000 to 92 as of March 2016, though the growth of ISPs and FWA providers has slowed in recent years with the rise in mobile access.[15] Five privately owned GSM mobile phone operators also provide internet access: MTN, Globacom, Airtel, Etisalat, and NTEL, which began operations in February 2016 after acquiring the license of the defunct First National Operator, NITEL.[16] In January, MTN acquired Visafone, securing access to its 800MHz spectrum as a possible precursor to the launch of 4G LTE service.[17]

Cybercafés (or telecentres) are required to obtain licenses, but the large number of unlicensed cybercafes in operation suggest that the regulator has not enforced the requirement.[18]

Regulatory Bodies

The 2003 Nigerian Telecommunications Act vests regulatory responsibilities over the ICT sector in the Nigerian Communications Commission (NCC). Although the government nominates the NCC's nine-member board of commissioners, the regulator's decisions have been viewed as relatively independent. On August 4, 2015, Professor Umar Garba Danbatta was appointed as the regulator's new CEO and Executive Vice Chairman through a process that was viewed as fair, particularly considering his role as a leading academic and industry expert.[19]

During the coverage period, the NCC produced a report investigating the regulatory implications of the fledgling "o er-the-top" service sector, as it has been perceived as a threat to mainstream telecommunications services.[20]

Limits on Content

No blocking or filtering of online content was reported during the coverage period, though self-censorship has increased following an unprecedented spate of blogger arrests in the past year. In May 2016, digital activists successfully lobbied for the withdrawal of the Frivolous Petitions Prohibition Bill 2015, which threatened to penalize critical speech disseminated on social media.

Blocking and Filtering

Online media is generally free from restrictions in Nigeria, and to date, the authorities have not carried out any blocking or fil ering of content. YouTube, Facebook, Twitter, WhatsApp, and other communications platforms are freely available and among the most popular websites in the coun-

15 92 licenses were listed as valid while 113 ISPs were listed in lighter font, with license in need of renewal. See: Nigerian Communications Commission, "Internet Services," accessed March 21, 2016, http://bit.ly/1U0Khi4

16 Chima Akwaja, "NTEL Begins Number Reservation For 4G Subscribers," Leadership Newspaper, March 9, 2016, http://bit.ly/1Zjhcho

17 Chima Akwaja, "MTN acquires Visafone, NCC okays deal," Leadership, February 7, 2016, http://bit.ly/1RKaKdv

18 National Communications Commission, "Class License Register: Telecenter/Cybercafé Category," NCC, http://www.ncc.gov.ng/index.php?option=com_docman&task=doc_download&gid=718&Itemid=

19 NCC, "Executive Vice Chairman: Prof. Umar Garba Danbatta," http://bit.ly/29Okr22

20 National Communications Commission, "An Overview of Provision of over-the-top (OTT) services," http://bit.ly/1M0P0h3

try.[21] The complex nature of Nigeria's internet infrastructure makes it difficult o carry out systematic fil ering or censorship.

In the past few years, however, a few high-level government officials ha e called for a clampdown on social media in response to the growing influence f critical commentary on the internet,[22] sparking fears of impending online censorship.[23] Legislative developments in 2015 added weight to those fears. The Frivolous Petitions Prohibition Bill sought to penalize social media speech, though it was withdrawn in May 2016 (see Digital Activism). The Cybercrime Act, which was signed into law in May 2015, has been used to arrest bloggers for critical content in the past year (see Legal Environment and Prosecutions and Detentions for Online Content).

Content Removal

The government did not issue any takedown requests, or force legitimate content to be removed from the internet during the coverage period.

Media, Diversity, and Content Manipulation

Nigeria is home to a diverse blogosphere, which has become a source of reliable news for many users, and provides space for lengthy debate on a broad array of political and social issues. Popular blogging platforms include Blogger and WordPress. Diverse political viewpoints are represented on Nigerian websites and blogs. Some independent online media outlets faced a backlash under previous governments but have since begun to thrive economically.

Instead, observers have noted an increase in government efforts to dominate the online news landscape and potentially manipulate online content. A growing number of Twitter accounts of unknown provenance actively attack critical voices, which some fear may be government sponsored trolls.

The unprecedented number of bloggers and ordinary citizens arrested under the new Cybercrime Law has resulted in a palpable sense of increasing self-censorship, particularly among professional journalists who also publish content online (see Prosecutions and Detentions for Online Activities). Nigeria's LBGTI (lesbian, gay, bisexual, transgender, and intersex) community is marginalized, and many LGBTI individuals report feeling unsafe using their real names online, preferring to engage anonymously.[24]

Digital Activism

As active social media users, Nigerians have become prolific digital cam aigners, innovatively using social media and communications apps to call for social or political change. The savviness of Nige-

21 "Whatsapp is Nigerian Professional Social Media," Android Nigeria, September 24, 2014, http://bit.ly/22fauOs

22 On July 26, 2012, the President of the Senate of the Federal Republic of Nigeria, third in command after the president and vice president, called for a clampdown on the use of social media in Nigeria while speaking at a media retreat. Government representatives from the Oyo State House of Assembly made similar declarations in 2012. Phillip Eta, "Clamp down on Social Media now! 'It is now an avenue for abusing government,' – David Mark," *Daily Post,* July 28, 2012, http://bit.ly/1NeOwR3.

23 Hauwa Gambo, "Get ready, guys: Legislator wants law against "abuse" of social media," Naija*,* November 2, 2012, http://bit.ly/1GfDV8T.

24 *Silenced Voices, Threatened Lives: The Impact of Nigeria's Anti-LGBT Law on Freedom of Expression,* PEN America, June 2015, https://pen.org/Nigeria-anti-LGBT-Laws

ria's digital activists led to a significant in ernet freedom success story in the past year, namely, the defeat of the Frivolous Petitions Prohibition Bill 2015. Among its goals, the bill sought to constrain critical expression on social media.

The Nigerian online community mobilized to defeat the bill using the hashtag #NoToSocialMedia-Bill.[25] Significant digital activism inspi ed offline con ersations, rallies, and petitions, while a consortium of civil society organizations made up of Enough is Enough (EiE) Nigeria, Media Rights Agenda (MRA), and Paradigm Initiative Nigeria (PIN) filed a lawsuit o stop the bill at a Federal High Court in Lagos on March 21, 2016. In what was seen as a major victory for freedom of speech, the bill was withdrawn on May 17, 2016. In their deliberations, senators reflec ed comments made by citizens and advocacy organizations on social media, demonstrating the direct influence f digital activism.[26]

Violations of User Rights

Numerous bloggers, online journalists, and ordinary internet users were arrested for their online activities, an unprecedented jump over numbers documented in previous years. Many were prosecuted based on the cybercrime law passed in May 2015. Civil society groups challenged the constitutionality of several of the law's provisions in May 2016. Intimidation and reprisals for online expression became more common.

Legal Environment

Nigeria's 1999 constitution guarantees freedom of expression and the press. The implementation of Sharia (or Islamic) law in 12 northern states has not affected internet freedom in those regions to date. Nonetheless, libel is a criminal offense in Nigeria, including online, with the burden of proof resting on the defendant. Print media journalists covering sensitive issues such as official corruption and communal violence are regularly subject to criminal prosecution.

In May 2015, outgoing President Jonathan signed the Cybercrime (Prohibition, Prevention, etc.) Act 2015 into law, providing a long-awaited framework to combat the country's notorious cybercrime epidemic.[27] The law, however, includes provisions that violate citizens' rights to privacy (Section 26, see Surveillance, Privacy, and Anonymity) and freedom of expression. Duplicating existing libel laws, Section 24 of the law penalizes "cyberstalking" or messages that are "false, for the purpose of causing annoyance, inconvenience danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another" with up to three years in prison, a fine, or both. Section 26 penalizes distribution of "racist or xenophonic material to the public through a computer system or network" with up to fi e years in prison, a fine f up to NGN 10 million (US$50,000), or both.[28] A coalition of civil society organizations led by the digital rights organization, Paradigm Initiative Nigeria (PIN), filed a suit o challenge the constitutionality of Sections 24 and 36 of the cybercrime law in May 2016.[29]

25 Adebayo Ademola, "Nigerians say #NoToSocialMediaBill," Daily Trust, March 7, 2016, http://bit.ly/1YSIn28

26 "Nigerians protest at NASS over Anti-Social Media Bill," The Citizen Online, December 8, 2015, http://bit.ly/1P8VGnW

27 "Nigeria's President Jonathan Sign the Cybercrime Bill Into Law," *Techloy,* May 16, 2015, http://bit.ly/1RdeipQ.

28 Cybercrimes (Prohibition, Prevention, ETC) Act, 2015, http://bit.ly/1LHHhTh.

29 Paradigm Initiative Nigeria, "PIN calls for immediate release of arrested blogger and review of Cybercrime Law," press release, August 9, 2016, http://bit.ly/2eKLOHn

PIN has also led efforts to codify protections for internet freedom through the introduction of the draft Digital Rights and Freedom Bill in April 2015, which has made considerable headway since. Sponsored by lawmaker Chukwuemeka Ujam, the bill had passed a second reading at the House of Representatives,[30] and been referred to the Committees on Telecommunications and Human Rights for further deliberation as of mid-2016. If the bill reaches a third reading, it will be considered fully passed by the House, then require concurrence by the Senate and the President's assent before becoming law.

Prosecutions and Detentions for Online Activities

The number of bloggers, online journalists, and ordinary users arrested for their online activities increased dramatically in the past year, many under Section 24 of the cybercrime law. Four prosecutions were documented between June 2015 and May 2016, while several other arrests were reported in late 2016, after the coverage period of this report.

In August 2015, Seun Oloketuyi, a blogger for the news website *Naija Hottest Gist*, was charged under the Cybercrime Act for publishing a story about an alleged extramarital affair between the managing director of Fidelity Bank and an employee.[31] Oloketuyi was remanded in prison and granted bail of NGN 3 million (US$15,000 in 2015).[32] Another popular blogger, Chris Kehinde Nwandu, was also arraigned for sharing the story on Facebook. Held for 21 days before being granted bail,[33] he was charged with cyberstalking and being an accomplice to defamation.[34] Nwandu's case was dropped in June 2016.[35]

In September 2015, blogger Emmanuel Ojo was arrested for a Facebook post that accused the wife of the Ogun state governor of laundering money.[36] He was granted bail after three days. Ojo later sued the police and chief security officer o the governor demanding N130 million (US$ 530,000) in damages. However, in a move that surprised observers, the blogger withdrew his suit after three weeks and sent the governor a written apology.[37] He later fled Nigeria eporting threats from "powerful people" in relation to the incident (see Intimidation and Violence).[38]

Blogger Desmond Ike Chima was arrested in October 2015 for publishing a story about an alleged affair between the managing director of the United Bank for Africa and a female actor, in a case similar to Seun Oloketuyi's. He was charged with cyberstalking under Section 24 of the Cybercrime Act

30 Paradigm Initiative Nigeria, "Digital Rights And Freedom Bill Passes Second Reading," press release, June 23, 2016, https://pinigeria.org/digital-rights-and-freedom-bill-passes-second-reading/

31 Nicholas Ibekwe, "Nigieran blogger accused of defaming Fidelity bank MD gets bail," Premium Times, September 1, 2015, http://bit.ly/1JEkS6w

32 "Court grants blogger N3 million bail," Invest Advocate, September 1, 2015, http://investadvocate.com.ng/2015/09/02/court-grants-blogger-n3-million-bail/

33 Nwandu later told the audience at a Stakeholders' Roundtable on the Digital Rights and Freedom Bill, hosted by Paradigm Initiative Nigeria, that he was actually held for 21 days, and not 13 days as widely reported. "BREAKING: Popular blogger Chris Kehinde Nwandu (CKN) granted bail," News Express, September 15, 2015, http://bit.ly/2eKHKqF

34 Azuka Jebose, "Journalism is not a crime: Free Chris Kehinde Nwandum" News24, September 8, 2015, http://bit.ly/2fHcBsX; Ameh Comrade Godwin, "Popular blogger, CKN arraigned in prison custody over false publication," Daily Post, September 5, 2015, http://bit.ly/2fpiJEN

35 "Court strikes out defamation case," CKN Nigeria, June 30, 2016, http://bit.ly/2frs9xP

36 Anike Nwodo, "Blogger Begs Governor Amosun For Forgiveness," Naij, November 2015, http://bit.ly/2a328UX

37 Anike Nwodo, "Blogger Begs Governor Amosun For Forgiveness," Naij, November 2015, http://bit.ly/2a328UX

38 "Falana, other activists slam Nigerian govt for prosecuting man who named dog Buhari," Naija Loaded, August 27, 2016, http://www.naijaloaded.com.ng/2016/08/27/falana-activists-slam-nigerian-govt-prosecuting-man-named-dog-buhari/

and spent six months in prison because he was unable to meet bail.[39] After civil society groups petitioned on his behalf, the charge was dropped and he was released in April 2016.[40]

Several other bloggers and online journalists have been arrested since the end of this report's coverage period. Abubakar Usman was arrested and held for two days in August 2016 for a report accusing the Economic and Financial Crimes Commission of corruption.[41] Musa Azare was also arrested by police in August after he allegedly criticized the Bauchi state governor on social media, though the governor himself demanded Azare's release, citing his support for freedom of expression.[42] In September 2016, blogger Jamil Mabai was arrested for criticizing the state governor's rationale for purchasing coffins on witter.[43]

Surveillance, Privacy, and Anonymity

Thus far, there has been no evidence that the Nigerian authorities proactively monitor internet and mobile phone communications, but many online journalists have long suspected that they are being monitored by the state. Several legal provisions may allow the government to conduct surveillance without respect for the Necessary and Proportionate Principles, international guidelines that apply human rights law to monitoring technologies.[44]

The cybercrime law enacted in May 2015 requires service providers to retain user data and intercept electronic communications.[45] Under Section 38 of the law, providers are required to "keep all traffic data and subscriber information…for a period of two years" and comply with requests from law enforcement agencies to access this data.[46] The law implies a degree of judicial oversight over these requests, but the procedure involved is unclear.[47]

Guidelines for the Provision of Internet Service published by the regulator in 2013 also require ISPs to cooperate with law enforcement and regulatory agencies in providing "any service-related information… including information regarding particular users and the content of their communications" during investigations of cybercrime or other illegal activity.[48] The guidelines do not include oversight of that cooperation, introducing scope for abuse. The guidelines also stipulate that ISPs must retain user data and "the content of user messages or routing data" for at least 12 months.[49]

39 "Another blogger, Desmond Ike-Chima, remanded in Ikoyi prison," Integrity Reporters, November 2, 2015, http://integrityreporters.com/news/another-blogger-desmond-ike-chima-remanded-in-ikoyi-prison/

40 "Falana, other activists slam Nigerian govt for prosecuting man who named dog Buhari," Naija Loaded, August 27, 2016.

41 Abubakar Usman, "The true story of my arrest by EFCC," Daily Post, August 18, 2016, http://bit.ly/2fpmydo

42 "Blogger and journalist Musa Azare arrested and released for criticizing Bauchi state government," Bella Naija, August 22, 2016, http://bit.ly/2fnO74g

43 "Another blogger arrested for criticizing Katsina governor's purchase of coffins for mosques" Nigeria Today, September 21, 2016, http://bit.ly/2eACDvi; "Photo: Outrage as Katsina Gov Masari allegedly buys 30 coffins at N40k & distribu es them to mosques," Lailas blog, September 6, 2016, http://www.lailasblog.com/2016/09/photooutrage-as-katsina-governor-masari.html

44 Necessary and Proportionate principles: https://necessaryandproportionate.org/about

45 Low Okezie, "Nigeria's President Jonathan Sign the Cybercrime Bill Into Law," Tech Loy, May 16, 2015, http://techloy.com/2015/05/16/nigerias-president-jonathan-signs-the-cybercrime-bill-into-law/

46 Cybercrimes (Prohibition, Prevention, ETC) Act, 2015, Section 38.

47 According to Section 38(4): "Any data retained, processed or retrieved by the service provider at the request of any law enforcement agency under this Act shall not be utilized except for legitimate purposes as may be provided for under this Act, any other legislation, regulation ***or*** by an order of a court of competent jurisdiction" (emphasis added). Cybercrimes (Prohibition, Prevention, ETC) Act, 2015, http://bit.ly/1LHHhTh.

48 Nigerian Communications Commission, "Guidelines for the Provision of Internet Service," 2, http://bit.ly/1hVbmA2.

49 "Guidelines for the Provision of Internet Service Published by the Nigerian Communications Commission," 3.

Data localization is mandated under the Guidelines for Nigerian Content Development in Information and Communications Technology, issued by the Nigerian National Information Technology Development Agency (NITDA) in 2013. The guidelines require ICT companies to "[h]ost all subscriber and consumer data locally within the country."[50] The stated aim was to boost local content and ICT development, but the requirement risks compromising user privacy and security, given the absence of adequate data protection laws.[51] The extent to which the guidelines have been enforced remained unclear as of 2016, as there have been no reports that international ICT companies have been compelled to comply.

A draft Lawful Interception of Communications Regulation introduced by the communications regulator in February 2013 is still under discussion.[52] If implemented, the regulation would enable interception both with and without a warrant under different circumstances, and require mobile phone companies to store voice and data communications for three years. It also directs telecommunications licensees to "provide the National Security Adviser and the State Security Service with the key, code, or access to…Protected or Encrypted Communication" on demand.[53] Critics said it bypassed the legislative process and threatens to citizens' privacy rights, since it lacks judicial safeguards against abuse or opportunities for redress.[54]

News of the government's acquisition of mass surveillance equipment over the past few years has deepened suspicions of surveillance. In July 2015, leaked emails from the Italian surveillance fi m Hacking Team revealed that the company had a contract with the Bayelsa state government that expired in November 2013.[55] The active period of the contract from 2012 to 2013 coincides with the state governor's crackdown on so-called "rumormongering" online.[56] Citizen Lab research from 2014 also found a FinFisher "Command and Control" server located on a private ISP in Nigeria.[57] As of October 2016, the extent to which that surveillance system is operational is not known.[58]

The government's intent to enhance its surveillance capabilities is indicated by the federal government's draft budget summary, which allocated NGN 15.4 billion (US $54.6 million) for internet and mobile surveillance in 2016, more than in previous years.[59] The 2016 budget for the National Security Adviser and allied agencies made provisions for the purchase of technologies including "Project

50 Section 12.1.4, Guidelines for Nigerian Content Development in Information and Communications Technology (ICT) (2013), http://bit.ly/2ftclca

51 "Anupam Chander and Uyen P. Le, "Data Nationalism," Emory Law Journal, Vol 64, 2015, http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf

52 Nigeria Communications Commission, "Draft Lawful Interception of Communication Regulations," http://bit.ly/1du7UKO; Ojo Madueke, "Revealed: SSS, Police Have Powers to Tap Phone Lines," This Day Live, January 30, 2013, http://bit.ly/1hH90GJ; Clement Ejiofor, "Mind That Conversation: Security Operatives To Tap Phones, Track E-mail," Naij, February 5, 2013, http://bit.ly/1VUWPsL; Ken Nwogbo, "SSS, Police Get Powers to Tap Phones," Nigeria Communications Week, January 29, 2013, http://bit.ly/1RdfTfd.

53 Nigeria Communications Commission, "Draft Lawful Interception of Communication Regulations."

54 Kunle Azeez, "Concerns over proposed lawful interception law," National Mirror Online, May 23, 2013, http://bit.ly/1kARPa1; Katie Collins, "Nigeria embarks on mobile phone surveillance project," Wired UK, September 4, 2013, http://bit.ly/1PvCpI2; John Dada and Theresa Tafida, "Online su veillance: Public concerns ignored in Nigeria," in *Communications Surveillance in the digital age 2014*, Global Information Society Watch, http://bit.ly/1PjVGXy.

55 Ibukun Taiwo, "TL;DR: The Curious Case of Hacking Team And A Southern Nigerian State," *Tech Cabal*, July 17, 2015, http://bit.ly/1J8RYg4

56 Ogala Emmanual, "Nigeria: Hacking Team, Bayelsa's Govt's Internet Surveillance Contractor, Hacked," *Premium Times,* July 6, 2015, http://bit.ly/1GfmXYj

57 "Command and control" server communicates with malware that can be used for surveillance. Morgan Marquis-Boire et al., *For Their Eyes Only: The Commercialization of Digital Spying*, Citizen Lab, April 30, 2013, http://bit.ly/1amNwJ1

58 When the author of this report asked for the state of the surveillance system during the Internet Freedom Forum 2016, the representative of the National Security Adviser said he was not aware of any such project.

59 Federal Government of Nigeria, 2016 Budget Proposal, http://bit.ly/1Rept0E

All Eye, Surveillance Equipment, IMSI catcher, Intel Profilin , Enhanced Field Communication Systems, Open Source Internet Monitoring System and Rapid Intervention Vehicles," among others.[60] In mid-2016, it was not clear if those purchases had taken place, or for what purpose. Government officials frequently assert the need for technologies to fight the Bo o Haram terrorist group.

SIM card registration requirements instituted in June 2009 threaten users' rights to anonymous communication and privacy,[61] particularly in the absence of a data protection law.[62] User registration is also required in cybercafes. An October 2013 directive from the regulator requires cybercafés to "maintain an up-to-date database of subscribers and users, including their full names, physical addresses, passport photos, and telephone numbers."[63] Under Section 7 of the cybercrime law, cybercafés must make their registers "available to law enforcement personnel whenever needed," with no clear requirement for judicial oversight.[64]

Intimidation and Violence

Unlike print and broadcast journalists, online journalists and internet users have not been subject to significant extralegal harassment, violence, or th eats for their activities, though intimidation and reprisals for online expression have become more common.

Following his arrest for "cyberstalking" and subsequent release in September 2015 (see Prosecutions and Detentions for Online Activities), blogger Emmanuel Ojo fled Nigeria, eportedly due to threats he received in connection with the charge against him.[65] In January 2016, Kaduna State University suspended lecturer John Danfulani after he criticized the Nigerian ruling party and its leaders on Facebook.[66] In a separate incident, Ruqaiyyat Tijjani Usman, a staff member of the Nasarawa State Ministry of Justice, was dismissed in February 2016 for posting critical comments of the government's handling of a labor dispute on Facebook.[67]

Technical Attacks

Cyberattacks have become less common in Nigeria in the past year, although the website of an online news platform, Naij.com, was subject to cyberattacks in July 2015. The source of the attacks remains unknown.[68]

60 Office f the National Security Adviser, "2016 FGN Budget Proposal," accessed on July 18, 2016, http://bit.ly/nsa2016

61 Nigerian Communications Commission and National Identity Management Commission, "Design, Development and Delivery of SIM Card Registration Solution," June 15, 2009, http://bit.ly/1clf91H

62 F. Franklin Akinsuyi, "Data Protection & Privacy Laws Nigeria, A Trillion Dollar Opportunity," Linkedin, April 15, 2015, http://bit.ly/1RdgvBs

63 "NCC orders cyber cafes to register users," Telecompaper, October 22, 2013, http://bit.ly/1LPOk7w

64 Cybercrimes (Prohibition, Prevention, ETC) Act, 2015, Section 7.

65 "Falana, other activists slam Nigerian govt for prosecuting man who named dog Buhari," Naija Loaded, August 27, 2016.

66 Mohammed Lere, "Kaduna University suspends lecturer over Facebook 'hate speech,'" Premium Times, January 27, 2016, http://bit.ly/250Dqc9

67 Donatus Nadi, "Nasarawa: NLC Threatens To Shutdown State Over Sack Of Female Worker For Facebook Comment," February 28, 2016, Leadership, http://bit.ly/1Uu1A9V

68 Clement Ejiofor, "From Cyberattacks on Naij.com to Cyber terrorism," Naij.com, http://bit.ly/1nJEfEm

Freedom House

Pakistan

	2015	2016
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	20	18
Limits on Content (0-35)	20	20
Violations of User Rights (0-40)	29	31
TOTAL* (0-100)	**69**	**69**

* 0=most free, 100=least free

Population:	**188.9 million**
Internet Penetration 2015 (ITU):	**18 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- The National Assembly approved the Prevention of Electronic Crimes Act, including clauses which would enable censorship, surveillance, and rights violations (see **Legal Environment**).
- In January 2016, YouTube was unblocked for the fi st time since 2012, redirecting users to a local version, YouTube PK (see **Blocking and Filtering**).
- Antiterrorism courts sentenced two individuals to 13 years in prison each in separate cases involving charges of promoting religious or sectarian hatred on Facebook (see **Prosecutions and Detentions for Online Activities**).
- Investigators charged a man in Peshawar with violating "privacy of information" and "damage to information systems" based on Twitter posts he wrote about a judge's relatives in September 2015 (see **Prosecutions and Detentions for Online Activities**).

Introduction

Internet freedom remained repressive in Pakistan in 2015-16, where the unblocking of YouTube was overshadowed by harsh punishments for online speech.

The Prevention of Electronic Crimes Bill, draft cybercrime legislation with scope to suppress free expression, came under intense criticism in 2015, in Pakistan and from international rights organizations and the United Nations Special Rapporteur on freedom of opinion and expression. On April 13, 2016, however, an amended bill that retained many problematic clauses was approved by the National Assembly. The Senate approved the bill outside the coverage period of this report, and it was adopted in August.[1]

New legal measures are particularly concerning in light of harsh punishments for online expression handed down in 2015 and 2016. Antiterrorism courts sentenced two men in separate cases to 13 years imprisonment for allegedly distributing "hateful" or "sectarian" material about religion on Facebook. Separately, individuals communicating online were charged under the 2002 Electronic Transactions Ordinance, an early ecommerce law, including a member of the Pakistan Tehreek-i-Insaf party who wrote about a judge on Twitter.

In a positive development, a local version of the popular video-sharing platform YouTube was made available for the fi st time since 2012, when the entire platform was blocked for hosting the anti-Islamic video, "The Innocence of Muslims." Users feared YouTube PK would be subject to stricter censorship than its international counterpart. Separately, Blackberry negotiated to continue offering encrypted messaging services in Pakistan after the government warned them they would need to shut down operations if they did not grant officials access o the content being exchanged through their servers.

Obstacles to Access

Internet penetration is limited in Pakistan by a lack of resources and infrastructure, but mobile internet access is increasing following the recent launch of faster 3G and 4G service. However, Pakistani authorities frequently disable mobile internet access during times of perceived political or religious sensitivity.

Availability and Ease of Access

The International Telecommunication Union reported internet penetration at 18 percent in 2015, based on figu es from the Pakistan Bureau of Statistics.[2] Pakistan's telecommunications regulator reported mobile penetration at 73 percent.[3] Internet penetration is expected to increase with the recent launch of 3G and 4G technology (see ICT Market). While the cost of internet use has fallen considerably in the last few years,[4] with prices around US$12 a month for a broadband package in 2015, access remains out of reach for the majority of the population.

1 Reuters, "Pakistan passes controversial cyber-crime law," August 12, 2016, http://www.reuters.com/article/us-pakistan-internet-idUSKCN10N0ST.

2 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1cblxxY.

3 "Cellular subscribers reach 132.33m with 73.5pc record penetration," *Pakistan Today*, February 10, 2014,http://bit.ly/1Nvtn8n.

4 "Average monthly Internet cost in Pakistan low," *Daily Times*, October 3, 2015, http://bit.ly/1N4iCa3.

Broadband subscriptions, based on DSL—which uses existing telephone networks—or wireless Wi-Max technology, are concentrated in urban areas. Most remote areas lack broadband, and a large number of users depend on slow dial-up connections or EDGE, an early mobile internet technology. In such areas, meaningful online activity like multimedia training can be challenging, though faster 3G and 4G networks are making inroads, albeit at a slow pace. Several parts of western areas of Pakistan lack internet access, partly because of underdevelopment and partly because of ongoing conflict. Acco ding to one study, more than 75 percent of tribal areas and 60 percent of Balochistan province lacked fiber optic connections in 2013. [5]

Low literacy, difficult economic conditions, and cultural esistance have limited the proliferation of ICTs in Pakistan.[6] Though internet access is gradually increasing among girls and women, online harassment unfortunately discourages greater utilization of ICTs by women, especially those under 30. Reports of criminal harassment on social media are frequent (see Intimidation and Violence).

Increasing security measures mean that users must register their fingerprints along with other ide - tifying information when applying for broadband internet packages and mobile service. This has worrying implications for human rights activists and others who rely on anonymous internet access, and may discourage some from seeking home service. Unregistered phones were subject to disconnection in 2015 (see Surveillance, Privacy, and Anonymity).

Restrictions on Connectivity

The predominantly state-owned Pakistan Telecommunication Company Limited (PTCL) controls the country's largest internet exchange point, Pakistan Internet Exchange (PIE), which has three main nodes—in Karachi, Islamabad, and Lahore—and 42 smaller nodes nationwide. PIE operated the nation's sole internet backbone until 2009, when additional bandwidth was offered by TransWorld Associates on its private fibe -optic cable, TW1.[7]

PTCL also controls access to the three international undersea fibe -optic cables: SEA-ME-WE 3 and SEA-ME-WE 4 connect Southeast Asia, the Middle East, and Western Europe; and I-ME-WE links India, the Middle East and Western Europe.[8] The company signed an agreement to build the fourth cable, considered to be one of the world's largest, in 2014. The AAE-1 cable, projected to be completed by the end of 2016, will connect countries in Asia, Africa, and Europe.[9]

Damage to these cables did not cause widespread access disruptions during the coverage period, as it has done in the past.[10] In early 2015, villages in the northern Drosh Valley faced internet and telephone disconnection because of damage to the open main cable.[11] As in previous years, however, Pakistan faced electricity shortages in 2015 and 2016, especially when demand peaked during the

5 Zakir Syed, "Overcoming the Digital Divide: The Need for Modern Telecommunication Infrastructure in the Federally Administered Tribal Areas (FATA) of Pakistan," *Tigah Journal* (2013) http://bit.ly/1LulYiV.

6 Arzak Khan, "Gender Dimensions of the Information Communication Technologies for Development," (Karlstad: University of Karlstad Press, 2011) doi: http://dx.doi.org/10.2139/ssrn.1829989.

7 OpenNet Initiative, "Country Profile— akistan," August 6, 2012, http://bit.ly/1LDXNEX.

8 "PTCL Expects 20pc Growth with Launch of IMEWE Cable: Official" *The News*, December 22, 2010, http://bit.ly/1huHRXs.

9 "PTCL to build largest int'l submarine cable consortium system," *Daily Times*, January 30, 2014, http://bit.ly/1L4dxO6; "AAE-1 subsea cable lands at Crete", *Capacity Media, April 19, 2016, http://bit.ly/1qXbCFs*

10 Farooq Baloch, "Undersea Cable Cut Affects 50% of Pakistan's Internet Traffic" *Express Tribune*, March 27, 2013, http://bit.ly/1FWOnSV.

11 Gul Hamaad Farooqi, "Chitral villages lack phone, internet facilities," *The Nation*, February 10, 2015, http://bit.ly/1GAOiPi.

summer months.

Security considerations continued to intrude on telecommunication services. In 2015 and 2016, as in previous years, the government suspended cellular services on some religious and national holidays on grounds that terrorists could use the networks to coordinate violent acts. In October 2015, for example, the Interior Minister directed cellular service operators to block service in parts of the country during the religious holiday Eid-ul-Fitr.[12] A 2015 report highlighted that shutting down cellular services places citizens at risk, rather than protect them. Both the state and telecommunications providers have lost millions in revenue during past shutdowns, according to the report.[13]

Orders to suspend service cite Section 54 of the 1996 Pakistan Telecommunications Act, though this should only apply during a state of emergency. The use of the law to support service suspension orders has been challenged in the Sindh High Court by Telenor Pakistan and a doctor who reported being unable to communicate with patients during a shutdown, among others. In 2016, the court had yet to issue a decision in those cases, which date from 2012.[14]

ICT Market

In the latest available data, the Internet Service Providers Association of Pakistan reported 50 ISPs operational in Pakistan as of October 2014; 10 of those provide DSL services.[15] The government regulator, the Pakistan Telecommunication Authority (PTA), exerts significant cont ol over internet and mobile providers through a bureaucratic process that includes hefty licensing fees.[16]

The predominantly-state-owned Pakistan Telecommunication Company Limited (PTCL) controls 60 percent of the broadband market. [17] In 2012, an antimonopoly inquiry said the prices it charged other companies to use its infrastructure had forced private DSL operators to leave the market, which PTCL denied.[18]

After several years delay, Pakistan finally int oduced internet-capable 3G mobile network and 4G spectrum, in 2014. The 3G spectrum auction was won by four foreign-owned companies, Mobilink, Zong, Telenor, and Ufone; Zong also won 4G spectrum. Pakistan secured US$903 million and US$210 million from the 3G and 4G spectrum auctions, respectively. These networks will provide faster internet services to consumers in Pakistan.[19] Although so far limited to urban centers, mobile companies report that they are rapidly expanding the networks.[20]

Internet cafes do not require a license to operate, and opening one is relatively easy.[21] Child rights

12 "Mobile phones services to be suspended in parts of country: Malik" *Dawn*, October 23, 2015, http://bit.ly/28Ifl6

13 "Mobile service suspension: A cause of panic and massive socio-economic loss". *Dawn*, October 23, 2015 http://www.dawn.com/news/1214782; Institute for Human Rights and Business, "Security v Access: The Impact of Mobile Network Shutdowns, Case Study Telenor Pakistan," September 2015, http://www.global.asc.upenn.edu/publications/security-v-access-the-impact-of-mobile-network-shutdowns-case-study-telenor-pakistan/.

14 "Security v Access: The Impact of Mobile Network Shutdowns, Case Study Telenor Pakistan."

15 Internet Service Providers Association of Pakistan, http://www.ispak.pk/.

16 Pakistan Telecommunication Authority, "Functions and Responsibilities," December 24, 2004, http://bit.ly/1OpRm9c.

17 Adam Senft, et al., *O Pakistan, We Stand on Guard for Thee: An Analysis of Canada-based Net sweeper's Role in Pakistan's Censorship Regime,* Citizen Lab, June 20, 2013, https://citizenlab.org/2013/06/o-pakistan/.

18 Iftikhar A. Khan, "PTCL forces half of DSL operators to quit," *Dawn*, June 20, 2012, http://bit.ly/1VJTOLT.

19 Sohail Iqbal Bhatti, "$1.1 billion raised from 3G, 4G auction," *Dawn*, April 24, 2014, http://www.dawn.com/news/1101760.

20 "In demand: 3G user base expanding, market surges forward," *The Express Tribune*, September 16, 2014, http://bit.ly/1L4ebv8.

21 Sehrish Wasif, "Dens of sleaze," *Express Tribune*, July 22, 2010, http://tribune.com.pk/story/29455/dens-of-sleaze/.

groups have argued that cafes should be regulated to prevent inappropriate access to pornography and gambling sites.[22]

Regulatory Bodies

The PTA is the regulatory body for the internet and mobile industry, and international free expression groups and experts have serious reservations about its openness and independence.[23] The prime minister appoints the chair and members of the three-person authority, which reports to the Ministry of Information Technology and Telecommunication.[24] The repeated failure to make new appointments since 2013 have further undermined the PTA's reputation. In March 2015, the PTA formally took responsibility for internet content management (see Blocking and Filtering).

In December 2015, Pakistan's Economic Coordination Council approved the Government of Pakistan's Telecommunications Policy 2015. [25] The Policy outlines and addresses issues faced by some network operators and also reinforces the PTA's authority to "monitor and manage content" online.[26] However, the Telecoms Policy does not address concerns from the telecoms industry in Pakistan in regards to the suspension of cellular services during religious or national holidays for security reasons. The Policy has been criticized for not addressing obstacles to greater internet penetration in a manner that offers fair pricing and choices for the consumer.[28]

Limits on Content

The Prevention of Electronic Crimes Act authorizes the PTA to undertake content management. In January 2016, YouTube was unblocked, but users in Pakistan can only visit a version subject to local laws restricting content. Other platforms, media, and communication tools are popular and contribute to a vibrant online space.

Blocking and Filtering

In April 2016, the National Assembly approved the Prevention of Electronic Crimes Act (see Legal Environment). It was later approved by the Senate, and passed in August. Section 37 authorizes the PTA to "issue directions for removal or blocking of access of any information through any information system" it considers necessary for "the glory of Islam or the integrity, security or defense of Pakistan… public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence under this Act."[27]

The task of ordering blocks was formerly undertaken by the Inter-Ministerial Committee for the Evaluation of Web Sites (IMCEW), comprised of representatives from PTA and the government, along

22 Qaiser Butt, "Dirty business in sequestered cubicles," The Express Tribune, February 16, 2015, http://bit.ly/1L4ekif.

23 Article 19, "Pakistan: Telecommunications (Re-organization) Act," legal analysis, February 2, 2012, http://bit.ly/1Pl5OOR.

24 Pakistan Telecommunication Authority, "Pakistan Telecommunication (Re-organization) Act 1996," *The Gazette of Pakistan,* October 17, 1996, http://bit.ly/16sASJI.

25 "ECC approves Telecom Policy 2015", *Pakistan Today*, December 12, 2015 http://bit.ly/1QTPqBo.

26 "An Overview of Telecom Policy 2015", Propakistani, December 12, 2015, http://propakistani.pk/2015/12/12/an-overview-of-telecom-policy-2015/

27 "Pak Telecom policy 2015 – another step forward for censorship" Digital Rights Foundation, February 10, 2016 http://bit.ly/1QTQAg9; http://digitalrightsfoundation.pk/wp-content/uploads/2016/08/PECB2016.pdf

with "men from the Ministry of Religious Affairs, the Inter-Services Intelligence, and Military Intelligence."[28] In March 2015, at the request of the Ministry of Information,[29] Prime Minister Sharif disbanded the Inter-Ministerial Committee and authorized the PTA to undertake content management.[30] The Prevention of Electronic Crimes Act provides the legal authority for this activity.

The Telecommunications Policy approved in December 2015 (see Regulatory Bodies) utilized similar language. Section 9.8.3 states that the PTA will be enabled to "monitor and manage content including any blasphemous and pornographic material in conflict with the principles f Islamic way of life as reflec ed in the Objectives Resolution and Article 31 of the Constitution" as well as material that is considered to be "detrimental to national security, or any other category stipulated in any other law."[28]

Overly broad provisions in the 1996 Pakistan Telecommunications Act already support censorship for the protection of national security or religious reasons.[31] Section 99 of the penal code allows the government to restrict information that might be prejudicial to the national interest, to justify fil ering antimilitary, blasphemous, or antistate content.[32] Critics believe these issues can serve as cover for politically motivated censorship of dissenting voices. Information perceived as damaging to the image of the military or top politicians, for example, is also targeted.

Historically, blocking orders have directed ISPs and backbone providers to implement manual blocks on individual URLs or IP addresses, their compliance ensured by licensing conditions.[33] Since 2012, successive administrations have sought to introduce technical fil ering.[34] The National ICT Research and Development Fund initially requested that companies develop nationwide blocking technology to "handle a block list of up to 50 million URLs,"[35] though the status of that project was left in doubt after widespread civil society protests.[36] News reports in 2013 and 2014 said PTA and government officials ere still pursuing fil ering solutions.[37] In 2013, the University of Toronto-based research group Citizen Lab reported that technology developed by the Canadian company Netsweeper was already fil ering political and social content at the national level on the PTCL network.[38] "In addition to using Netsweeper technology to block websites, ISPs also use other less transparent methods,

28 "Banistan: Why Is YouTube Still Blocked In Pakistan?" *New Yorker*, August 7, 2013, http://nyr.kr/1WS2dtH.

29 Mehtab Haider, "PTA may be empowered to undertake Internet content management," *The News*, February 22, 2015, http://bit.ly/1R2KLyZ.

30 Mehtab Haider, "PTA given powers for content management on internet," *The News*, March 21, 2015, http://bit.ly/1ED2NjN.

31 Article 19, "Pakistan: Telecommunications (Re-organization) Act."

32 "Pakistan: Code of Criminal Procedure," available at the Organization for Economic Co-operation and Development, accessed August 2013, http://bit.ly/1R2Kyfg.

33 PTA Act 1996, art. 23.

34 Danny O'Brien, "Pakistan's Excessive Internet Censorship Plans," Committee to Protect Journalists (blog), March 1, 2012, https://cpj.org/x/4995.

35 National ICT Research and Development Fund, "Request for Proposal: National URL Filtering and Blocking System," accessed August 2012, http://bit.ly/1QeBBiD; "PTA determined to block websites with 'objectionable' content," *The Express Tribune*, March 9, 2012, http://bit.ly/xEND9P.

36 Shahbaz Rana, "IT Ministry Shelves Plan to Install Massive URL Blocking System," *The Express Tribune*, March 19, 2012, http://bit.ly/1MilIIQ.

37 Anwer Abbas, "PTA, IT Ministry at Odds Over Internet Censorship System," *Pakistan Today*, January 3, 2013, http://bit.ly/1N47IkG; ApurvaChaudhary, "Pakistan To Unblock YouTube After Building Filtering Mechanism," *Medianama*, January 10, 2013, http://bit.ly/TMmcvh; Abdul Quayyum Khan Kundi, "The Saga of YouTube Ban," Pakistan Press Foundation, January 2, 2013, http://bit.ly/1bhpMEP; "Ministry Wants Treaty, Law to Block Blasphemous Content," *The News*, March 28, 2013, http://bit.ly/16JP6yo. Associated Press of Pakistan, "IT Minister plans to ban 'objectionable content' across entire internet," *The Express Tribune*, http://bit.ly/1VJApFx.

38 Senft, et al., *O Pakistan, We Stand on Guard for Thee: An Analysis of Canada-based Net sweeper's Role in Pakistan's Censorship Regime.*

such as DNS tampering," Citizen Lab noted. [39] The report highlighted the lack of transparency and accountability surrounding censorship in Pakistan.

The same lack of transparency extends to the content affected by censorship, which is often inconsistent based on location or across ISPs.[40] There are no published guidelines outlining why content is blocked or how to appeal. Individuals and groups can also initiate censorship by petitioning courts to enact moral bans on online or traditional media content.[41] In April 2016, attempts to access the website of the French satirical magazine *Charlie Hebdo* from within Pakistan prompted the message, "Surf Safely! The website is not accessible. The site you are trying to access contains content that is prohibited for viewership within Pakistan as per the law." The magazine is known for mocking religion and was attacked by extremists in January 2015.

Blocking frequently targets social media and communication apps. In 2012, the government blocked YouTube in response to the anti-Islamic video "The Innocence of Muslims."[42] The site was briefly u -blocked in December 2012 until a broadcast journalist demonstrated that the offensive clip was still available, [43] and it remained off limits for users in Pakistan until this year. In January 2016, a localized version of the platform, YouTube PK, became accessible.[44] A government statement about the new platform said that "Google has provided an online web process through which requests to blocking access of offending material can be made by the PTA to Google directly." YouTube said that the company may remove content from local versions of its platforms based on local laws after a thorough review.[45]

No other applications were subject to deliberate blocking at the domain level during the coverage period. Pakistani users of WhatsApp, the widely-used instant-messaging service owned by Facebook, could not connect to the service's iOS or Android apps for a brief period on May 18, 2016, but it is not known what caused the outage.[46]

Censorship targeting pornography can affect access to health information and other legitimate content like Scarleteen, a U.S.-based sex education website for teenagers.[47] In January 2016, the PTA informed internet service providers that 429,343 websites must be blocked at the domain level,[48] in an attempt to prevent access to pornographic sites. The manner in which the list of websites has been vetted to avoid non-pornographic websites from being blocked has not been made clear to the public.

Political dissent and secessionist movements in areas including Baluchistan and Sindh province, where a Sindhi nationalist movement advocates for political divisions along ethnic lines, is among the nation's most systematically censored content.[49] In 2013, the PTA requested that ISPs block the

39 DNS tampering intercepts the user's request to visit a functioning website and returns an error message.

40 OpenNet Initiative, "Country Profile— akistan," 2012.

41 "Internet censorship: Court asked to ban inappropriate content," *The Express Tribune*, June 14, 2011, http://bit.ly/jOCZFP.

42 Jon Boone, "Dissenting voices silenced in Pakistan's war of the web," *The Guardian*, February 18, 2015, http://gu.com/p/45yba/stw.

43 Umar Farooq, "Pakistan Courts YouTube Comeback," *Wall Street Journal,* August 14, 2013, http://on.wsj.com/1jiCfkv.

44 Requests to access Youtube.com redirect users within Pakistan to youtube.com/?hl=ur&gl=PK

45 "Pakistan lifts three-year YouTube ban with censor-friendly version", *Newsweek*, January 19, 2016 http://bit.ly/1WSumCK.

46 "After Brief Outage, Whatsapp Services Restored in Pakistan", ProPakistani, May 18, 2016, http://bit.ly/28IeLoN

47 "Pakistan blocks access to teen sex-ed site," *The Express Tribune*, March 20, 2012, http://bit.ly/1QeD0pE.

48 " Pakistan to block over 400,000 porn websites", *The Express Tribune*, January 26, 2016 http://bit.ly/1TIIsGk.

49 "PTA letter blocking websites April 25, 06," *Pakistan 451* (blog), April 27, 2006, http://bit.ly/1Lmn18M.

international website IMDb (Internet Movie Database), an order they reversed after two days.[50] Analysts said the apparent ban—which attracted widespread criticism on social media—was related to the upcoming release of a British short film, The Line of Freedom," a fictional depiction f Pakistani security agencies abducting Baloch separatists. [51] The IMDb page documenting "The Line of Freedom" remained inaccessible for longer, but it was also ultimately unblocked.[52]

Authorities also target users seeking to access blocked content. In 2011, the PTA sent a legal notice to all ISPs in the country urging them to report customers using encryption and virtual private networks (VPNs)[53] —technology that allows internet users to interact online undetected and access blocked websites—to curb communication between terrorists.[54] International and civil society organizations in Pakistan protested,[55] and the tools were widely used to access YouTube when it was blocked.[56] Two of the best-known services, Spotflux and HotSpot VPN, became inaccessible in 2014, and Spotflux said the go ernment had actively blocked its services.[57] Both were later restored.

Content Removal

State and other actors are known to exert extralegal pressure on publishers and content producers to remove content, but it frequently goes unreported. Takedowns by international companies are more high profile. acebook reported restricting 6 items "that were alleged to violate local laws prohibiting blasphemy" in the second half of 2015.[58]

Official equests to remove content generally lack transparency. Following a major terrorist attack in December 2014, the government ordered material published by banned terrorist outfits o be removed from the internet, though published reports did not elaborated on the process involved.[59]

Media, Diversity, and Content Manipulation

Despite existing limitations on online content—and looming new ones—Pakistanis have open access to international news organizations and other independent media, as well as a range of websites representing Pakistani political parties, local civil society groups, and international human rights organizations. [60] ICTs, particularly mobile phones, promote social mobilization. After YouTube was

50 "Climbdown: PTA restores IMDb access after public outcry," *The Express Tribune*, November 23, 2013, http://bit.ly/1R2MVyv;Nighat Dad, "Why was IMDb blocked?" *The Express Tribune*, November 23, 2013, http://bit.ly/1QeE3Wz.

51 IMDb, "The Line of Freedom," http://www.imdb.com/title/tt2616400/.

52 Digital Rights Foundation, "First Case of Selective / Targeted Online Censorship: Pakistani Government Successfully Blocks Specific Links" press release, November 25, 2013, http://bit.ly/1Lmnjg7.

53 Josh Halliday and Saeed Shah, "Pakistan to ban encryption software," *The Guardian*, August 30, 2011, http://bit.ly/outDAD.

54 Nighat Dad, "Pakistan Needs Comms Security Not Restrictions," Privacy International (blog), September 12, 2011, http://bit.ly/1QeEvEi.

55 Barbora Bukovska, "Pakistan: Ban on internet encryption a violation of freedom of expression," Article 19, September 2, 2011, http://bit.ly/1Mlv3ja.

56 The VPN blocking is authorized under section 5(2)(b) of the PTA Act 1996 and the "Monitoring and Reconciliation of Telephony Traffic egulation. See, "Part II, S.R.O. Pakistan Telecommunication Authority Notification" *The Gazette of Pakistan*, March 15, 2010, http://bit.ly/1Lby01z.

57 "Creeping censorship: Spotflux claims its se vice is being 'actively blocked' in Pakistan," *The Express Tribune,* January 28, 2014, http://bit.ly/1dK9W3U.

58 "Governmen Requests Report for Pakistan", Facebook, https://govtrequests.facebook.com/country/Pakistan/2015-H2/.

59 "Govt directs PTA to remove banned outfits' ha e-material from internet, *"Dunya News*, 16 January 2015, http://bit.ly/1huNqoR

60 OpenNet Initiative, "Country Profile— akistan," 2012.

unblocked, all social networking, blogging, and VoIP applications were available and widely used during the coverage period. Nevertheless, most online commentators exercise a degree of self-censorship when writing on topics such as religion, blasphemy, separatist movements, and women's and LGBTI (lesbian, gay, bisexual, transgender, and intersex) rights.

Digital Activism

Human rights activists have galvanized public support against militancy using digital technology. In December 2014, when an influential cleric in Islama ad refused to categorically condemn a terrorist attack on a school, activists gathered outside the cleric's mosque, demanding an apology for the previous statement.[61] The call to protest originated through social media and text messages using the #ReclaimYourMosque hashtag.[62] A Taliban spokesman contacted the protest organizer, threatening him to back off or "be ready for consequences."[63]

The coverage period saw a continuation of the fight by rights o ganizations in Pakistan against the Prevention of Electronic Crimes Bill, using hashtags like #MyLifeAfterPECB and #PakRejectsCyberBill to raise awareness of threats to digital rights in the draft (see Legal Environment).

Violations of User Rights

Violations of user rights continued at high levels during the coverage period, including two 13-year prison sentences handed down by antiterrorism courts for content shared on Facebook. Civil society groups say the Prevention of Electronics Crimes Act approved in 2016 criminalizes legitimate online activity. Researchers uncovered compelling information about Pakistani agencies' surveillance ambitions and capabilities during the coverage period.

Legal Environment

Article 19 of the Pakistani constitution establishes freedom of speech as a fundamental right, although it is subject to several restrictions.[64] Pakistan became a signatory to the International Covenant on Civil and Political Rights in 2010.[65]

Several laws have the potential to restrict internet users. The 2004 Defamation Act allows for imprisonment of up to fi e years, and observers fear a chilling effect if it is used to launch court cases for online expression. Section 124 of the penal code on sedition "by words" or "visible representation" is broadly worded, though it has yet to be applied in an online context.[66]

Section 295(c) of the penal code, which covers blasphemy, is frequently invoked to limit freedom of expression. Any citizen can file a blasphemy complaint against any othe , and human rights groups say charges have been abused in the past to settle personal vendettas. The imputation of blasphemy

61 Ikram Junadi, "Islamabad stands fi m on Lal Masjid," *Dawn,* December 20, 2014, http://www.dawn.com/news/1151985.
62 Ikram Junadi, "Citizens arrive at Lal Masjid to 'reclaim their mosque'," *Dawn*, December 19, 2014, http://bit.ly/1v7dPtz.
63 "Lal Masjid protest activist receives threatening phone call," *Dawn*, December 22, 2014, http://www.dawn.com/news/1152467.
64 The Constitution of Pakistan, accessed September 2012, http://bit.ly/pQqk0.
65 "President signs convention on civil, political rights," *Daily Times*, June 4, 2010, http://bit.ly/1fyK9Tl.
66 "Pakistan Penal Code," accessed August 2013, http://bit.ly/98T1L8.

leaves the accused vulnerable to reprisals, regardless of whether it has foundation. Many cases have involved electronic media (see Prosecutions and Detentions for Online Activities).

Laws to combat terrorism can also been exploited against internet users. The Pakistan Protection Act passed in July 2014, reformulating a problematic Pakistan Protection Ordinance. Despite the reformulation, critics said it failed to address concerns expressed by lawyers and civil society groups, who said language categorizing unspecified cybe crimes as acts of terror was vague and open to abuse.[67]

The National Assembly approved the Prevention of Electronics Crimes Act during the coverage period of this report; at the end of the coverage period, it was pending Senate approval.[68] It passed in August 2016. Observers reported that the drafting process lacked transparency. The National Standing Committee on Information Technology and Telecommunication held a hearing to discuss the bill in May 2015, which included some criticism from civil society. But no major changes were incorporated in the version which the committee subsequently approved in September, and some committee members said they had not even been allowed to read it.[69] That draft was rejected by the Senate. In April 2016, an amended version of the bill was put forward again, and approved by the National Assembly.[70] Although the amended bill was approved on April 13, it was not released to the public until May 7,[71] though an unofficial copy was lea ed to journalists.[72]

Though it contained some procedural safeguards for cybercrime investigations by law enforcement agencies, international and local human rights groups condemned the Act's overly broad language and disproportionate penalties, including 14 year prison terms for acts of cyberterrorism that the law failed to adequately define [73] The law also punishes preparing or disseminating electronic communication to glorify terrorism; and preparing or disseminating information that is likely to advance religious, ethnic or sectarian hatred, both with up to seven years in prison. Section 18 criminalizes displaying or transmitting information that intimidates or harms the "reputation or privacy of a natural person" with a maximum three year prison term or a fine f PKR 1 million (US$9,500) or both.[74] Other problematic features of the include Section 37, which grants the PTA broad censorship powers (see Blocking and Filtering), and other sections governing officials' access to data (see Surveillance, Privacy, and Anonymity).

The Surveying and Mapping Act 2014 limits digital mapping activity to organizations registered with the governmental authority Survey of Pakistan, with federal permission required for mapping collab-

67 Bolo Bhi, "Human Rights Experts: Pakistan Could Become a "Police State" Under Protection Ordinance," *Global Voices Advocacy*, August 13, 2014, http://bit.ly/1OqLFGd.

68 "Cybercrime bill relegated to yet another committee", Dawn, June 23, 2016, http://www.dawn.com/news/1266681/

69 Fazal Sher, "Absence of comprehensive law against cybercrimes: NR3C of FIA unable to take action against criminals," *Business Recorder*, February 10, 2015, http://bit.ly/1PlaioF; Digital Rights Foundation, "Standing Comm. Passes Draft of PECB, Unseen by Comm. Members," September 21, 2015, http://bit.ly/1QeGTuA.

70 "Controversial Cyber Crime Bill approved by NA" Dawn, April 13, 2016 http://www.dawn.com/news/1251853

71 "The Peculiar timing of NA's decision to release Cyber Crime Law's final dra t", Digital Rights Foundation, May 7, 2016, http://bit.ly/28BaVna.

72 APC Impact, "Deconstructing Prevention of Electronic Crimes Bill 2015 – "Chapter II Offences and Punishments" – Part 1," April 18, 2015, http://www.netfreedom.pk/deconstructing-prevention-of-electronic-crimes-bill-2015-chapter-ii-offences-and-punishments-part-1/.

73 Digital Rights Foundation, "The Prevention of Electronic Crimes Bill 2015 - An Analysis," June 2016, https://www.article19.org/data/files/medialibra y/38416/PECB-Analysis-June-2016.pdf.

74 Prevention of Electronic Crimes Bill, accessible: http://digitalrightsfoundation.pk/wp-content/uploads/2016/08/PECB2016.pdf.

oration with foreign companies.[75]

Prosecutions and Detentions for Online Activities

Electronic speech perceived as blasphemous has been prosecuted in the past several years in Pakistan. In a new development during the coverage period, individuals were sentenced to 13 years in prison in two separate cases for allegedly distributing "hateful" or "sectarian" material on Facebook. Though little is known about the details of the cases, neither was publicly reported to involve threats of violence. The secrecy surrounding verdicts apparently penalizing online speech was concerning. In both instances, the men were tried and sentenced by Pakistani antiterrorism courts, rather than civil or criminal courts.[76] Antiterrorism courts were established under the Anti-Terrorism Act passed in 2007 and repeatedly amended to cover more offenses. They have been criticized for violating human rights, since trials take place behind closed doors and defendants are denied a full defense and the presumption of innocence.[77]

In November 2015, an antiterrorism court in Lahore sentenced a man belonging to the Shia sect of Islam to 13 years in prison and a fine f PKR 250,000 (US$2,400) under the antiterrorism act for posting "sectarian hate speech" characterized as "against companions of the Prophet of Islam" on Facebook, according to international news reports citing local officials [78] Local digital rights group Bytes for All said they had not been able to independently verify the details of the case.[79]

In March 2016, in a separate case, another Shia man was sentenced to 13 years in prison and a fine of PKR 250,000 (US$2,400), also by an antiterrorism court in Lahore, on three counts of promoting sectarian hatred on Facebook. His lawyer told Agence France-Presse that he was not responsible for distributing the content, but had only "liked" it on Facebook. The public prosecutor described the post as being "against the belief of Sunni Muslims," according to Agence France-Presse.[80]

On June 8, 2016, the Supreme Court granted bail to two women from Rawalpindi who had been detained for two months for allegedly sharing "vulgar pictures and defamatory text messages."[81] Some news reports said they had sent the messages to another woman, but at least one reported they had tampered with images of a female relative and distributed them on WhatsApp.[82] The Islamabad High Court had rejected initial pleas for bail. News reports said they were charged under Sections 36 and 37 of the Electronic Transaction Ordinance of 2002, which punish "violations of privacy of information" and "damage to information systems" respectively.

75 Nighat Dad, "Pakistan Considering Bill that Would Ban Independent Mapping Projects," Tech President, November 28, 2012, http://bit.ly/1OpVqpK; Pakistan National Assembly, Bill to provide for constitution and regulation of Survey of Pakistan, No. 225/25/2012, November 14, 2012, http://bit.ly/1OpVwOc.

76 Agence France-Presse, 25-year-old sentenced to 13 years in prison over 'religiously offensive' Facebook post," via *Express Tribune,* March 3, 2016, http://tribune.com.pk/story/1058813/25-year-old-jailed-for-13-years-over-facebook-post/.

77 Huma Yusuf, "Pakistan's Anti-Terrorism Courts," *CTC Sentinel,*March 3, 2010, https://www.ctc.usma.edu/posts/pakistan%E2%80%99s-anti-terrorism-courts.

78 Press Trust of India, "Pak sentences man to 13 years in jail for FB hate speech," *Business Standard,* November 24, 2015, http://www.business-standard.com/article/pti-stories/pak-sentences-man-to-13-years-in-jail-for-fb-hate-speech-115112400011_1.html.

79 "Pakistani Shia man jailed for 13 years for Facebook 'hate speech'", Dawn November 24, 2015, http://www.dawn.com/news/1221725.

80 Agence France-Presse, 25-year-old sentenced to 13 years in prison.

81 "SC grants bail to two women jailed for sending 'vulgar' texts" Express Tribune, June 9, 2016 http://bit.ly/24NZ8Nv

82 Shahid Rao, "Bail pleas of victim's in-laws rejected," *The Nation,* April 29, 2016, http://nation.com.pk/islamabad/29-Apr-2016/bail-pleas-of-victim-s-in-laws-rejected.

On October 28, 2015, Pakistan's Federal Investigation Agency arrested an activist and member of the Pakistan Tehreek-i-Insaf political party for comments posted on Twitter in September. The comments, which pertained to relatives of a member of the judiciary presiding over a corruption case, have since been deleted.[83] The activist, Jalal Qazi, was also charged with violating clauses 36 and 37 of the Electronic Transaction Ordinance. Each clause carries a maximum seven year jail term, fines up o PKR 1 million rupees, or both."[84] He was released on bail on November 3, 2015.[85]

Fresh blasphemy accusations were reported during the coverage period, but had not gone to trial in mid-2016. On May 25, 2016, a Christian man, named in reports as Usman Masi, was charged by police in Sheikhupura, with allegedly posting "blasphemous" material on an unspecified social media website.[86] He was not reported to be in custody.

Surveillance, Privacy, and Anonymity

The Prevention of Electronics Crimes Act passed after the coverage period of this report, granted overly broad surveillance powers, both to agencies within Pakistan, and potentially beyond, since it includes provisions that permit the sharing of data with international agencies without adequate oversight.[87]

A 2007 Prevention of Electronic Crimes Ordinance requiring telecommunications companies to retain user traffic data for a minimum f 90 days, and share logs of customer communications with security agencies when directed by the PTA, expired in 2009, though the practices reportedly continued.[88] The Prevention of Electronic Crimes Act retained the 90-day minimum, and allows an "authorized office " to request extended data retention without oversight. The PECB also grants "authorized office s" to request that users hand over their decryption keys (if the data is encrypted), or else face prosecution.[89]

Government surveillance was already a concern for activists, bloggers, and media representatives, as well as ordinary internet users. Pakistani authorities, particularly intelligence agencies, appear to have been expanding their monitoring activities in recent years, while provincial officials ha e been exerting pressure on the central government to grant local police forces greater surveillance powers and location tracking abilities, ostensibly to curb terrorism and violent crimes.[90]

In 2015, an investigation by U.K.-based Privacy International revealed that the government's surveillance capability, particularly that of the Inter-Services Intelligence Agency, outstrips domestic and

83 "Qazi Jalal arrested in Peshawar for a Tweet", Teeth Maestro Blog, October 28, 2015, http://bit.ly/1ttMCaL.

84 "Can a Tweet get you arrested in Pakistan? Yes, it can", Express Tribune, October 29, 2015 http://bit.ly/1RhJ018.

85 "FIA arrests PTI's social media member over violation of cyber laws", The News, October 29, 2015 http://bit.ly/1Tzkso6.

86 "Christian man booked for posting blasphemous text on social media" May 26, 2016, http://bit.ly/21jJg0d.

87 Data includes the "communication's origin, destination, route, time, data, size, duration or type of underlying service." See, Nighat Dad, Adnan Chaudhri, "The Sorry Tale of the PECB, Pakistan's Terrible Electronic Crimes Bill" Digital Rights Foundation, November 26, 2015, http://bit.ly/1WcxTwb.

88 Kelly O'Connell, "INTERNET LAW – Pakistan's Prevention of Electronic Crimes Ordinance, 2007," *Internet Business Law Services*, http://bit.ly/1NvN1kw.

89 "A Deeper Look Inside the PECB, Pakistan's Terrible Cyber-Crime Bill", Electronic Frontier Foundation, November 30, 2015 http://bit.ly/24lAjtW.

90 Masroor Afzal Pasha, "Sindh Police to Get Mobile Tracking Technology," *Daily Times*, October 29, 2010, http://bit.ly/16TKfLY; "Punjab Police Lack Facility of 'Phone Locator', PA Told," *The News*, January 12, 2011, http://bit.ly/1bRl6bx.

international law regulating that surveillance.[91] "Mass network surveillance has been in place in Pakistan since at least 2005," using technology obtained "from both domestic and foreign surveillance companies, including Alcatel, Ericsson, Huawei, SS8 and Utimaco," according to the report.

A report released in 2013 by Citizen Lab indicated that Pakistani citizens may be vulnerable to oversight through a software tool present in the country. FinFisher's "Governmental IT Intrusion and Remote Monitoring Solutions" package includes the FinSpy tool, which attacks the victim's machine with malware to collect data including Skype audio, key logs, and screenshots. [92] The analysis found FinFisher's command and control servers in 36 countries worldwide, including on the PTCL network in Pakistan. This did not confi m that actors in Pakistan are knowingly taking advantage of its capabilities. In 2014, however, hackers released internal FinFisher documents indicating that a client identified as "Cus omer 32" licensed software from FinFisher to infect Microsoft office documents with malware to steal files f om target computers in Pakistan.[93]

In July 2015, data belonging to Italian commercial digital surveillance company Hacking Team was leaked online by hackers, revealing communications between senior Hacking Team personnel and private-sector representatives of foreign intelligence agencies. In the case of Pakistan, these communications went back to 2011, and documented meetings with intelligence agents, and requests for mobile interception technologies. No purchases were reported. [94]

Official agencies also use less co ert means to obtain user data. According to the most recent transparency reports, Twitter received one specific account equest from the Pakistani government between July 2015 and December 2015. [95] Facebook reported nearly 500 user data requests by the Pakistani government during the same period, of which 66 percent led to "some data...produced."[96]

In July 2015, the government instructed Blackberry to allow officials access o encrypted messages sent through the company's servers or discontinue operating in Pakistan.[97] In December, the company reported it had been allowed to continue operating even though it had not complied.[98]

The Fair Trial Act, passed in 2013, [99] allows security agencies to seek a judicial warrant to monitor private communications "to neutralize and prevent [a] threat or any attempt to carry out scheduled offences." It covers information sent from or received in Pakistan, or between Pakistani citizens whether they are resident in the country or not. Under the law, service providers face a one-year jail term or a fine f up to PKR 10 million (US$103,000) for failing to cooperate with warrants. Warrants can be issued if a law enforcement official has " eason to believe" in a terrorism risk; it can also be temporarily waived by intelligence agencies. A 2014 white paper issued by the Digital Rights Group said

91 Matthew Rice, "Tipping the Scales: Security and surveillance in Pakistan," Privacy International, July 21, 2015, https://www.privacyinternational.org/node/624.

92 Morgan Marquis-Boire et al, *For Their Eyes Only: The Commercialization of Digital Spying*, Citizen Lab, May 1, 2013, http://bit.ly/ZVVnrb.

93 Sohail Abid, "Massive Leak Opens New Investigation of FinFisher Surveillance Tools in Pakistan," Digital Rights Foundation, via Global Voices Advocacy, August 22, 2014, https://advox.globalvoices.org/2014/08/22/massive-leak-opens-new-investigation-of-finfisher-surveillance-tools-in-pakistan/.

94 Bolo Bhi, "Hacking Team in Pakistan," http://bolobhi.org/hacking-team-in-pakistan/.

95 "Transparency Report" for Pakistan, Twitter, accessed May 3 2016 https://transparency.twitter.com/country/pk

96 Government Requests Report for Pakistan", Facebook, https://govtrequests.facebook.com/country/Pakistan/2015-H2/.

97 BBC News, "Blackberry to keep operating in Pakistan," December 31, 2015, http://www.bbc.com/news/technology-35204922.

98 Marty Beard, "Continuing our Operations in Pakistan," December 31, 2015, *Inside Blackberry,* http://blogs.blackberry.com/2015/12/continuing-our-operations-in-pakistan/.

99 "Investigation for Fair Trial Act 2013," *The Gazette of Pakistan,* February 22, 2013, http://bit.ly/18esYjq.

that provisions of the Fair Trial Act contravene the Constitution and international treaties Pakistan has signed in the past.[100]

ISPs, telecommunications companies, and SIM card vendors are required to authenticate the Computerized National Identity Card details of prospective customers with the National Database Registration Authority before providing service.[101] A registration drive was launched following a December 2014 attack on a school that dozens of students. Investigators tracked three unregistered SIM cards used by the terrorists for communication during the attack.[102] Following the attack, the government required citizens to verify numbers registered against their names and added a biometric thumb impression to SIM card registration requirements.[103] In 2015, SIM card owners without biometric identification ere warned of automatic disconnection, and 26 million SIM cards were subsequently disconnected or blocked.[104]

Pakistanis are also vulnerable to surveillance from overseas intelligence agencies. In June 2015, digital security and intelligence magazine *The Intercept* published revelations of hacking and infiltration f the Pakistan Internet Exchange (PIE) by Britain's GCHQ intelligence agency prior to 2008. According to *The Intercept*, this gave GCHQ "access to almost any user of the internet inside Pakistan" and the ability to "re-route selected traffic ac oss international links towards GCHQ's passive collection systems."[105]

Intimidation and Violence

Pakistan is one of the world's most dangerous countries for traditional journalists.[106] Online journalists can also be vulnerable.

Violence against women thought to have brought shame on their communities—including murder via "honor killings"—has begun to involve ICT usage. In April 2016, a 16-year old girl was killed by her older brother for using a mobile phone.[107]

Leaking explicit photos, threats of blackmail, and other incidences of online harassment are increasing in Pakistan. More than three thousand cybercrimes were reported to the Federal Investigation Agency from August 2014 to August 2015.[108] Of those cases, 45 percent targeted women on social

100 "Privacy rights: Whitepaper on surveillance in Pakistan presented," *The Express Tribune*, November 16, 2014, http://bit.ly/1L4h8Mc; Waqqas Mir, et al. "Digital Surveillance Laws in Pakistan," eds. Carly Nyst and Nighat Dad, (a white paper by Digital Rights Foundation, November 2011) http://bit.ly/1jg2IzH.

101 Bilal Sarwari, "SIM Activation New Procedure," *Pak Telecom*, September 3, 2010, http://bit.ly/pqCKJ9.

102 Akhtar Amin, "PTA fails to block unregistered SIMs despite court orders," *The News*, December 26, 2014, http://bit.ly/1P4zSyZ.

103 Ahmad Fuad, "Biometric SIM verification: a th eat or opportunity for cellular fi ms?" *The Express Tribune*, February 1, 2015, http://bit.ly/1LbAtJe.

104 Aamir Attaa, "Biometric Verification f SIMs is not Fool Proof: Chairman PTA," ProPakistani, March 16, 2015, http://bit.ly/1QeImAZ; "26 million SIMs Blocked As SIM Reverification Dri e Ends, ProPakistani, April 13, 2015 http://bit.ly/24Bm5VT.

105 "Spies Hacked Computers Thanks To Sweeping Secret Warrants, Aggressively Stretching UK Law", The Intercept, June 22, 2015, http://bit.ly/1VMfTZN.

106 Committee to Protect Journalists, "56 Journalists Killed in Pakistan since 1992/Motive Confi med," accessed January 2014, http://bit.ly/1LE6kYI.

107 Chris Summers, "Man stabs his 16-year-old sister to death in Pakistan 'honour killing' - because she was using a mobile phone," *Daily Mail,* April 28, 2016, http://www.dailymail.co.uk/news/article-3563679/Pakistan-police-arrest-man-honour-killing-sister.html.

108 Noorwali Shah, "In the cyberspace: Technology illiteracy leads to online harassment," *The Express Tribune*, August 12, 2015, http://bit.ly/1N4gWgJ.

media. The figu es only represent reported cases—many victims do not come forward for fear of losing access to ICTs. No data has been provided for other provinces.

Militant Islamic groups have launched attacks on cybercafes and mobile phone stores in the past for allegedly encouraging moral degradation.[109] No attacks were documented during the coverage period of this report.

Free expression activists and bloggers have also reported receiving death threats. Many publicize the threats—and sometimes attract more—on Twitter. Most are sent via text message from mobile phones, often originating from the tribal areas of the country, and several include specific details from the recipient's social media profiles or other online activit .

Technical Attacks

Technical attacks against the websites of nongovernmental organizations, opposition groups, and activists are common in Pakistan but typically go unreported due to self-censorship, and were not publicized during the coverage period. The websites of government agencies are also commonly attacked, often by ideological hackers attempting to make a political statement.[110] In 2015, the website of the religious political party Jamaat-e-Islami was hacked for its alleged support of terrorists.[111]

Officials allege that most cyberattacks origina e in India; groups based in Pakistan also hack Indian websites.[112]

109 "Blast in Nowshera destroys internet cafe, music store," *Dawn*, February 2, 2013, http://bit.ly/1jiOhdA; "Fresh Bomb Attacks Kill 2 Shias, wound 20 in Pakistan," *Press TV,* January 13, 2013, http://bit.ly/Ssoth2; Associated Press, "Police: Bomb Blast at Mall in Northwestern Pakistan Kills 1 Person, Wounds 12," *Fox News*, February 21, 2013, http://fxn.ws/YI5QCq.

110 Hisham Almiraat, "Cyber Attack on Pakistan's Electoral Commission Website," *Global Voices Advocacy*, April 1, 2013, http://bit.ly/1WSbWQL.

111 Usman Khan, "Jamaat-e-Islami website hacked over 'alleged support for terrorism," *The News Tribe,* January 20, 2015, http://bit.ly/1P4CvB5.

112 "Cybercrimes: Pakistan lacks facilities to trace hackers," *The Express Tribune*, February 1, 2015, http://bit.ly/1FWXTW7.

Freedom House

Philippines

	2015	2016
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	10	9
Limits on Content (0-35)	5	5
Violations of User Rights (0-40)	12	12
TOTAL* (0-100)	**27**	**26**

* 0=most free, 100=least free

Population:	**100.7 million**
Internet Penetration 2015 (ITU):	**41 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2016 Status:	**Partly Free**

Key Developments: June 2015 – May 2016

- At the height of the 2016 national election campaign, police warned that spreading "destructive" memes about candidates could be grounds for criminal charges (see **Media, Diversity, and Content Manipulation**).
- Outgoing President Benigno Aquino signed the country's fi st antitrust law, which analysts hope will strengthen competition in the telecommunications sector (see **ICT Market**).
- The Department of Information and Communications Technology Act of 2015 created a dedicated government agency for the ICT sector (see **Regulatory Bodies**).

Introduction

Internet freedom improved since there was no recurrence of the internet shutdown imposed during the previous reporting period.

The Philippines held a general election on May 9, 2016. Presidential candidate Rodrigo Duterte, who openly encourages extrajudicial killings to combat crime, beat the incumbent administration's candidate. In his first press conference, Duterte said during that corrupt journalists deserved to be assassinated, a troubling omen for freedom of expression.

The threat of criminal liability may already be deterring free speech online in the Philippines, since digital activism appears to have decreased in the past two years. The 2012 cybercrime act criminalized online libel, and after a temporary suspension, the Supreme Court upheld the act's libel clause in 2014. Over 200 libel cases had been filed under the law by August 2015, though none involving legitimate speech were resulted in criminal detention during the coverage period. At the height of election campaigns in early 2016, satirical memes about candidates were widely shared online. The national police—one of two agencies tasked to enforce the cybercrime law—warned the public that anyone spreading "destructive" political memes on the internet could face charges.

Before handing power to the new administration, President Benigno Aquino, Jr. signed two pieces of legislation that are expected to be game changers in the information and communications technology (ICT) sector. The first was an antitrust law, which penalizes anticompetitive business practices to drive down costs for consumers and is expected to attract new investment in the ICT market; the second created a dedicated government agency for the sector. One of two pending bills that promoted internet freedom—the Magna Carta for Internet Freedom, was absorbed into the latter, losing many of its strongest provisions. The second, a Crowdsourcing Act which encourages citizens to participate in the legislative process, was stalled in Congress.

Obstacles to Access

Connection speeds remain among the slowest in the world but the government is addressing low internet penetration by providing thousands of free Wi-Fi hotspots with the aim of connecting 99 percent of the population. Outgoing President Benigno Aquino III signed Republic Act 10667 or the Philippine Competition Act after 25 years stalled in Congress. The country's first antitrust law could level the playing field for new entrants to the telecoms sector, which was historically dominated by the Philippine Long Distance Telephone Company. Aquino also signed Republic Act 10844 to create the Department of Information and Communications Technology.

Availability and Ease of Access

The International Telecommunication Union estimated internet penetration at 41 percent in 2015, up from 40 percent in 2014.[1] Connectivity is concentrated mainly in urban areas, while rural areas remain largely underserved.[2] To bridge this gap, the government started rolling out a free internet ser-

1 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1cblxxY.

2 John Carlos Rodriguez, "How many Filipinos are still not connected to Internet?" *ABS-CBN News*, October 3, 2014, http://bit.ly/1Nkv4nd.

vice in 2013 using TV White Space technologies, initially to serve communities struck by destructive typhoons in the Visayas region.[3] In July 2015, the government launched another multimillion-dollar project to provide more than 7,000 free Wi-Fi hotspots in 43 cities. The stated aim of the *Juan Konek!* Digital Empowerment Program is to connect 99 percent of the population, with lower-income municipalities given priority.[4]

Mobile phones remain the most widely used wireless communication tool with a penetration rate of 118 percent in 2015, indicating that some users have more than one device.[5] The leading telco, Philippine Long Distance Telephone Company (PLDT), reported having 69.6 million mobile phone subscribers in the first quarter of 2015,[6] while closest rival Globe Telecommunications had 50 million by the third quarter of the year.[7] Mobile internet usage has been slow to take off. There were only 3.1 million mobile broadband subscribers in 2014,[8] following the deployment of 4G LTE and HSPA+ technologies in 2013.[9]

The slow uptake of broadband internet in the country, and the consequent low internet penetration, is largely due to steep subscription fees. The cost and slow speed of internet service has been a prominent issue since 2014, and prompted the National Telecommunications Commission (NTC) to conduct an isolated speed test of major ISPs in September 2015 to determine if they are providing subscribers with their advertised speed. Only PLDT was found to exceed its advertised speed, while Globe was found to be slower but still compliant.[10] Akamai reported the average connection speed in the country at 2.8 Mbps in the third quarter of 2015, a slight increase from last year's 2.5, but still putting the Philippines just 108 out of 145 countries assessed.[11] Internet subscriptions are also comparatively expensive.[12] In early 2016, PLDT was charging a minimum monthly subscription fee of US$21 for fixed broadband for up to 1 Mbps, compared to US$29 for up to 2 Mbps the previous year; while Globe charges US$23 for up to 2 Mbps compared to US$24 in 2015.[13]

Restrictions on Connectivity

There was no reported incidence of intentional blocking or limiting of cellular services during the reporting period. Such a restriction was imposed for the first time in the Philippines when the government ordered a sporadic regional suspension of cellular services during the visit of Pope Francis from January 15 to 19, 2015.[14] Mobile phone subscribers received text messages from service pro-

3 Marife Carpio and Jo Ann Guillao, "Scoping study on the use of TV White Space in Philippine education," *Asian Journal of Educational Research,* Vol. 4, No. 1, 2016, http://bit.ly/1LnHFrS.

4 "DOST project to narrow digital divide in PH," *Manila Times*, March 8, 2016, http://bit.ly/1pI8AEX.

5 ITU, "Mobile-Cellular Telephone Subscriptions, 2000-2015," http://bit.ly/1cblxxY.

6 Quarterly report to the Securities and Exchange Commission (SEC), as of March 2015. This is the latest report made available by PLDT.

7 Quarterly report to the Securities and Exchange Commission, as of September 30, 2015.

8 Quarterly reports to the SEC, as of September 30, 2014.

9 Lawrence Agcaoili, "Smart, Globe race to put up more 4G LTE infra sites," *The Philippine Star,* October 14, 2013, http://bit.ly/1A8l0Ea.

10 Andrei Medina, "NTC: 3 ISPs deemed 'compliant,' one failed speed test," *GMA News Online,* September 18, 2015, http://bit.ly/1iqeBBZ.

11 Akamai, *State of the Internet Report*, Q3 2015 Report, December 2015, http://akamai.me/1LFk9B7.

12 Lorenz S. Marasigan, "PHL's slow but expensive internet service," *Business Mirror*, August 23, 2015, http://bit.ly/1SPtzAX.

13 PLDT Products, http://shop.pldthome.com/; Globe Telecom, http://bit.ly/1YVoZSk.

14 Mica Basa, "No network service? It's for Pope's safety, say telcos," *Rappler*, January 16, 2015, http://bit.ly/18siEsm

viders citing a directive from the NTC to block network coverage for security reasons.[15] Following the unpopular move, the government announced in advance that it would not block cellular services during the Asia Pacific Economic Cooperation Summit, another high-p ofile e ent held on November 18 and 19, 2015.[16]

There were 400 ISPs registered with the NTC in 2013, according to most recent government data.[17] Many of these connect to PLDT, which owns the majority of fi ed-line connections as well as the 10,000 kilometer domestic fibe -optic network that connects to several international networks. Since the completion of a new cable linking the central provinces of Palawan and Iloilo in January 2014,[18] the company now owns or partly owns fi e out of nine international cable landing stations.[19] In October 2015, PLDT announced the construction a US$40 million international cable to link to the U.S. and Japan with a landing station in Mindanao.[20]

ICT Market

Companies entering the market go through a two-stage process. First, they must obtain a congressional license that involves parliamentary hearings and the approval of both the upper and lower houses. Second, they need to apply for certification f om the NTC.

The constitution limits foreign ownership of local businesses to 40 percent. Internet service is currently classified as a alue-added service and is therefore subject to fewer regulatory requirements than mobile and fi ed phone services.

In the 1990s, government legislation allowed competitors a foothold in a market dominated by the PLDT, a company that had been U.S.-owned and Philippine government-owned before becoming a private entity.[21] Until recently, the country did not have antitrust laws to promote healthy competition between businesses. But in a development welcomed by observers, the president signed Republic Act 10667, or the Philippine Competition Act, in July 2015, 25 years after it was filed in the eighth Congress (1987-1992) as House Bill 5286.[22] According to its principal author, Senator Bam Aquino, the law is "expected to eliminate cartels, and penalize anti-competitive agreements and abuses of dominant players in the markets that lead to high prices of goods and services."[23] He clarified that the law does not directly prohibit the existence of monopolies," and will not stop an entity from maintaining its dominance in the market as long as it does not commit abuses such as driving away competition.[24]

In September 2015, shortly after the law was signed, San Miguel Corporation announced its plans

15 Danessa O. Rivera, "Telcos note govt has say in blocking network coverage for papal visit," *GMA News Online*, January 16, 2015, http://bit.ly/1MhdUTL.

16 Julliane Love de Jesus, "No phone signal disruption during Apec meet – PNP chief," *Inquirer.net,* November 12, 2015, http://bit.ly/1QUvhyt.

17 National Statistics Office, "Philippines in Figu es 2015."

18 Miguel R. Camus, "PLDT Completes Palawan-Iloilo Link," *Philippine Daily Inquirer*, January 26, 2014, http://bit.ly/1BVowGD.

19 "Submarine Cable Map," *TeleGeography*, last updated March 14, 2016, http://bit.ly/181agjA

20 Darwin G. Amojelar, "PLDT to build $40-m Mindanao cable link," *The Standard,* October 20, 2015, http://bit.ly/1QUZRJv

21 Mary Ann Ll. Reyes, "PLDT: From voice to multi-media (First of Two Parts)," *The Philippine Star*, http://bit.ly/1O45UKY.

22 Louis Bacani, "PNoy OKs landmark Philippine Competition Act, Cabotage Law amendments," *PhilStar.com*, July 21, 2015, http://bit.ly/1V9oR1o.

23 "After long wait, Congress ratifies Act penalizing ca tels, abuse of dominant positions," website of Senator Bam Aquino, July 11, 2015, http://bit.ly/1QUHgfo.

24 Josiah Go, "Finally, Congress passes Philippine Competition Act," *Inquirer.net,* July 10, 2015, http://bit.ly/1CsluuO.

to enter the telecommunications industry in partnership with Australia's Telstra Corporation,[25] a joint venture seen as much-needed by an industry in need of competition.[26] However, after months of talks, the venture appeared to have stalled amid disagreements between the parties concerning risk-sharing brought about by potential regulatory problems.[27] One major concern was a PLDT and Globe petition to the NTC to auction the 700 MHz frequency currently owned by San Miguel, which would supposedly be tapped by the joint venture. Telstra required a 100 percent refund of its US$1 billion investment if the frequency issue was not resolved.[28]

Regulatory Bodies

On May 23, 2016, before ending his term as president, Benigno Aquino, Jr. signed into law Senate Bill No. 2686 (a reintroduction of Senate Bill No. 50 filed in 2010), o create a separate and dedicated agency to head the development of ICTs. Republic Act 10844, known as the Department of Information and Communications Technology Act (DICT) of 2015, either abolished or absorbed institutions governing the ICT sector.[29]

Among the abolished offices a e the Information and Communications Technology Office, the N - tional Computer Center, National Computer Institute and all units pertinent to communications under the Department of Transportation and Communications.[30] Three offices a e now attached to the DICT: The National Privacy Commission; the Cybercrime Investigation and Coordination Center (see Legal Environment); and the National Telecommunications Commission, which has regulated the industry with quasi-judicial powers and developed tariff and technical regulations, licensing conditions, and competition and interconnection requirements since its creation in 1979. All three offices will continue to function according to their mandate.

The newly formed DICT will be headed by a Secretary, three undersecretaries, and four assistant secretaries; all of whom are to be appointed by the president. The law provides that these positions must be filled in by people with se en years of experience in areas including ICTs, IT service management, information security, cybersecurity, and data privacy.

Limits on Content

During the 2016 national elections, netizens turned to social media to know more about candidates, especially for those vying for the presidency, and to express their support or disapproval. This activity did not escape the anti-cybercrime group of the Philippine National Police, which warned the public that "spreading destructive memes" could be grounds for libel charges. In late 2015, the DOJ issued an advisory reminding ISPs to report online activity involving child pornography and emphasizing strong penalties for noncompliance.

25 Chrisee Dela Paz, "San Miguel targets to double revenues in 5 years," *Rappler,* September 20, 2015, http://bit.ly/1nLw9Lg.

26 Grace Mirandilla-Santos, "Impending Telstra-SMC partnership puts pressure on PH telecom," *telecomasia.net,* October 26, 2015, http://bit.ly/1QVdzfq

27 Daxim M. Lucas, "Risk sharing broke SMC-Telstra talks," *Inquirer.net,* March 15, 2016, http://bit.ly/22iUOXk.

28 Jose Bimbo F. Santos, "PLDT, Globe hit SMC control of 700 MHz as 'anti-competitive'," *Interaksyon,* February 17, 2016, http://bit.ly/1olDGvz.

29 Kathrina Charmaine Alvarez, "PNoy signs law creating Department of Information and Communications Technology," *GMA News Online*, May 23, 2016, http://bit.ly/25cNZb6

30 The Department of Transportation and Communications has also been renamed the Department of Transportation. Republic Act 10844.

Blocking and Filtering

No systematic government censorship of online content has been documented in the Philippines, and internet users enjoyed unrestricted access to both domestic and international sources of information during the coverage period of this report. Internet users freely access social networks and communication apps including YouTube, Facebook, Twitter, and international blog-hosting services. Although rare, blocking and fil ering of content is allowed under a law that requires ISPs to prevent access to pornographic sites.[31] Other than the DOJ's brief call to ISPs to block Canada-based online dating site Ashley Madison in November 2014,[32] which it retracted a month later, no disproportionate blocking of online content has been documented.

On September 1, 2015, The Department of Justice (DOJ) released an advisory reminding ISPs of their responsibility to block and report access to child pornography. Penalties for violations include fines of up to US$10,000 and loss of license.[33]

The Supreme Court ruled in February 2014 against Section 19, the infamous "takedown" clause of the 2012 Cybercrime Prevention Act that would have allowed the Department of Justice to "restrict or block" overly broad categories of content without a court order;[34] however, it upheld other provisions criminalizing online libel (see Legal Environment).

Content Removal

The government does not usually order removal of online content. One exception in early 2015 involved an online video depicting the killing of 44 members of the Philippine National Police Special Action Force in Mamasapano, Maguindanao, in the southern Philippines, allegedly by Muslim insurgents. The video went viral on YouTube, eliciting public anger against the uploader of the video as well as the perpetrators, on grounds that sharing the footage was insensitive to the families. The Office f the President ordered the uploader to take down the video.[35] After the individual refused to comply, the National Bureau of Investigation (NBI) threatened to go after the individual, and those who subsequently shared or "liked" it on social media.[36] This announcement was issued in spite of the fact that the Supreme Court had found in their 2014 ruling against Section 5 of the Cybercrime law that it was unconstitutional to punish those who simply like or share a post or video online. The NBI later said they had identified the sou ce of the video, but no criminal charges were reported.[37] The video, in several edited versions, remained accessible.

The Magna Carta for Philippine Internet Freedom, filed by Sena or Miriam Defensor Santiago in July

31 TJ Dimacali, "ISPs tasked to block just child porn, not all adult sites – NTC," *GMA News* Online, March 17, 2014, http://bit.ly/1FnJD5x.

32 Agence France-Presse, "DOJ seeks to block adultery website Ashley Madison," *GMA News* Online, November 30, 2014, http://bit.ly/1Emkir6.

33 Buena Bernal, "Penalty awaits ISPs not blocking child porn sites – DOJ," *Rappler,* September 1, 2015, http://bit.ly/1R92571.

34 Rep. Act 10175 (2012), http://bit.ly/1wjGai4.

35 Andrea Calonzo, "Palace: Take down video of Mamasapano clash," *GMA News Online*, February 11, 2015, http://bit.ly/1x5MrmH.

36 Aie Balagtas See, "NBI to hunt people sharing raw footage of SAF massacre," *The Philippine Star*, February 21, 2015, http://bit.ly/1HTVBTO.

37 Mark Mereuñas, "Man who uploaded Mamasapano video goes to NBI in Davao," *GMA News Online*, February 18, 2015, http://bit.ly/1x5Vhkc.

2013, attracted widespread support and discussion on social media,[38] particularly a provision that "provides for court proceedings in cases where websites or networks are to be taken down and prohibits censorship of content without a court order."[39] The legislation met an undistinguished conclusion in the Senate during the coverage period when it was absorbed into Senate Bill No. 2686 and later signed into law as Republic Act 10844, creating a government agency for ICTs (see Regulatory Bodies). The requirement for a court order to support content removal requests was not included.[40] Since so many internet freedom protections were diluted or lost, supporters hope the original legislation will be reintroduced.

Media, Diversity, and Content Manipulation

Generally, the Philippine blogosphere is rich and thriving. Both state and non-state actors actively use the internet as a platform to discuss politics, especially during elections. There have been no explicit government restrictions in place against any social media or communication applications.

Many news websites are online versions of traditional media, which may reflect sel -censorship due to the level of violence against journalists in the Philippines.

There are periodic reports of state officials and pri ate authorities using harassment to suppress online speech. In January, as campaigning for the 2016 national elections heated up, the Philippine National Police issued a warning against spreading "destructive memes" about candidates on the internet. The statement did not elaborate on the definition f "destructive," saying only that its anti-cybercrime group can easily track down offenders on social media and have them charged with online libel.[41] It also remains unclear what they meant by "spreading"—as the term could cover a range of activities, from creating to reposting and "liking."

Digital Activism

No prominent online calls for action occurred during the reporting period, in contrast to previous years. Digital activism in the Philippines has had a significant im act on a number of contentious sociopolitical issues, making national and international headlines and prompting positive action from the government. Past successes include a 2013 protest against the alleged misuse of PHP 10 billion (US$220 million) from a Priority Development Assistance Fund, locally dubbed the "pork barrel," by senators and members of Congress. A Facebook petition called for the abolition of the fund and the filing f criminal charges against the lawmakers,[42] and helped fuel nationwide protests.[43] The Su-

38 "Pinoy netizens welcome Miriam's online rights bill," *ABS-CBN News*, July 4, 2013, http://bit.ly/1xp4iQ0. Its counterpart, House Bill No. 1086, was also filed in House f Representatives; Center for Media Freedom and Responsibility, "Update: the Cybercrime Prevention Act of 2012," September 12, 2013, http://bit.ly/1BGpYez.

39 Norman Bordadora, "Santiago Proposes Magna Carta for Internet," *Inquirer*, December 1, 2012, http://bit.ly/18rVQt6; Louis Bacani, "'Crowdsourcing' bill allows citizens' online participation in lawmaking," *The Philippine Star*, July 4, 2013, http://bit.ly/1DnofxQ.

40 Republic Act 10844, *Official Gazette*, May 23, 2016, http://www.gov.ph/2016/05/23/republic-act-no-10844/.

41 Kristine Felisse Mangunay, "Spreading foul election memes could lead to online libel raps," *Inquirer.net,* January 8, 2016, http://bit.ly/1odeY5H.

42 David Lozada, "Aug 26 anti-pork barrel protests spread nationwide," *Rappler*, August 24, 2013, http://bit.ly/1Og4yMw.

43 "Thousands join Million People March vs pork," *ABS-CBN News*, August 26, 2013, http://bit.ly/1Qrp8IT.

preme Court subsequently declared the fund unconstitutional,[44] and three senators and several NGO officials ent on to face corruption charges, while other lawmakers are still being investigated.[45]

Anticipating the role of netizens in the 2016 elections, a group of prominent online activists launched the "iVote, iWatch" social media campaign on BlogWatch.tv on September 24, 2015, enabling netizens to share election-related content.[46] BlogWatch reports having been the fi st citizen media outlet to cover the 2010 elections and has been conducting interviews with presidential candidates ever since.[47]

Violations of User Rights

On August 12, 2015, the government issued Implementing Rules and Regulations of the Cybercrime Prevention Act, three years after the law's enactment. It contained specific provisions addressing some vague sections in the law such as the overlapping of administrative functions of government agencies; the role of ISPs in collecting and preserving data; and the need for a court order before law enforcers can gather computer data. The national police reported that incidents of cybercrime went up to more than 1,000 as of August 2015. These included high-profile libel cases against an online media organization and a prominent fashion blogger.

Legal Environment

The Bill of Rights of the 1987 constitution protects freedom of expression (Section 4) and privacy of communication (Section 1).[48] However, some laws undermine those protections. Libel is punishable by fines and imprisonment under A ticles 353 and 360 of the revised penal code. This has historically been challenging to prove in online cases which lack a physical place of publication—one of the requirements for an offline p osecution—and in 2007, a Department of Justice resolution established that the provisions do not apply to statements posted on websites.[49]

Section 4c (4) of the 2012 Cybercrime Prevention Act, however, classified libel as a cybe crime. Section 6 stipulates a higher degree of punishment for online libel, with prison terms of up to eight years,[50] almost double the maximum penalty for the identical offense perpetrated offline, which is punishable by prison terms of six months to four years and two months.[51] The Supreme Court suspended implementation of the law after widespread protests, but in February 2014 ruled that the libel provision was constitutional, keeping the disproportionate penalties on the books. However, it

44 Mark Merueñas, "Supreme Court Declares PDAF Unconstitutional," *GMA News Online,* November 19, 2013, http://bit.ly/1NkzXN2.

45 Patricia Denise Chiu, "Govt lawyers block ex-solon's request to be detained at Camp Crame," *GMA News Online*, February 25, 2015, http://bit.ly/1MCZD3Q.

46 Janvic Mateo, "Netizens to play big role in 2016 polls," *PhilStar,* September 26, 2015, http://bit.ly/22quLAN.

47 BlogWatch.tv

48 Cons. (1987), art. III, Bill of Rights, http://bit.ly/1Qrp8IT.

49 Department of Justice, Resolution No. 05-1-11895 on Malayan Insurance vs. Philip Piccio, et al., June 20, 2007. Article 353 states that, "libel is committed by means of writing, printing, lithography, engraving, radio, phonograph, painting, theatrical exhibition, cinematographic exhibition, or any similar means." The Department also stated that the accused are not culpable because they cannot be considered as authors, editors, or publishers as provided for in Article 360. Critics have further noted that the Revised Penal Code of the Philippines dates from 1932, long predating digital technology.

50 SC Decision, G.R. No. 203335, February 11, 2014, http://bit.ly/1EZnzAA ;"Concurring and Dissenting Opinion," C.J. Sereno, http://bit.ly/1KHhICy.

51 Purple Romero, "DOJ holds dialogue on 'E-Martial Law'," October 9, 2012, *Rappler*, http://bit.ly/1NXmTx2.

clarified that users reacting online to a libelous post—by "liking" it, for example—could not be held liable, and struck down Sections 12 and 19 that would have allowed law enforcers to monitor and collect real-time traffic data without a court order.[52]

After a three-year delay, the DOJ released the Implementing Rules and Regulations (IRR) governing the act on August 12, 2015.[53] The IRR provides for the establishment of the Cybercrime Investigation and Coordinating Center, a central investigative body under the Office of the President. Law enforcement authorities tasked with investigating cybercrime, the National Bureau of Investigation and the Philippine National Police cybercrime unit, and have the power to collect or record any computer data, but only with a court order (Section 13).[54] Regarding the hotly-contested criminalization of online libel, DOJ Secretary De Lima stated that the justice department had wanted it out of the law from the beginning, but that it had a responsibility to include it in the IRR and enforce the provision.[55]

Other pending legislation could strengthen internet freedom. Senator Teofisto Guingona III filed a crowdsourcing bill in 2013. Also known as Senate Bill No. 73, the act would allow citizens to participate in the legislative process through the use of ICTs, and require lawmakers to include citizens' comments in committee reports concerning pending bills. If passed, it would make some important measures mandatory: people's committee hearings to be held in Congress (Section 6); continuous online participation by citizens while debates are being held on the floor (Section 7); and a pre-approval consultation (Section 8) wherein the president of the Philippines must allow people to send online comments about a pending bill for five days, and subsequently consider those comments for at least another three days, before signing a bill into law.[56] In early 2016, the Crowdsourcing Act has not gone beyond first reading.

Twenty-two years after it was first filed in Congress, the Senate approved the People's Freedom of Information Act of 2013 in March 2014.[57] In November, the lower chamber also approved the bill, which critics said was watered down.[58] The bill passed the Committee on Appropriations on March 4, 2015; the bill is awaiting second reading, the timeframe for which is not known.[59]

Prosecutions and Detentions for Online Activities

The Supreme Court's ruling in favor of punishing online libel under the Cybercrime Prevention Act resulted in a flood of charges. In a report released on August 27, 2015, the Philippine National Police

52 SC Decision, G.R. No. 203335, February 11, 2014, http://bit.ly/1EZnzAA.

53 Ina Reformina, "Anti-Cybercrime Law's IRR signed after 3 years," *ABS-CBN News*, August 13, 2015, http://bit.ly/1Sb7gmY.

54 Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012," http://bit.ly/1HN2kwq.

55 Vince Alvic A. F. Nonato, "New rules for cybercrime law iron out overlaps, official says" *Business World Online*, August 12, 2015, http://bit.ly/1WRYV9n.

56 SB 73 (73), "Philippine Crowdsourcing Act," http://www.senate.gov.ph/lisdata/1589313132!.pdf; The Guingona Project, http://theguingonaproject.com/.

57 Center for Media Freedom and Responsibility, "Freedom of Information: Timeline of FOI Legislation in the Philippines," http://bit.ly/1x81L21.

58 Xianne Arcangel, "House panel approves FOI bill," *GMA News Online*, November 24, 2014, http://bit.ly/1x6fdnh.

59 Official Gazette of the Republic of the Philippines, "Freedom of Information Bill update," http://www.gov.ph/foi/.

Anti Cybercrime Group reported an increase in cybercrime cases from 150 in 2013 to 1,211 in 2015,[60] including 240 libel cases.[61]

A number of high-profile examples came o light during the reporting period, though no-one was reported to have been detained as a result. On November 16, 2015, a judge dismissed a libel case filed by business oman Janet Lim Napoles against a reporter for the online news outfit *Rappler,* who reported on the lavish lifestyle of Napoles' daughter. In April 2015, Napoles was convicted of working with politicians to skim funds from a Priority Development Assistance Fund known as "the pork barrel" (see Digital Activism). In the libel case, the judge ruled that *Rappler's* report was neither "defamatory nor malicious."[62] Fashion blogger Michael Sy Lim was sued twice in late 2015 for allegedly publishing false accusations against another designer and an actress on his blog *Fashion Pulis*. While the actress dropped the charges in December,[63] the case involving the designer is pending.[64]

In a separate 2015 case involving online speech, the government initiated deportation proceedings against a Thai national after he posted derogatory statements about Filipinos on Facebook and in an online community page. He is not allowed re-entry to the country.[65]

Surveillance, Privacy, and Anonymity

A 2012 Data Privacy Act established parameters for the collection of personal financial info mation and an independent privacy regulator.[66] Other laws with privacy implications include the Anti-Child Pornography Act of 2009 which explicitly states that its section on ISPs may not be "construed to require an ISP to engage in the monitoring of any user,"[67] though it does require them to "obtain" and "preserve" evidence of violations, and threatens to revoke their license for noncompliance. Section 12 of the law also authorizes local government units to monitor and regulate commercial establishments that provide internet services. Under the Human Security Act of 2007, law enforcement officials must obtain a cou t order to intercept communications or conduct surveillance activities against individuals or organizations suspected of terrorist activity.[68] To date, no abuse of this law has been reported.

There are no restrictions on anonymous communication in the Philippines. The government does not require user registration for internet and mobile access, and prepaid services are widely available, even in small neighborhood stores. During this coverage period however, the senate renewed a proposal to make prepaid SIM card registration mandatory amid reports of increasing cybercrime, particularly child pornography. Senator Vicente Sotto III, the same lawmaker who pushed for online libel to be included in the cybercrime law,[69] presented the Cellphone Registration Act in a senate

60 Julian Love de Jesus, "Number of cybercrime cases surged in last 2 years—PNP-ACG," *Inquirer.net*, August 27, 2015, http://bit.ly/1RXKNHz.

61 Julian Love de Jesus, "Number of cybercrime cases surged in last 2 years—PNP-ACG," *Inquirer.net,* August 27, 2015, http://bit.ly/1RXKNHz.

62 Rappler.com, "Prosecutor junks Napoles' libel complaint vs Rappler reporter," January 18, 2016, http://bit.ly/1Rt2R1P.

63 Rappler.com, "Deniece Cornejo to drop libel complaint against Fashion Pulis," December 4, 2015, http://bit.ly/1RcH3Ci.

64 Alexa Villano, "Liz Uy on complaint against Fashion Pulis," *Rappler.com,* January 29, 2016, http://bit.ly/1Miw6SN.

65 Mong Palatino, "Philippines Deports Thai Worker for Insulting Filipinos on Facebook," May 9, 2015, http://bit.ly/29n1v6i.

66 Alec Christie and Arthur Cheuk, "Australia: New tough privacy regime in the Philippines Data Privacy Act signed into law," DLA *Mondaq*, October 27, 2012, http://bit.ly/1HVsGie; Rep. Act 10173 (2012), http://bit.ly/PcYtpj; Janette Toral, "Salient Features of Data Privacy Act of 2012 – Republic Act 10173," *Digital Filipino*, December 17, 2012, http://bit.ly/1Clq5hl/.

67 Rep. Act 9775 (2009), "Anti-Child Pornography Act of 2009," http://bit.ly/1Nshm2Y.

68 Rep. Act 9372 (2007), "Human Security Act," http://bit.ly/1UJSzXj.

69 Norman Bordadora, "Sotto admits he proposed online libel provision," *Inquirer.net*, October 2, 2012, http://bit.ly/1MsuUw9.

hearing on August 11, 2015, a proposal which telcos vigorously opposed. Globe stated that the bill violated people's right to privacy, citing the absence of data privacy in the bill;[70] and their right to communicate, citing a provision that prohibits people under the age of 15 from owning a registered SIM card.[71]

Intimidation and Violence

Violence against journalists is a significant p oblem in the Philippines. As of December 2015, the Committee to Protect Journalists reported at least 77 Philippine journalists had been killed in relation to their work—most covering political issues like corruption—since 1992.[72] An entrenched culture of impunity for these attacks sends the message that individuals exercising free speech can be attacked at will.

During his fi st press conference a month before being sworn in, President-elect Rodrigo Duterte said that journalists taking bribes or getting paid to attack or defend politicians deserve be killed.[73] "If you are an upright journalist, nothing will happen to you," he said. Local and international journalists' rights groups condemned the statement.[74]

There were no reports of physical violence targeting internet users during the coverage period of this report, though threats were sent using digital communication tools. In July 2015, several journalists in southern Mindanao reported receiving a text message from a group threatening them with "death by firing squad" for failing o cover a march organized by the group to promote their cause of recovering former Philippine territories.[75]

Technical Attacks

There have been no reports of politically motivated incidents of technical violence or cyberattacks perpetrated by the government toward private individuals. In previous years, the hacktivist group Anonymous Philippines attacked several government websites. Individuals claiming association with the group stepped up their defacing and hacking activity against government and celebrity websites in late 2015, posting invitations to join a peaceful global protest.[76] In March 2016, Anonymous warned the Commission on Election (Comelec) that it had deployed a dormant virus in voting machines in advance of May 2016 elections which would be activated if a machine's receipt feature, which verifies that a ote has been cast, was not switched on.[77]

70 Anna Estanislao, "Senate discusses Cellphone Registration Act," *CNN Philippines*, August 11, 2015, http://bit.ly/1RITRK8.

71 Leila B. Salaverria, "Telecom fi ms oppose SIM card registration bill," *Inquirer.net*, August 12, 2015, http://bit.ly/1odQjhb.

72 Committee to Protect Journalists, "77 Journalists killed in Philippines since 1992/Motive Confi med," Accessed April 28, 2016, http://bit.ly/1DrMpre.

73 Agence France-Presse, "Duterte endorses killing corrupt journalists," *Inquirer.net,* June 1, 2016, http://bit.ly/1P3ClpP.

74 Katerina Francisco, "Journalists' groups hit Duterte's justification f media killings," June 1, 2016, http://bit.ly/29n04EV.

75 Center for Media Freedom and Responsibility, "In Philippines, anti-communist group threatens journalists via SMS," July 20, 2015, https://www.ifex.org/philippines/2015/07/20/threats_usaffe_group/.

76 Victor Barreiro Jr., "Anonymous PH defaces gov't sites to promote rally," *Rappler.com*, November 3, 2015, http://bit.ly/1UtQF1Z.

77 "Anonymous warns: Virus will infect voting machines if receipts feature turned off," *InterAksyon.com*, March 23, 2016, http://bit.ly/1RsZmDq.

Freedom House

Russia

	2015	2016
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	10	10
Limits on Content (0-35)	23	23
Violations of User Rights (0-40)	29	32
TOTAL* (0-100)	**62**	**65**

* 0=most free, 100=least free

Population:	**144.1 million**
Internet Penetration 2015 (ITU):	**73 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- A package of antiterrorist legislative amendments known as Yarovaya's Law was proposed during the coverage period, and signed into law in July. The law undermines the security of encrypted communications and increases authorities' access to user data (see **Surveillance, Privacy, and Anonymity**).
- The past year saw a dramatic hike in arrests of social media users, with the first maximum five-year sentence issued for so-called extremist expression online (see **Prosecutions and Detentions for Online Activities**).
- An unprecedented number of attacks were registered against social media users in the past year, with members of political VKontakte groups targeted with physical violence and suffering property damage (see **Intimidation and Violence**).

Introduction

The Russian government continued to erode user rights, imprisoning social media users, while online activists have been targeted with violence and cyberattacks.

Internet freedom in Russia has deteriorated steadily over the past few years, as Vladimir Putin continues to consolidate power in his third term as president. The authorities have demonstrated a low tolerance for critical expression, readily blocking content critical of Russia's annexation of Crimea and involvement in the conflict in the Don ass region of Ukraine. Anti-extremism laws are widely used as a pretext to block political content, often without judicial oversight. Independent online news outlets continue to face legal and economic pressure from the government, and are often forced to take down politically sensitive content or otherwise face retaliatory action. LGBTI social media groups and websites are also routinely censored, as well as websites run by the political opposition.

The past year saw an unprecedented crackdown on social media users, with the authorities issuing long prison sentences and applying other legal sanctions against users who post or even share material online that contradicts the official K emlin position on controversial issues. While the coverage period saw the fi st maximum fi e-year sentence issued in December 2015 to a social media user under Russia's broad anti-extremism laws, a new law passed in July 2016 increases the maximum sentence to seven years for "inciting" or "justifying" terrorism online, expanding the powers of authorities to target social media users. Social media users who are openly critical of the Russian regime have also faced a targeted campaign of physical violence and acts of intimidation, often perpetrated by unidentified assailants encoun ered on the street or near their homes.

The Russian government has continued to undermine citizens' privacy and security online, passing laws which grant the authorities greater legal access to personal data and more power over tech companies. Data localization rules, which entered into force in September 2015, may make it easier for the Russian government to access internet users' information. Coupled with new laws passed in July 2016 mandating extensive data retention, conditions are rife for future infringements on users' right to privacy.

Obstacles to Access

Access to the internet is affordable in Russia and connection speeds are high compared to the rest of the region, while internet penetration rates continue to increase. However, the ICT industry is concentrated, with a state-owned ISP dominating the market and planning to expand.

Availability and Ease of Access

Internet access in Russia continues to gradually expand. According to the Public Opinion Foundation, the internet penetration rate reached 57 percent by the end of 2015, compared with 51 percent by the end of 2014.[1] The International Telecommunication Union (ITU) places the figu e somewhat

1 Public Opinion Foundation, "Internet in Russia: Dynamics of Penetration. Winter 2015-2016" [in Russian], April 22, 8, 2016 http://ow.ly/uj5Q300xtdl.

higher, reporting an internet penetration rate of 73 percent by the end of 2015, compared to 71 percent in 2013 and just 29 percent in 2009.[2]

The speed of access is also increasing. According to Akamai, Russia was one of 20 countries in the third quarter of 2015 with average connection speeds at, or above, 10 Mbps. This is 12 percent higher than in 2014, and places Russia far ahead of other post-Soviet states. However, connection speeds remain behind top-performing countries such as Sweden, which enjoys a connection speed of 17.4 Mbps.[3]

According to TNS Russia, 62 percent of Russians living in cities with over 100,000 inhabitants use smartphones to access mobile internet, and 34 percent access the web via tablets. Meanwhile, 59 percent of Russians in this group use home computers and 53 percent use laptops.[4] According to the ITU, the mobile phone penetration rate reached 160 percent in 2015,[5] indicating a greater number of subscriptions than inhabitants; for mobile broadband subscriptions, the rate was 65.9 percent.[6]

The average cost of a monthly internet plan in Russia is approximately US$6 (RUB 400) for 3 Mbps.[7] Though there is no significant gender divide when it comes o internet access in Russia,[8] a regional divide persists with respect to internet speed and price. Inhabitants of the subarctic cities of Yakutsk and Novy Urengoy pay the highest prices in Russia, more than double the national average for monthly internet access.[9]

The average cost of internet access makes up approximately 1 percent of an average salary, indicating that access is relatively affordable for most citizens. According to figu es cited by the authors of the study Economics of the Russian Internet 2013–2014, only 4 percent of Russians stated that they could not afford to access the internet.[10] The median monthly income of Russia citizens according to the Ministry of Labor and Social Protection was US$499 (RUB 30,514) in the third quarter of 2015.[11]

Nevertheless, while people with median and higher incomes can easily afford the internet, 20.3 million Russians—nearly 14 percent of the population—lived below the poverty line as of the end of 2015. This is an increase of 2 million from the previous year.[12]

Restrictions on Connectivity

During the coverage period, there were no government-imposed internet outages or disruptions to communication platforms. However, certain bills currently under discussion may make it easier for the government to do so in the future. In February 2016, *Vedomosti*, a business daily, reported that the Communications Ministry was in the early stages of drafting a bill titled "On the Autonomous Internet System," which seeks to increase government control over internet infrastructure in Russia by

2 International Telecommunication Union, "Percentage of Individuals Using the Internet," 2000–2015, http://bit.ly/1cblxxY.
3 Akamai, "State of the Internet Q3 2015 Report", .
4 TNS Russia, "TNS Web Index", April 2016, http://ow.ly/pAWV300xrJW.
5 International Telecommunication Union, "Percentage of individuals using the Internet," 2015, http://bit.ly/1cblxxY.
6 Broadband Commission, *The State of Broadband 2015: Universalizing Broadband,* September 2015, http://bit.ly/ICdQnO.
7 Yandex. "Internet in Russian regions" [in Russian], Spring 2016. http://ow.ly/mGWQ300CBd5
8 TNS Russia, "TNS Web Index", April 2016, http://ow.ly/pAWV300xrJW
9 Yandex, "Internet in Russian regions" [in Russian], Spring 2016, http://ow.ly/mGWQ300CBd5.
10 Russian Association of Internet Communication and Higher School of Economics, Economics of Runet.
11 Ministry of Labor and Social Protection, "Per capita incomes in the Russian Federation" [in Russian], December 18, 2015, .
12 Georgy Peremitin, "The number of the poor in Russia increased by more than two million in 2015" [in Russian], *RBC*, December 10, 2015, .

transferring control of traffic e change points and .ru and .pф domains to the government. Further, the bill seeks to control international internet traffic in Russia by equiring operators of autonomous systems to set up SORM, the system Russia uses to conduct state surveillance[13] (see Surveillance, Privacy, and Anonymity).

In May 2016, the Ministry of Telecommunications and Mass Communications published amendments to its state program "Information Society", aiming to bring 99 percent of Russian internet traffic within Russian bo ders by 2020, compared to 70 percent in 2014.[14] The ministry plans to establish a system for monitoring the connectivity and network stability in the Russian segment of the Internet, claiming that these changes will bring increased stability to internet, safeguarding it from foreign interference or disconnection. However, observers such as Alexey Platonov, director of the "Technical Center Internet," which provides technical support for domain infrastructure in Russia, have suggested that the changes resemble a move towards the Chinese Firewall model. The move may increase the authorities' ability to block international traffic and po entially cut Russia's network off from the rest of the world.[15]

ICT Market

The communications market in Russia is still relatively concentrated among a few companies. State-owned Rostelecom controls 37 percent of the broadband internet market, followed by ER-Telecom with 9 percent, MTS with 9 percent, and Vimpel Communications (Beeline) owning 7 percent. The remaining market share is split among smaller, local ISPs.[16] Rostelecom plans to expand further, and will spend approximately US$163 million (RUB 10 billion) on mergers and acquisitions to sustain and grow its market share.[17] The market for mobile phone access is similarly concentrated. In the fi st quarter of 2016, four major companies—Mobile TeleSystems, Megafon, Vimpel Communications, and Tele2—controlled 99 percent of the market.[18]

Regulatory Bodies

The ICT and media sector is regulated by the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor), under the control of the Ministry of Communications and Mass Media. The head of Roskomnadzor, Aleksandr Zharov, was appointed by executive decree on May 3, 2012. Roskomnadzor is responsible for carrying out orders issued by the Prosecutor General's Office o block content that is extremist or contains calls for participation in unsanctioned public actions, according to a law that went into effect on February 1, 2014. As a result, Roskomnadzor has become a primary player in the field f controlling and fil ering information on the internet. In addition to conducting its own monitoring of the internet, Roskomnadzor receives

13 Anastasia Golitsyna, Elizabeth Sergina Peter Kozlov "The government wants to control the internet traffic in the count y" [in Russian], *Vedomosti*, February 11, 2016, http://ow.ly/ZTJJt. Under the bill, domain name systems would be associated with IP address assignment, and a traffic moni oring system would be introduced.

14 Pavel Kantyshev, Anastasia Golitsyna "Russian internet will be completely isolated in 2020" [in Russian], *Vedomosti*, May 13, 2016, http://ow.ly/3eHq300CCja.

15 Alyona Sukharevskaya, ""Hints of China": whether it is possible to turn off Russia from the global Internet" [in Russian], *RBC*, February 11, 2016, http://ow.ly/ZTKs9.

16 ICT Online, "TMT Consulting" published the rating about broadband Internet in Russia in 2015 [In Russian], February 16, 2016, http://ict-online.ru/news/n128614/.

17 Vladislav Novy, Denis Skorobogatko, Anna Balashova, "Rostelecom is going shopping," *Kommersant*, November 20, 2015,

18 Advanced Communication & Media, "Cellular Data, Q4 2014," accessed July 14, 2016, http://www.acm-consulting.com/news-and-data/data-downloads/doc_download/140-1q-2015-cellular-data.html.

complaints about online content from the public, the courts, and other official bodies such as the General Prosecutor's Office [19] Roskomnadzor is also in charge of implementing the so-called "Bloggers' Law," requiring bloggers with more than 3,000 daily readers to register with the regulator.

Limits on Content

The Russian authorities censor a wide range of topics online, most often under the pretext of anti-extremism measures. Content subject to blacklisting or removal includes LGBTI expression, the conflict in Ukraine, and political opposition. The authorities have also pressured international platforms, such as Wikipedia, into removing select pages. Online outlets are subject to political and economic pressure to publish Kremlin-friendly content, while the government actively manipulates public opinion through state-controlled media and paid commentators.

Blocking and Filtering

Within the coverage period, Russian authorities have continued to use anti-extremism legislation to restrict access to content related to radical Islam, political opposition, nationalism, the conflict with Ukraine, and other topics. According to the SOVA Center for Information and Analysis, a Moscow-based nonprofit, many ebsites continue to be blocked without proper justification [20]

From 2012 to 2013 the Russian government enacted legal amendments that gave several agencies—including Roskomnadzor, the Prosecutor General's Office, the Federal Se vice for Surveillance on Consumer Rights and Human Wellbeing (Rospotrebnadzor), and the Federal Drug Control Service—the authority to make decisions about blocking various categories of information. Currently, these agencies have the authority to block the following types of content without a court order: information about suicide, drug propaganda, child pornography, information about juvenile victims of crimes, materials that violate copyright, content related to extremism, and calls for unsanctioned public actions or rallies. Any other information may be blocked by a court order, provided that the court finds the con ent illegal.

According to the nonprofit o ganization RosComSvoboda, which conducts ongoing monitoring of blocked content, the following were blocked by the end of May 2016:

- 1,587 sites for extremism and calls for protests (by orders of Prosecutor General's Office
- 9,982 sites containing drug-related content (by orders of the Federal Drug Control Service)
- 228 sites containing suicide propaganda (by orders of the Federal Service for Surveillance on Consumer Rights Protection and Human Wellbeing, or Rospotrebnadzor)
- 5,253 sites for the distribution of child pornography (by orders of Roskomnadzor)
- 9,593 sites for the publication of various prohibited information (based on court decisions)
- 1,465 sites for copyright infringement (based on decisions of Moscow City Court)

19 Daniil Turovsky, "How Roskomnadzor operates" [in Russian], *Meduza*, March 13, 2015,

20 Marya Kravchenko, Alexander Verhovsky, "Misuse of anti-extremism legislation in Russia in 2015" [in Russian], *Sova Center*, March 2, 2016 http://www.sova-center.ru/misuse/publications/2016/03/d33946/.

- 6,313 sites for information about gambling (by orders of the Federal Tax Service).[21]

Ukraine and Crimea remain areas of particular sensitivity for Russian authorities, with numerous Ukrainian websites blocked from within Russia. Ukrainian news websites Korrespondent.net, Bigmir.net, and Liga.net were blocked without a court order for quoting Refat Chubarov, the leader of the Crimean Tatar national movement in Ukraine, as saying that Crimea should be returned to Ukraine.[22] In May 2016, Krym.Realii ("Crimea.Realities"), a project of Radio Free Europe/Radio Liberty, was blocked within Russia and Crimea by Roskomnadzor after Crimea's de facto Prosecutor-General called for the website's closure for allegedly inciting inter-ethnic hatred and extremism.[23] Additionally, the website of the Consumer Rights Defenders Society was blocked for several months until September 2015, after the group posted an article recommending that Russian travelers to Crimea enter through Ukraine, a statement seen by some as undermining Russia's sovereignty in Crimea. Roskomnadzor blocked the site on extremism grounds according Federal law 398, known as "Lugovoi's law," which allows authorities to block websites for extremism on the orders of the Prosecutor General Office without a cou t order.

The authorities continue to censor information online on political opposition, including the website of opposition leader Garry Kasparov which was originally blocked in 2014 by Roskomnadzor for containing calls to illegal activity.[24] Two websites— srywwyborow.blogspot.ru and activism.win—were blocked by Roskomnadzor in July 2016 for posting calls to boycott upcoming legislative elections. A Roskomnadzor spokesman described the websites as pure propaganda.[25] Roskomnadzor also temporarily blocked the website of the Communist workers movement, work-way.com, after it posted articles related to an upcoming truck-drivers' strike.[26]

In cases where websites employ the HTTPS protocol, which prevents ISPs from blocking individual pages within the domain, ISPs are often forced to block entire platforms in order to comply with Roskomnadzor's instructions to block a single page. For example in June 2015, the Internet Archive, a platform which allows users to view webpages that have been modified or emoved, was blocked in its entirety after Roskomnadzor banned a saved webpage called "Solitary Jihad in Russia."[27] Similarly, ISPs temporarily blocked all of Wikipedia and Reddit in August 2015 after an order from Roskomnadzor banning articles related to recreational drug use.[28]

In most cases the legal framework offers no clear criteria for evaluating the legality of content, and public authorities do not always offer a detailed explanation for blocking decisions. The lack of precise guidelines sometimes leads telecom operators, which are responsible for complying with block-

21 RosComSvododa, "Distribution of blocked sites across departments" [in Russian]. Accessed on July 18, 2016, https://reestr.rublacklist.net/visual/.

22 SOVA Center for Information and Analysis, "Chronology of the Internet filtration in Russia" [in Russian], Februa y 29, 2016, http://www.sova-center.ru/misuse/publications/filtr/2016/01/d33687 .

23 TASS, "Online media "Crimea.Realities" is banned in Russia" [in Russian], May 16, 2016, http://special.itar-tass.com/politika/3274509.

24 "Russia blocks internet sites of Putin critics,' Reuters, March 13, 2014, http://www.reuters.com/article/us-russia-internet-idUSBREA2C21L20140313.

25 SOVA Center for Information and Analysis, "Chronology of the Internet filtration in Russia" [in Russian], July 8, 2016, http://www.sova-center.ru/misuse/news/elections/2016/07/d35001.

26 SOVA Center for Information and Analysis, "Chronology of the Internet filtration in Russia" [in Russian], Februa y 29, 2016, http://www.sova-center.ru/misuse/publications/filtr/2016/01/d33687 .

27 Kevin Rothrock, "Russia Bans the Internet Archive's 'Wayback Machine,'" *Global Voices*, June 25, 2015, http://ow.ly/ZVex2.

28 Shaun Walker, "Russia briefly ans Wikipedia over page relating to drug use," *Guardian*, August 25, 2015, http://bit.ly/1hbjdvn; Andrew Griffin, " eddit banned in Russia because of one thread," *Independent*, August 13, 2015, http://ind.pn/1PvYKzY.

ing orders, to carry out the widest blocking possible so as to avoid fines and th eats to their licenses. Telecom operators are obliged to regularly consult the "blacklist" of banned websites, updated by Roskomnadzor. Moreover, the law does not specify how ISPs should restrict access; for example, based on the internet protocol (IP) address, the domain name, or the URL of the targeted page. Often the authorities do not consider it necessary to clearly indicate the specific ages that are meant to be blocked on a given site. According to RosComSvoboda, 93 percent of accidental blockings occurred due to blocking orders carried out on the basis of IP addresses.[29]

The head of Roskomdanzor, Alexander Zharov, announced in December 2015 that the regulatory body is in the process of launching an automated online content analysis and fil ering system. The technology, which will assist Roskomnadzor in identifying content to be blocked, has been test-launched in 19 regions across the country.[30] Some regions, such as Tatarstan, have separately introduced automated content monitoring systems. [31]

Providers of public internet access, including libraries, cafes, and educational institutions, are responsible for ensuring that the content available to their users is fil ered in compliance with Article 6.17 of the administrative code on protecting children from harmful information.[32]

Content Removal

Roskomnadzor typically receives orders from government bodies, including the Prosecutor General's Office and Federal Drug Cont ol Service, to enforce the censorship of content deemed illegal and, in some cases, Roskomnadzor itself identifies illegal con ent. Roskomnadzor must then instruct the hosting provider to issue a warning to the website. Website owners have the right to appeal the restriction in court, but are often given a short window of time to do so. As a result, website owners quickly delete the banned information, rather than risk having the entire site blocked. If the content is not removed, the page is then included on a blacklist and must be blocked by ISPs within 24 hours after receiving a warning from Roskomnadzor. ISPs face fines for failing o block websites included on Roskomnadzor's blacklist.

In cases where websites are registered as mass media, Roskomnadzor has additional powers to issue warnings to the editorial board about "abuse of freedom of mass media." Article 4 of the law "On Mass Media" implies that such abuse can include, for example, incitement to terrorism, extremism, propaganda of violence and cruelty, information about illegal drugs, and obscene language. If a media outlet receives two warnings within a year, Roskomnadzor has the right to apply for a court order to shut down the media outlet. Usually, the warnings from Roskomnadzor contain instructions to remove or edit the offending material. "Open Russia," an online portal launched by opposition figu e Mikhail Khodorkovsky, was urged to delete an article about a demonstration in the memory of murdered opposition leader Boris Nemtsov.[33] Similarly, *The New Times*, a Moscow-based publication that

29 RosComSvododa, "Distribution of blocked sites across departments" [in Russian]. Accessed on July 18, 2016, https://reestr.rublacklist.net/visual/.

30 Vladimir Zykov, "Roskomnadzor tests a monitoring system to analyze online media" [in Russian], Izvestia, December 25, 2015, http://ow.ly/ZTVLX.

31 Official si e of the prosecutor's office f Tatarstan, "Tatarstan Prosecutor's Office continues o implement large-scale project to counter offenses on the internet," [in Russian], December 16, 2015, http://ow.ly/ZTXno.

32 Sova Center, "Inappropriate enforcement of anti-extremist legislation in Russia in 2015," June 6, 2016, http://www.sova-center.ru/en/misuse/reports-analyses/2016/06/d34694/.

33 SOVA Center for Information and Analysis, "Chronology of the Internet filtration in Russia" [in Russian], anuary 25, 2016, http://www.sova-center.ru/misuse/publications/filtr/2016/02/d33930 .

is critical of the Kremlin, received a warning about an article in February 2016 for failing to mention that the Ukrainian ultra-nationalist group Right Sector is banned in Russia. Interestingly, *the New Times* received this warning on the same day it published an investigative article about President Putin's daughter, raising speculation that the warning was retaliation for publishing about Putin's secretive family. [34]

In August 2015, Wikipedia was temporarily blocked in Russia for less than a day after Russian authorities were unsuccessful in removing a single Wikipedia article about "charas," a form of cannabis, due to Wikipedia's HTTPS protocol. Though access to Wikipedia was promptly restored, some have speculated that this could be part of a wider strategy to threaten platforms such as Wikipedia with bans over single pages in order to, ultimately, force them to give up on HTTPS, allowing the authorities to conduct targeted blocking. [35] Roskomnadzor had reportedly failed to provide Wikipedia with the appropriate warning prior to blocking.[36] Wikipedia's community of authors voted to remove the offending content in order to safeguard Wikipedia in Russia, and the article was ultimately edited so as to comply with Russian law.[37]

Russian authorities continue to target LGBTI groups on social media. In September 2015, Roskomnadzor ordered VKontakte to block fi e accounts of LGBTI groups on the social media platform, after a court in Barnaul found that the pages constituted illegal "gay propaganda." The most prominent of these groups was Children-404, a support group for Russian LGBTI teenagers. VKontakte complied with the order, claiming that Roskomnadzor would have otherwise blocked the social media platform in its entirety.[38]

Foreign companies do not always comply with the demands of Russian authorities. According to a transparency report from Twitter, Russian authorities submitted 1,735 requests for content removal between July and December 2015—a 25-fold increase on the previous year. Twitter found that only 5 percent of these requests constituted a violation of the company's rules.[39] In July-December 2015, Facebook complied with 56 requests issued by Russian authorities to restrict content, up from 28 in the prior six months. [40] Meanwhile, Google received 1,570 requests from the Russian government to restrict content from July-December 2015, complying in more than 75 percent of cases. Russia accounted for 32 percent of the total requests Google received in this period.[41]

In July 2015, President Putin approved a law on "the right to be forgotten," requiring search engines to remove links to false or outdated information about an individual.[42] The petitioning individual must prove that the information warrants removal, though a court order is not required. Russia's search engine, Yandex, had voiced opposition to the law, highlighting that altering search results vi-

34 Alec Luhn, "Russian magazine cyber-attacked and fined a ter article on Putin's daughter," *The Guardian*, February 1, 2016, http://ow.ly/ZYfGY.

35 Shaun Walker, "Russia briefly ans Wikipedia over page relating to drug use," *The Guardian*, August 25, 2015, http://ow.ly/ZVcpb.

36 Stanislav Kozlovky, a message on Facebook to the author, March 23, 2016.

37 Shaun Walker, "Russia briefly ans Wikipedia over page relating to drug use," *The Guardian*, August 25, 2015, http://ow.ly/ZVcpb.

38 "Access to Children 404 group blocked for VKontakte users in Russia," *Russia Beyond the Headlines,* September 25, 2015, https://rbth.com/news/2015/09/25/access_to_children-404_group_blocked_for_vkontakte_users_in_russia_49555.html.

39 Twitter transparency report, http://ow.ly/ZVeSB.

40 Facebook, "Report on governmental requests" [in Russian], https://govtrequests.facebook.com/country/Russia/2015-H2/.

41 Google, "Transparency Report--Russia," https://www.google.com/transparencyreport/removals/government/RU/?hl=en.

42 Tetyana Lokot, "President Putin Signs Russian 'Right to Be Forgotten' Into Law", *Global Voices*, July 17, 2015, http://ow.ly/ZVkr3.

olates the constitutional right to seek, obtain, produce, and spread information,[43] in addition to raising concerns regarding the added burden placed on the company to make decisions about which content to remove. Though "right to be forgotten" laws exist in other jurisdictions, Russia's law fails to provide limits in cases where the information relates to the public good or pertains to public fi - ures.[44] In March 2016, three months after the law had been enacted, Yandex released data showing it received 3,600 removal requests, 51 percent of which were requests to remove truthful, but outdated information, often related to crimes. Yandex approved 27 percent of the requests it received.[45]

Search engines and news aggregators such as Google News and Yandex.Novosti (Yandex News) will be placed under additional pressures once an amendment to the Law on Information, Information Technology and Data Protection, passed in June 2016, enters into force in January 2017.[46] The new law will require aggregators with over one million daily users to prevent the dissemination on their platforms of terrorist content, pornography, cruelty, the disclosure of state secrets, and other content, facing fines if they do not compl .[47] News aggregators will also be responsible for the accuracy of some of the information disseminated through their platforms with some exceptions, such as direct quotes from the media.[48] Russian news aggregators like Yandex and Mail.ru have strongly pushed back against the amendments, calling the measures excessive and arguing that it may become impossible to provide their services under the new regulations.[49]

Media, Diversity, and Content Manipulation

As the space for independent print and broadcast media in Russia shrinks, online publications and social networks become increasingly important platforms for critical expression and social mobilization, with 48 percent of Russians now turning to the internet to find trust orthy news sources.[50] However, while Russians are still able to access a wide variety of outside sources, many independent online media outlets within Russia have been forced to shut down over the past two years due to increasing pressure from the government. Self-censorship is encouraged by the vague wording of restrictive legislation, the seemingly arbitrary manner in which these laws are enforced, and the near-total ineffectiveness of judicial remedies. Laws prohibiting "extremist content" and the government's crackdown on several media outlets have resulted in a chilling effect on free speech, particularly with regard to such sensitive topics as governance failures, corruption, war with Ukraine, the annexation of Crimea, violations of civil rights, religion, and the LGBTI community.

Several online media outlets that were originally blocked in March 2014 remain restricted, including Grani.ru, Kasparov.ru, and Ej.ru. A number of other media outlets have received warnings from Roskomnadzor for their coverage of protests, the attack on Charlie Hebdo, or the criminal cases of Aleksey Navalny, meaning they run the risk of receiving a second warning and losing their licenses. While

43 Yandex, "Right to forget about search," [in Russian] June 5, 2015, http://ow.ly/ZVkLE.

44 Article 19, "Legal analysis: Russia's right to be forgotten," September 16, 2015, https://www.article19.org/resources.php/resource/38099/en/legal-analysis:-russia's-right-to-be-forgotten.

45 Yandex, "About the implementation of the right to be forgotten," [in Russian] March 25, 2016, http://ow.ly/ZVlfR.

46 Consultant Plus, Act 208, June 23, 2016, http://www.consultant.ru/document/cons_doc_LAW_200019/.

47 Ekaterina Bryzgalova, "Deputies satisfied demands f the Internet industry" [in Russian], *Vedomosti*, June 13, 2016, https://www.vedomosti.ru/technology/articles/2016/06/14/645179-novostnim-agregatoram.

48 "The draft law about news aggregators passed Duma," [in Russian] *BBC Russian,* June 10, 2016, http://www.bbc.com/russian/news/2016/06/160610_duma_news_agregator.

49 Anastasia Golitsyna, "Mail.Ru Group may close its news service," [in Russian] *Vedomosti*, April 21, 2016, http://ow.ly/cWou300CNGQ.

50 Public Opinion Foundation, "News on the internet", January 25, 2016, http://ow.ly/ZYd7X.

individuals are still able to use circumvention tools to access blocked content, officials at arious levels have repeatedly spoken about the need to block access to such tools, though legislation to that effect has not yet been adopted. Despite the continued availability of some circumvention tools, all blocked resources have reported a significant eduction in traffic.

Online outlets continue to face government pressure to publish news in line with the Kremlin's views. In the spring of 2015, hackers published leaks of correspondence from the deputy head of the Office of Internal Policy of the Presidential Administration, which indicated that the administration is actively involved in a number of media outlets' editorial policies and uses Roskomnadzor and the Prosecutor General's Office o exert pressure on those who resist such directives.[51]

One of the few independent major media outlets, RBC, owned by Russian billionaire Mikhail Prokhorov, sacked its key managers and reporters in May 2016, reportedly under the pressure from Kremlin.[52] RBC was renowned for its critical investigatory journalism exposing corruption, often targeting Putin and his inner-circle. The RBC website alone had 11,765,000 monthly readers in Russia in April 2016, and was the only major media outlet in Russia to report on Putin's links to the Panama Papers revelations. Elizaveta Osetinskaya stated that the publication had become a "red rag" for the Kremlin because of its critical coverage of the Panama papers, though the Kremlin denied any involvement in the sacking of RBC's top editors.[53]

Russian authorities continue to use the assistance of paid commentators to influence online con ent. In March 2015, journalists at *Novaya Gazeta* and the St. Petersburg outlet *Moy Rayon* published an investigation into the activity of pro-Kremlin paid commentators, revealing more than 500 accounts on the LiveJournal blogging platform that specialized in the publication of progovernment views and the harassment of opposition activists. Media outlets including *Forbes* and *the Guardian* have reported increases in anti-Western user comments on any comments related to Russia or Ukraine.[54] The issue of progovernment trolling gained significant at ention in Russia in May 2015 when the Internet Research Agency, a "troll factory" located in St. Petersburg, was sued by a former employee to bring the activities of the agency to public attention, a case which received much media attention domestically and internationally.[55] In an attempt to counter the prevalence of government manipulation in the media, Alexey Kovalev, a former employee of state-friendly media outlet RIA Novosti (now Rossiya Segodnya), created an online platform called Noodle Remover, which aims to debunk false or misleading news published in the Russian media. [56]

Authorities have continued to introduce onerous regulatory requirements and restrictive laws affecting online media, pushing some outlets to downsize, sell, or exit the market altogether. On January 1, 2016, new amendments to the Law on Mass Media came into force, prohibiting foreign citizens and organizations from owning more than a 20 percent stake in Russian media. As a result, foreign media holdings are leaving Russia and, in some cases, ownership is being transferred to Russian entities.[57] For instance, German publishing house Axel Springer sold its assets, including *Forbes* (the

51 "The modern history of the Russian policy told in SMS," [in Russian] *Insider*, April 1, 2015, http://bit.ly/1IRolhh.

52 Ksenia Boletskaya, "RBC is not approved for reading," [in Russian] *Vedomosti*, May 13, 2016 http://ow.ly/E9yx300CFxU.

53 Max Seddon, "Editors at Russia's RBC media group sacked after Putin article," *Financial Times*, May 18, 2016, http://ow.ly/iJX3300CG5T.

54 Annika von Taube, "Russische Botschaft" [in German], *Zeit Online*, January 27, 2014, http://bit.ly/1GQlUJ7.

55 Adrian Chen, "The Agency," *The New York Times*, June 2, 2015, http://ow.ly/ZYdJu.

56 Kevin Rothrock, "One Man's Revenge Against Russian Propaganda," *Global Voices*, November 3, 2015, http://ow.ly/ZUduA.

57 Anastasia Bazenkov, "Foreign publishers quit Russia over media ownership law," *Moscow Times*, September 9, 2015, http://ow.ly/ZYf2C.

magazine and the website Forbes.ru), to Alexander Fedotov, the owner of Artcom Media Group. Sanoma Corp, a Helsinki-based media group, sold its share of the company that produces *Vedomosti*, a business daily and news portal (Vedomosti.ru), to Demyan Kudryavtsev, the former publisher of business media outlet *Kommersant*. Many observers regard the new local ownership requirements as an attempt by the Kremlin to secure greater influence and edi orial control over these high-reach news outlets.[58] Furthermore, in May 2015, a new law on "undesirable organizations" introduced bans on disseminating information from blacklisted organizations, silencing many civil society voices. Individuals and smaller, independent outlets have been targeted by the "Bloggers' Law." Introduced in May 2014, the law requires sites with 3,000 or more daily visitors to register as a mass media outlet, which means bloggers can no longer remain anonymous and are held responsible for the accuracy of the content posted on the website, including comments made by third parties.

In response to the increasingly restrictive environment for independent online commentary, some publications choose to operate overseas. Perhaps the most notable example is Meduza.io, a critical online news outlet launched in Latvia. Meduza targets Russian audiences, reaching approximately 4 million monthly visitors,[59] and also publishes some content in English.

Another legislative development likely to curb online media diversity came in the form of a data localization law (Federal Law No. 242-FZ). The law entered into effect in September 2015, and requires companies to store personal data pertaining to Russian citizens on servers located in the country. In addition to surveillance and privacy concerns, the law is likely to force foreign tech companies out of Russia, with Spotify already reversing plans to enter the Russian market partly due to its inability to comply with data localization requirements as a cloud-based service.[60]

Digital Activism

Despite continued government pressure, the internet remains the most versatile and effective tool for activism in the country, with frequent efforts to confront state propaganda, fight corruption, and organize protests. Videos exposing corruption on prominent activist Alexey Navalny's YouTube channel frequently receive millions of views. A 2015 video exposing links between general prosecutor Yuri Chaika and the Tsapok gang, the criminals behind a notorious massacre in the town of Kushevskaya in southern Russia,[61] has been viewed over 5 million times. The Chaika investigation has had a notable impact on the Russian public, with a study by *Kommersant* finding that 38 pe cent of Russians have at least heard of the YouTube video, and 78 percent believe it to be accurate.[62]

Individuals are also creating online platforms and organizations to expose and scale back restrictions imposed on the internet in Russia. In December 2015, IT professional Leonid Volkov launched the Society for Defending the Internet (OZI), an organization working to defend internet freedom.[63] OZI has launched an online crowdfunding campaign to support its efforts to challenge the legality of SORM, technology used by the FSB to conduct surveillance online, ultimately aiming to creates a so-

58 Peter Hobson, "Russian Owner Wants Modernised Moscow Times, Not Kremlin Stooge," *The Moscow Times*, May 4, 2015, http://bit.ly/2dtd3ok.

59 Ilya Krasilchik, Facebook post [in Russian], April 1, 2016, http://ow.ly/tLku300CNxt.

60 Darya Luganskaya, "Spotify changed its mind to enter the Russian market," [in Russian] *RBC*, February 2, 2015, http://ow.ly/ZVnA3.

61 FBK, "Chaika" [in Russian], December 1, 2015, http://ow.ly/ZUbtn.

62 Andrey Pertsev, "Almost half of Russians know about the film Chaika' about the family of general prosecutor,"[in Russian] *Kommersant*, December 23, 2015, http://ow.ly/ZUcuh.

63 Kevin Rothrock,"ISPs Take Kremlin to Court Over Online Surveillance," *Global Voices*, February 3, 2016, http://ow.ly/ZUdkp.

called "people's ISP" that would then sue the FSB once it is required to install SORM technology.[64] By July 2016, the activists had successfully obtained the necessary license to operate as an ISP.[65]

Ruslan Leviev, an activist and programmer, established Conflict In elligence Team (CIT), an online platform which publishes investigations into the actions of Russian troops in Ukraine and Syria, often using information sourced from social networks.[66] Leviev's team was the fi st to reveal evidence of the deployment of Russian soldiers in ground operations in Syria, using the geolocations of photos found on social media.[67] CIT aims to bring more transparency to the Russian government's involvement in foreign conflicts [68]

Violations of User Rights

Over the past year, Russian authorities substantially restricted user rights by passing laws which increase penalties for expression online while expanding the government's access to personal data. More social media users than ever before faced arrests for voicing their criticism, and many face lengthy prison sentences. The authorities have taken steps to undermine the security of encrypted communications, passing a law in July 2016 that will compel encryption providers to grant access to authorities, a move which is likely to expose more netizens to legal sanction for their activities online.

Legal Environment

Although the constitution grants the right to free speech, this right is routinely violated, and there are no special laws protecting online expression. Online journalists do not possess the same rights as traditional journalists unless they register their websites as mass media. Russia remains a member of the Council of Europe and a party to the European Convention on Human Rights and Fundamental Freedoms, which enshrines the right to freedom of expression. However, over the past few years Russia has adopted a set of laws and other acts that, coupled with repressive law enforcement and judicial systems, have eroded freedom of expression in practice. Courts tend to side with the executive authorities, refusing to apply provisions of the constitution and international treaties that protect the basic rights of journalists and internet users.

In July 2016, the Russian government introduced some of the harshest legislative amendments in post-Soviet Russia, collectively known as "Yarovaya's Law," amending nearly a dozen laws with wide ramifications for in ernet freedom.[69] The laws introduce prison terms of up to seven years for publicly calling for or justifying terrorism online.[70] The harsh penalties and broad wording of the law opens the door to abuse, namely the targeting of legitimate, nonviolent expression online.

64 Interview with Leonid Volkov conducted in March 2016.

65 Leonid Volkov, "The People's ISP: Step 2" [in Russian], *leonidvolkov.ru*, July 5, 2016, http://www.leonidvolkov.ru/p/147/.

66 Darya Luganskaya, "Inside Big Brother: How Russians Created the 'Red Web,'" *Global Voices*, November 17, 2015, http://ow.ly/ZUefL.

67 "Russian soldiers geolocated by photos in multiple Syria locations," *Reuters,* November 8, 2015, http://www.reuters.com/article/us-mideast-crisis-syria-russia-idUSKCN0SX0H820151108.

68 Interview with Ruslan Leviev conducted in Moscow on March 26, 2016.

69 Consultant Plus, Act 375, Amendment to the Russian Criminal Code, Introducing Additional Counterterrorism Measures and Ensuring Public Safety, http://bit.ly/2dt782G.

70 Consultant Plus, Act 375, Amendment to the Russian Criminal Code, Introducing Additional Counterterrorism Measures and Ensuring Public Safety, http://bit.ly/2dt782G.

Penalties for extremist had been raised only a couple of years previously, with the passage of a series of amendments to the criminal code in 2014. The amendments significantly inc eased the penalties for online incitement to separatism or calls for extremism,[71] with prison terms up to fi e years, and incitement to hatred, with prison terms up to six years.[72] In addition to the criminal penalties, the mere opening of a criminal case could serve as a basis for the inclusion of the accused on a list of extremists maintained by the Federal Financial Monitoring Service. Individuals on this list are restricted from certain professions and their bank accounts can be frozen, even if they have not been convicted.

Russia's anti-extremism law is particularly broad as, according to Andrei Richter, Senior Advisor at OSCE Office f the Representative on Freedom of the Media. Richter noted Russia penalizes expression which is not necessarily abusive or discriminatory in nature.[73] Moreover, the interpretation of extremism in Russian has gradually expanded to include not only incitement of national, racial or religious enmity, humiliation of national dignity, but also propaganda of exceptionalism, superiority or inferiority of citizens on grounds of their religion, nationality or race, and public justification f terrorism.

Russian users may also be prosecuted under a host of older laws in the criminal code that may be applied to online speech. The Russian law establishes penalties for defamation (Article 128.1 of the criminal code), defamation against a judge or prosecutor (Article 298.1), insulting the authorities (Article 319), calls for terrorism (Article 205.1), insulting religious feelings (Article 148), calls for extremism (Article 280), calls for separatism (Article 280.1), incitement of hatred (Article 282), spreading false information on the activities of the Soviet Union in World War II (Article 354.1), displaying Nazi symbols or symbols of organizations deemed extremist (Article 20.3 of the administrative code), the dissemination of extremist materials (Article 20.29), or insult (Article 5.61).

Prosecutions and Detentions for Online Activities

Criminal charges are widely used in Russia to stifle critical discussion online. Acco ding to the SOVA Center for Information and Analysis, more journalists, activists, and online editors were subject to administrative and criminal prosecution within the past year. Individuals have been targeted for their posts on social media, including reposts, and many individuals prosecuted were targeted for posts related to Russia's conflict with Ukraine. Most ar ests within the coverage period fell under Article 282 ("actions aimed at inciting hate or enmity") and Article 280 ("public calls to extremist activity"). Prison terms issued during the coverage period have also been lengthier than in the past.

The fi st non-suspended sentence for promoting extremism on social media under Article 282 of the Criminal Code was given to Oleg Novozhenin from the Siberian town of Surgut.[74] Novozhenin was sentenced in December 2015 to one year in a penal colony for posting audio and video files on s -

71 Criminal Code of the Russian Federation, Article 280.1 "Public calls to separatism," http://www.consultant.ru/document/cons_doc_LAW_10699/8b38952a3e743c7996551cbfe4b32d4d336a35ad/; Criminal Code of the Russian Federation, Article 280, "Public calls to extremist activity," http://www.consultant.ru/document/cons_doc_LAW_10699/c10532ab76df5c84c18ee550a79b1fc8cb8449b2/.

72 Criminal Code of the Russian Federation, Article 282, "Incitement to hatred," http://www.consultant.ru/document/cons_doc_LAW_10699/d350878ee36f956a74c2c86830d066eafce20149/.

73 Written comment provided by Andrei Richet via LinkedIn on March 27, 2016.

74 Igor Lesovsky, "A Russian court assigned a fi st real imprisonment for propaganda of extremism on social networks," [in Russian] *Kommersant*, December 1, 2015, http://ow.ly/ZVgUB.

cial media which, according to the court, contained propaganda for Ukrainian nationalist party Right Sector and the Ukrainian Azov Battalion.[75]

Soon after, in another precedent setting case, the fi st maximum sentence was issued under Russia's anti-extremism provisions. Vadim Tyumentsev, a blogger from the city of Tomsk, was sentenced to fi e years in prison in December 2015 for posting hate speech and calls to extremism online.[76] Tyumentsev had uploaded videos of himself calling on local citizens to participate in a rally against high bus fares and criticizing Russia's involvement in eastern Ukraine, suggesting that Ukrainian refugees should be expelled from Russia.[77]

In December 2015, Krasnodar activist Darya Polyudova was sentenced to two years in a penal colony for public calls to separatism and extremism [78] after posting on VKontakte claims that Kuban is an ethnically Ukrainian region.[79]

In May 2106, mechanical engineer and Tver resident Andrei Bubeev was sentenced to two years imprisonment for reposting material critical of Russia's actions in Crimea as well as an image of a toothpaste tube captioned "Squeeze the Russia Out of Yourself." According to the court's ruling, Bubeev's reposts amounted to public incitement of extremism and calls for the violation of the territorial integrity of the Russian Federation. Bubeev reportedly had only 12 friends on VKontakte.[80]

Russian authorities have also targeted LGBTI expression, using a law against propaganda of non-traditional sexual relationships among minors to prosecute members of the LGBTI community. In December 2015, Sergey Alekseenko of Murmansk was found to have distributed "homosexual propaganda" among minors on the internet after he posted a supportive message in the VKontakte page of an LGBTI nonprofit. Alekseen o was fined RUB 100,000 (app oximately US $1,300).[81]

The Russian government continues to display a low tolerance for expression undermining the Russian Orthodox Church. In September 2016, Ruslan Sokolovsky, a blogger from Yekaterinburg, was sentenced to house arrest for incitement to hatred and insulting religious feelings after he uploaded videos of himself playing PokemonGo in a Yekaterinburg church.[82]

A prominent blogger, Anton Nossik, was fined for inciting hat ed after he posted a blog piece calling on President Putin to "wipe Syria off the map". Nossik was fined RUB 500,000 (US $8,000) [83]

75 Tetyana Lokot, "Russia Sees Its First Real Prison Sentence for 'Promoting Extremism' on Social Media," *Global Voices*, December 1, 2015 http://ow.ly/ZVh6E.

76 Freedom House, "Russia: Blogger Sentenced to Five Years Imprisonment", December 30, 2015, http://ow.ly/ZVhFp

77 "Russian court jails blogger for fi e years for 'extremist' posts," *Reuters,* December 30, 2015, http://uk.reuters.com/article/uk-russia-blogger-idUKKBN0UD16O20151230.

78 Tetyana Lokot, "Russian Activist Gets Two-Year Sentence for 'Calls to Extremism' on Social Networks," *Global Voices*, December 21, 2015, http://ow.ly/ZVhq0.

79 "Russian Activist Faces Trial On Separatism Charges," *Radio Free Europe*, September 3, 2015, http://ow.ly/ZVhmD.

80 Daniil Turovsky, "A trial for other people's words: a Tver resident is sentenced to two years in prison for the repost," [in Russian] *Meduza*, May 6, 2016, http://ow.ly/Hw5Z300CXuc.

81 "Russian LGBT activist fined for p opaganda of homosexuality online," *Global Voices,* January 22, 2016, https://globalvoices.org/2016/01/22/russian-lgbt-activist-fined-fo -propaganda-of-homosexuality-online/.

82 Sova Center, "Criminal case launched against blogger for playing PokemonGo in church," September 2, 2016, http://www.sova-center.ru/misuse/news/persecution/2016/09/d35335/.

83 "Russian blogger fined for call o 'wipe Syria off the map,'" *Al Arabiya,* October 4, 2016, http://english.alarabiya.net/en/media/digital/2016/10/04/Russian-blogger-fined-fo -call-to-wipe-Syria-off-the-map-.html.

Surveillance, Privacy, and Anonymity

Over the past couple of years, Russian lawmakers have enacted legislation which gives authorities ever-increasing powers to conduct intrusive surveillance online. Most recently, "Yarovaya's Law," a package of antiterrorism legislative amendments passed in July 2016, represents a bold attack on fundamental privacy safeguards on the internet. The new laws mandate that online services which provide encryption must assist the FSB with decoding encrypted data. Though this is an impossible task for many service providers—for example, due to the use of end-to-end encryption by many platforms—"organizers" that fail to cooperate could face a RUB 1,000,000 fine (USD $15,000). The Electronic Frontier Foundation has suggested that the impossibility of full compliance is a deliberate feature of the law, ensuring that some service providers are de-facto breaking the law and thus giving Russian authorities great leverage.[84] Yarovaya's Law also gives the authorities' greater access to user data by requiring telecoms, ISPs, and "organizers of information" to store the content of users' online communication—including text, video, and audio communication—for up to six months, while metadata must be stored for up to three years. Russian authorities will have access to this data without requiring a court order.[85] Following the passage of these antiterrorism amendments, 100,000 citizens signed a petition calling for the laws to be repealed.[86]

Though the new data retention rules have not yet come into effect, the authorities have reportedly started taking measures to intimidate companies into compliance. Private Internet Access, a VPN provider, claimed in July 2016 that authorities raided their Russia office and seized some f their servers. The company believed the raid was linked to the fact that they do not log any user data. Private Internet Access decided to exit the Russian market as a result of the incident.[87]

In what appears to be part of a wider effort to control user data, a data localization law was enacted in September 2015, requiring foreign companies which have personal data of Russian citizens to store their servers on Russian territory, potentially enabling easier access for security services.[88] Some foreign companies such as Uber[89] and Viber[90] have reportedly moved to comply with the law. Facebook and Twitter have declined to make public statements on the matter.

The Russian government employs SORM, or "system for operational investigative measures," for its online surveillance activities, and must be installed by all ISPs. The current version, SORM-3, uses DPI technology, enhancing the ability of the security services to monitor content on all telecommunications networks in Russia. SORM has been used for political purposes in the past, including the targeting of opposition leaders. In a Supreme Court case in November 2012 involving Maksim Petlin, an opposition leader in the city of Yekaterinburg, the court upheld the government's right to eaves-

84 Electronic Frontier Foundation, "Russia asks impossible in its new surveillance laws," July 2016, https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws.

85 Elizaveta Archangelskaya, Alyona Sukharevskaya, "Yarovaya's law: what an 'anti-terrorist' law means for internet users," *RBC*, June 24, 2016 http://www.rbc.ru/technology_and_media/24/06/2016/576c0a529a79471bc44d2b57?from=rbc_choice.

86 "100,00 signatures collected calling for Yarovaya's Law to be repealed," *Radio Svoboda*, August 13, 2016, http://www.svoboda.org/a/27919682.html/.

87 Private Internet Access, "We are removing our Russian presence," July 11, 206, https://www.privateinternetaccess.com/forum/discussion/21779/we-are-removing-our-russian-presence.

88 Vladimir Prokushev, "Journalists Andrei Soldatov and Irina Borogan: the internet is for the enlightened," [in Russian] *Horizontal Russia*, February 26, 2016, http://ow.ly/ZVHMP.

89 "Uber agreed to move the personal data or Russians to Russia" [in Russian], *Lenta.ru*, July 19, 2015, https://lenta.ru/news/2015/07/10/uber/.

90 Vladimir Zykov, "Viber moved its servers to Russia" [in Russian], *Izvestia*, December 19, 2015, http://izvestia.ru/news/593438.

drop on Petlin's phone conversations because he had taken part in "extremist activities," namely anti-government protests.

Under current legislation, in order to receive an operating license, ISPs are required to install equipment that allows security services to monitor internet traffic. ISPs that do not comply with SORM system requirements are promptly fined, and may ha e their licenses revoked if problems persist. Russian authorities are technically required to obtain a court order before accessing an individual's electronic communications data; however, the authorities are not required to show the warrant to ISPs or telecom providers, and FSB office s have direct access to operators' servers through local control centers. Experts note that there is no information about any government efforts to punish security office s who abuse tracking methods.[91] ISPs and mobile providers are required to grant network access to law enforcement agencies conducting search operations, and to turn over other information requested by the prosecutor's office, the In erior Ministry, the FSB, or the Investigative Committee.

Use of circumvention tools is on the rise, with growing numbers of Russians turning to Tor[92] and VPNs[93] to mask their identity online and access blocked content, particularly after Rutracker.org, a popular torrent tracker, was banned in Russia in January 2016.[94] According to Andrei Soldatov, Russian authorities are unsure of how to tackle this phenomenon,[95] though it is clear that circumvention tools are viewed with suspicion and regional courts are increasingly targeting these tools. In February 2016, a court in Anapa, a city in southern Russia, issued a verdict against RosComSvoboda, a nonprofit moni oring banned content, ruling that an article with instructions on how to use anonymizers to access banned information was illegal.[96] However, RosComSvoboda succeeded in demonstrating to the Ministry of Telecommunications and Mass Communications that the article had not violated any law and the article remains available.[97] Later in 2016, the Ministry of Telecoms and Mass Communications proposed a draft bill under which ISPs could be fined if ebsites publish "propaganda" outlining how to use anonymizers.[98]

Intimidation and Violence

While attacks on journalists have been commonplace in Russia in past years, this year saw a dramatic spike in violent attacks against social media users, indicating a possible coordinated campaign to intimidate critical social media users into silence. Human rights organization Agora registered a total of 28 threats and attacks on online journalists and bloggers in 2015.[99] VKontakte users and group administrators in particular have been victims of intimidation and violence.

91 Aleksey Alikin "SORM in public," [in Russian], *Russkaya Planeta*, July 29, 2013, http://rusplt.ru/policy/policy_3890.html.

92 Tor Metrics, "Top-10 countries by directly connecting users," http://ow.ly/icSE300CWR2.

93 Alexey Rezvanov, "Invasion of anonymous: how the ban on torrents affects the advertising market?" [in Russian] April 14, 2016, *RBC*, http://ow.ly/NY0F300CWTT.

94 Interview with Andrei Soldatov conducted in Moscow on March 25, 2016.

95 Interview with Andrei Soldatov conducted in Moscow on March 25, 2016.

96 Elizaveta Surganova, "A site was blacklisted for information about anonymizers," [in Russian] *RBC*, February 10, 2016, http://ow.ly/ZXaQD.

97 "RosComSvoboda found a way to avoid blocking," [in Russian] *RBC* February 12, 2016, http://ow.ly/ZXaRK.

98 Alyona Sukharevskaya, "Telecom operators are proposed to be fined for info mation about anonymizers," [in Russian] May 19, 2016, http://ow.ly/EkBe300Euuw.

99 Damir Gaynutdinov, Pavel Chikov, "Internet freedom 2015: the triumph of censorship," [in Russian] *Agora*, February 16, 2016, https://rublacklist.net/14661/ p.10.

In March 2016, Aleksandr Markov, an administrator of the VKontakte group "Criminal Regime" which is critical of Kremlin policies, was brutally assaulted when two strangers showed up at his Saint Petersburg apartment, pushed him down a staircase, and beat him. In June 2016, another Criminal Regime administrator, Yegor Alekseev, was attacked on the street by two men and suffered a broken nose, a concussion, and a fractured skull. Also in June, a VKontakte employee well known for his antigovernment posts was physically attacked in the street by unidentified men who called him a n - tional traitor, a Jew, and member of the "fi th column".[100]

Social media users have also been subject to arson attacks in the past year. In April 2016, after student Ruslan Starostin posted a satirical image of Putin to his VKontakte page, his wife received a friend request from an unknown user who sent threatening messages related to the Putin post. Starostin's car was then torched several hours later.[101]

A number of opposition activists and social media users have been subject to intimidation via VKontakte. In February 2016, Daniel Alexandrov, a political activist associated with the Watchers of Saint Petersburg opposition movement, came across a spoof VKontakte profile whose p ofile pictu e was a photo secretly taken of Alexandrov walking his dog.[102]

In March 2016, a group of journalists, including correspondents from online publications *Mediazona* and *The New Times*, in addition to local and international human rights activists brought together by the Committee Against Torture on a tour of the Caucasus, were attacked by a group of masked men armed with batons and sharp objects. The assailants then set the bus on fi e[103] and stole computers and other equipment from the group.[104] The Kremlin and Putin personally reacted to the accident saying that it should be investigated, though little progress has been made so far.[105]

Technical Attacks

Cyberattacks against independent media, blogs, and news portals continue to inhibit Russian internet users' ability to access such sites. In 2015, the human rights group Agora registered 30 hacking attacks against independent media and blogs, as well as hacks of emails and social media accounts.[106] In the past year, dozens of Russian civil society activists and journalists have been notified of attempts to compromise their accounts online, including Telegram and Gmail accounts, suggesting a coordinated campaign to compromise their security and access private information.

In May 2016, activists Oleg Kozlovsky and Georgy Alburov reported that their Telegram accounts were hacked through the messaging app's SMS login feature. The activists never received an SMS

100 "Violence against Russian web dissidents raises fresh fears for internet freedoms," *The Guardian*, June 23, 2016, https://www.theguardian.com/world/2016/jun/23/violence-against-russias-web-dissidents-raises-fresh-fears-for-internet-freedoms.

101 "People against Putin are beaten and their cars are burned," *Real Time*, June 14, 2016, http://www.currenttime.tv/a/27797019.html.

102 "In St Petersburg, 'Free Ingria' activist beaten," *The Village*, February 9, 2016, http://www.the-village.ru/village/city/city/231301-alexandrov.

103 Shaun Walker, "Journalists and activists beaten and bus torched on Chechnya tour," *The Guardian*, March 10, 2016, https://www.theguardian.com/world/2016/mar/10/journalists-beaten-and-bus-torched-on-chechnya-tour-say-activists.

104 Ilya Rozhdestvensky, "The equipment of the journalists and human rights activists beaten in Ingushetia has been stolen" [in Russian], *RBC*, March 11, 2016, http://ow.ly/ZUhUa.

105 Maria Bondarenko,"Putin ordered to deal with the attack on journalists on their way to Chechnya." [in Russian] *RBC*, http://ow.ly/ZUiE2.

106 Damir Gaynutdinov, Pavel Chikov, "Internet freedom 2015: the triumph of censorship," [in Russian] *Agora*, February 16, 2016, http://ow.ly/ZTWQn.

notification f the login requests, and later discovered that their mobile phone company, MTS, had switched off SMS delivery for their SIM cards for several hours on the night of the breach. Though it remains unclear who accessed their accounts, Kozlovsky and Alburov strongly suspect that MTS colluded with the FSB to access their private communications.[107]

Kozlovsky was targeted again in October 2016 among a group of Russian journalists and activists who received a notification f om Google that "government-backed hackers" were trying to gain access to their accounts. At least 16 people received this message within a similar time frame, including journalist Ilya Klishin and Bellingcat researcher Aric Toler.[108]

Earlier, in September 2015, two investigative journalists and a spokesperson for opposition leader Alexey Navalny reported that their email accounts had been breached using copies of SIM cards issued by MTS and Vympelcom (Beeline).[109]

Independent news sites also continue to be targeted for their work. In June 2015, hackers called "Group SMERSH" published the emails of Elena Myasnikova, the vice president of the independent media group RBC.[110] In February 2016, *The New Times*, an independent Moscow-based magazine and online news portal, became inaccessible following the publication of its investigation on Putin's daughter. The editor-in-chief of *The New Times*, Yevgenia Albats, speculated that the outage was a result of massive distributed denial-of-service (DDoS) attacks.[111]

In previous years, websites that suffered DDoS attacks included the internet project Demokrator.ru, St Petersburg news portals Zaks.ru and Lenizdat.ru, the website of the SOVA Center for Information and Analysis, the website of the daily newspaper *Moskovsky Komsomolets*, the Murmansk-based portal Bloger51.ru, and the websites of *Novaya Gazeta* and TV Dozhd.

107 "Neither pro-Kremlin pundits nor opposition safe from hackers," *The Moscow Times,* May 4, 2016, https://themoscowtimes.com/articles/neither-pro-kremlin-pundits-nor-opposition-safe-from-hackers-52782.

108 "Google warned Russian activists and journalists of attempts by secret services to access their email," *Meduza,* October 11, 2016, https://meduza.io/news/2016/10/11/google-predupredil-rossiyskih-aktivistov-i-zhurnalistov-o-popytkah-spetssluzhb-vzlomat-ih-pochtu.

109 "Novaya Gazeta journalists complained of email hacks," *TJournal*, September 1, 2015, https://tjournal.ru/p/novaya-gazeta-sim-violations.

110 "Hackers posted the correspondence of the RBC vice president Elena Myasnikova," [in Russian] *Roem,* June 2, 2015, http://ow.ly/ZU9ib.

111 Svetlana Reiter, Elizaveta Surganova, Ilya Rozhdestvensky, "The magazine The New Times received a warning for the "Right Sector" [in Russian], *RBC*, February 1, 2016, http://ow.ly/ZU77x.

Freedom House

Rwanda

	2015	2016
Internet Freedom Status	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	11	10
Limits on Content (0-35)	20	21
Violations of User Rights (0-40)	19	20
TOTAL* (0-100)	**50**	**51**

* 0=most free, 100=least free

Population:	**11.6 million**
Internet Penetration 2015 (ITU):	**18 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- The *Ireme* news website was blocked in December 2015, joining a number of other independent online media outlets (see **Blocking and Filtering**).
- Authorities told online news editors to withhold or delete content on sensitive topics, such as the December 2015 constitutional referendum to extend presidential term limits (see **Media, Diversity, and Content Manipulation**).
- In January 2016, an *Ireme* editor and investigative reporter was arrested for sexual assault against a minor, a charge observers believe was fabricated to silence his critical reporting (see **Prosecutions and Detentions for Online Activities**).

Introduction

While access improved in Rwanda, internet freedom declined due to increasing online censorship and self-censorship around the topic of presidential term limits in 2015 and 2016.

Rwanda continued to project itself as an emerging technology hub in the past year, investing heavily in the country's information and communications technology (ICT) sector to establish itself as a vibrant knowledge economy. The government hosted the second Transform Africa Summit in October 2015 and the World Economic Forum on Africa in May 2016, which both focused on leveraging opportunities for digital transformations and economic growth, and helped entrench Rwanda's position as a regional leader. Nonetheless, only 18 percent of Rwandans have access to the internet, and poverty continues to be the primary impediment to increasing access.

In sharp contrast to Rwanda's remarkable progress on economic development, tight restrictions on freedom of speech and political activity are among the world's worst, imposed under the pretext of political and ethnic tension resulting from the 1994 genocide. Independent civil society and journalism have been crippled by years of repression. Pro-government views dominate domestic media, while the authorities work quickly to censor critical viewpoints, resulting in an information environment that projects a single narrative of unity, peace, and progress. Numerous unlawful detentions in secret detention centers, torture, and even extralegal killings of citizens for their critical viewpoints go unreported, along with efforts to uphold the rule of law.[1]

While the environment is still freer online than offline for jou nalists and citizens alike, the government's efforts to limit internet freedom have increased in the last few years. Numerous independent online news outlets have been blocked, including the British Broadcasting Corporation's (BBC)'s local language websites, and pressure on editors to delete critical content or toe the government line is high. The independent news outlet *Ireme* was newly blocked in December 2015, and an editor and reporter for the site was arrested in January 2016, likely for his critical reporting.

A December 2015 constitutional referendum sought to revise presidential term limits, potentially extending President Paul Kagame's rule for up to 17 more years. The issue became a new redline for censors, who issued more directives to online news outlets to remove or hold back content. As a result, journalists self-censored when reporting on the vote, which officials said was 98 pe cent in favor of the change.[2]

Obstacles to Access

Rwanda continued making significant investments in its ICT sector to expand internet access and improve affordability. Innovative e-government initiatives were launched to enhance the government's service delivery to citizens via the internet and mobile devices.

Availability and Ease of Access

1 "Rwanda poor, homeless detained, says HRW," Deutche Welle, July 21, 2016, http://www.dw.com/en/rwandan-poor-homeless-detained-says-hrw/a-19416530.

2 Clement Uwiringiyimana, "Rwandans approve extension of presidential term limits," Reuters, December 19, 2015, http://uk.reuters.com/article/uk-rwanda-politics-idUKKBN0U209D20151219

Access to information and communication technologies (ICTs) has increased notably in Rwanda over the past few years, bolstered by investments by the Rwandan government to transform the country into an information economy. According to June 2016 statistics by the Rwanda Utilities Regulatory Agency (RURA), the sector regulator, internet penetration reached 33 percent, growing from 28 percent the previous year.[3] Estimates from the International Telecommunication Union (ITU) were lower at 18 percent, up from 11 percent a year prior.[4] Mobile telephone penetration is significantly highe , reaching 70 percent in 2015 according to ITU data, while the government reported 79 percent as of June 2016. Notably, rural communities which comprise 90 percent of the population have a relatively high rate of mobile phone usage, made possible by a well-developed mobile network that covers nearly 100 percent of the country.

Government investments in broadband technology across the country continued to grow, as well as access to electricity via hydropower and solar energy projects, which have helped improve speeds and decrease costs. According to Akamai's *State of the Internet* report, Rwanda's average internet connection speed was 8.7 Mbps in 2016, increasing from 5.6 Mbps the previous year and above the global average of 6.3 Mbps.[5] Access has also become more affordable. The Alliance for Affordable Internet ranked Rwanda as the 11th most affordable internet environment among 51 developing countries in 2015.[6] A 4G LTE network launched by the government in partnership with the Korean Embassy in December 2014, offers the fastest high-speed data for mobile phones and internet-enabled devices. In a new initiative, some public buses in the capital, Kigali, are now wired with 4G internet connections, providing passengers with full access to free fast internet.[7]

Innovative initiatives encouraging both urban and rural populations people to use ICTs have expanded in recent years. The e-Soko ("e-market") program provides farmers with real-time information about market prices for their agricultural produce on their mobile devices. Others include a Rwanda National Police mobile registration system for scheduling driver's license exams and renewals;[8] online tax filing with the Rwanda evenue Authority;[9] an online system for registering commercial companies;[10] and an online system for national exam results published by the Rwanda Education Board.[11] The government also launched Irembo, a platform to improve delivery of government services to citizens and businesses, in October 2015.[12]

Nonetheless, poverty continues to be the primary impediment to ICT uptake, especially the internet, with the majority of the population engaged in subsistence agriculture. Internet access is concentrated primarily in Kigali and remains beyond the reach of many citizens, particularly those in rural areas

3 "Statistics and tariff information in telecom, media, and postal service as of the second quarter 2016," RURA, August 2016, http://www.rura.rw/fileadmin/docs/Monthly_ elecom_subscribers_of_August_2016.pdf

4 International Telecommunication Union, "Percentage of Individuals Using the Internet," 2000-2015, http://bit.ly/1cblxxY.

5 Akamai, "Average Connection Speed: Rwanda," map visualization, *The State of the Internet Q1 2016*, http://akamai.me/1OqvpoS.

6 Alliance for Affordable Internet, The Affordability Report, 2015, http://a4ai.org/2015-16-a4ai-affordability-report-out-today/

7 Julius Bizimungu, "Smark Kigali: 400 buses connected to 4G internet," The New Times, February 20, 2016, http://www.newtimes.co.rw/section/article/2016-02-20/197264/

8 "Registration for driving license tests start," Rwanda National Police, press release, January 18, 2014, http://www.police.gov.rw/news-detail/?tx_ttnews%5Btt_news%5D=863&cHash=8412a9646f4dd409486ed87c75141e6a

9 See, http://onlineservices.rra.gov.rw

10 See, http://org.rdb.rw/busregonline

11 See, Rwanda Education Board, http://196.44.242.28

12 See, Irembo, https://irembo.gov.rw/rolportal/web/rol/aboutus

who are limited by low income and low levels of ICT awareness.[13] Only 11 percent of Rwandans are ICT literate,[14] and over 70 percent of the population speaks only Kinyarwanda, making internet content in English inaccessible to the majority of Rwandans.[15] Only 17 percent of Rwandan households have regular access to electricity.[16]

Restrictions on Connectivity

There were no restrictions on connectivity reported in Rwanda during the coverage period, though Article 52 of the 2001 Law Governing Telecommunications gives the government powers over telecommunications networks in the name of preserving "national integrity." These powers include the ability to "suspend a telecommunications service for an indeterminate period, either generally or for certain communications."[17] Furthermore, the government has some control over the country's internet infrastructure. The ITU has characterized the level of competition for Rwanda's international gateway as "partial."[18]

The local internet exchange point (IXP), the Rwanda Internet Exchange (RINEX),[19] is managed by the Rwanda Information & Communications Technology Association, a non-profit comprised f ICT institutions and professionals.[20] As of mid-2016, fi e of Rwanda's nine ISPs exchange internet traffic through RINEX, and ISPs can also opt to connect via RINEX to the international internet.[21]

ICT Market

Rwanda's ICT market continues to be vibrant and competitive, with no reported interference from the government during the period of study. Following market liberalization policies implemented in 2001,[22] there are nine internet service providers (ISPs) and three mobile phone companies,[23] all privately owned. The three main mobile phone operators are MTN, TIGO, and Airtel, with market shares of 49 percent, 35 percent, and 16 percent, respectively.[24]

13 Ministry of Youth and ICT, "Measuring ICT sector performance and Tracking ICT for Development (ICT4D)," 2014, http://bit.ly/1NfV6Hb.

14 Philippe Mwema Bahati, "Rwanda to develop a master plan for e-Government," Rwanda Focus via All Africa, December 14, 2013, http://bit.ly/1Loqu3j.

15 Beth Lewis Samuelson and Sarah Warshauer Freedman, "Language Policy, Multilingual Education, and Power in Rwanda," *Language Policy* 9, no. 3 (June 2010), http://bit.ly/1bmZW5X.

16 The Independent, "Rwanda Signs a U.S. $40 Million Loan to Boost Electricity Rollout," All Africa, January 14, 2015, http://bit.ly/1G9m4AA.

17 Law No. 44/2001 of 30/11/2001 Governing Telecommunications, http://bit.ly/1G9mOG3.

18 International Telecommunication Union, "Rwanda Profile (La est data available: 2013)," *ICT-Eye*, accessed January 3, 2016, http://bit.ly/1LS1oJs.

19 RINEX, accessed December 13, 2014, http://www.rinex.org.rw/about.html.

20 R.I.C.T.A, "About Us," http://www.ricta.org.rw/about-us/.

21 Rwanda Internet Exchange (RINEX), "About Us," http://www.rinex.org.rw/about.html.

22 Albert Nsengiyumva and Emmanuel Habumuremyi, *A review of telecommunications policy development and challenges in Rwanda*, Association for Progressive Communications (APC), September 2009, http://bit.ly/1MtFpZY.

23 These include fi ed-line providers (Liquid Telecom and MTN Rwanda), mobile phone providers (MTN Rwandacell, TIGO and AIRTEL), and internet service providers (MTN Rwanda, Liquid Telecom, TIGO Rwanda, New Artel, ISPA, 4G Networks, BSC, Airtel Rwanda, and AXOIM). See: RURA, "Statistics and Tariff Information in Telecom Sector as of March 2014."

24 RURA, "Statistics and Tariff Information in Telecom Sector as of March 2015."

Regulatory Bodies

The Rwanda Utilities Regulatory Agency (RURA) oversees the regulatory framework and implementation of policy and strategy in the telecommunications sector.[25] Officiall , RURA has administrative and financial au onomy. Nevertheless, the government audits RURA's budget while the president nominates its seven board members, supervisory board, and director general, who all work under government oversight, which limits that autonomy in practice.[26]

In 2015, RURA demonstrated its allegiance to the government in its decision to indefini ely ban BBC radio services and block BBC websites following the October 2014 broadcast of a controversial documentary (see Blocking and Filtering).[27] In doing so, it overruled vocal objections voiced by Fred Muvunyi, then-head of the media self-regulatory body, the Rwanda Media Commission (RMC). Muvunyi subsequently fled the count y in May 2015 after months of threats and intimidation.[28] Journalists interviewed for this report said that the RMC now exists only on paper, acting under instruction from government authorities or security officials.

Limits on Content

Censorship of online content remained high, with a number of independent online media outlets still blocked in the country. Editors of online news sites regularly received official demands to delete critical content or avoid writing critically about certain topics, such as the constitutional referendum to extend presidential term limits in December 2015.

Blocking and Filtering

The Rwandan government endeavors to restrict the types of content that users can access, particularly content that strays from the government's official line. In 2016, nume ous independent news outlets and opposition blogs that have been blocked for years remained inaccessible, including the websites of *Inyenyeri News*, *Veritas Info*, *The Rwandan*, and *Leprophete*, among others.[29] The news website *Ireme* was added to the block list in December 2015, likely for its critical reporting on the referendum on presidential term limits.[30] There is no transparency behind the government's blocking decisions and no avenue for appeal.

Several BBC websites were blocked in Rwanda following the government's outcry against the television broadcast of the documentary, "Rwanda, The Untold Story," in October 2014, which said that the number of Hutus who died during the genocide was much higher than officially ecognized. Though

25 RURA, "About RURA," accessed December 10, 2014, http://www.rura.rw/index.php?id=3.

26 "Law N.09/2013 of 01/03/2013 Establishing Rwanda Utilities Regulatory Authority (RURA) and Determining its Mission, Powers, Organisation and Functioning," *Official Gazette n.14bis of 08/04/2013*, http://bit.ly/1RMmWwg.

27 RURA, "Decision N°…/RURA/2015 of 29 May, 2015 on the Inquiry Into the Documentary Aired By BBC: 'Rwanda's Untold Story'," news release, May 30, 2015, http://bit.ly/1MtG3GV.

28 Sue Valentine, "Hopes of independent press in Rwanda fade as head of media body flees" Committee to Protect Journalists (blog), July 8, 2015, https://cpj.org/x/64d5.

29 Study conducted by Freedom House consultant, March 2016. Other opposition blog websites that were unavailable as of May 2016 were: http://ww.iwacu1.com; http://ww.musabyimana.be; http://rwandarwabanyarwanda.over-blog.com, http://ww.banyarwandapoliticalparty.org.

30 "Rwanda news website Ireme latest to be blocked," Great Lakes Voice, December 1, 2015, http://greatlakesvoice.com/rwanda-news-website-ireme-latest-to-be-blocked/

the documentary had not been aired in Rwanda, the government suspended the BBC's popular radio services, accusing the outlet of "genocide denial," a crime under the country's harsh media laws.[31] The regulator RURA indefini ely banned BBC broadcasts in May 2015.[32] BBC websites, including BBC Swahili, BBC Africa, BBC Afrique were also blocked, according to a May 2015 report by the Rwanda Media Commission.[33] The website of the local language service, BBC Gahuzamiryango, was also inaccessible in 2016.[34]

Social-networking sites such as YouTube, Facebook, Twitter, and international blog-hosting services are freely available.

Content Removal

The extent to which the government forces websites to delete certain content is unknown, though anecdotal incidents over the past few years suggest it happens frequently. Similar to the restrictive traditional media environment, editors of online news sites often receive calls from the authorities with demands to delete certain content, mostly related to government leaders.[35] Such ad hoc requirements lack a legal basis or transparency.[36]

According to a 2010 law relating to electronic messages, signatures, and transactions, intermediaries and service providers are not held liable for content transmitted through their networks.[37] Nonetheless, service providers are required to taken down content when handed a takedown notice, and there are no avenues for appeal.

Media, Diversity, and Content Manipulation

Government repression of the media greatly limits the diversity of the information landscape both online and offline. Critical and independent online news p oduced by opposition supporters overseas—mainly in Europe, the United States, and South Africa—are blocked in Rwanda. Few Rwandans are aware of this practice, though savvy journalists seeking independent sources of information report using proxy servers to access critical information.[38]

While Rwandans are active on Facebook and Twitter, which have become popular with the rise of internet-enabled mobile phone use, self-censorship has become more pervasive among both online journalists and ordinary users due to increasing government repression, social pressure to toe the government line, and fear of reprisals. Pro-government trolls also harass online users for their critical

31 Reporters Without Borders, "BBC's Kinyarwanda Broadcasts Suspended Indefini ely," October 24, 2014, http://bit.ly/1hIHBV2.

32 RURA, "Decision N°.../RURA/2015 of 29 May, 2015 on the Inquiry Into the Documentary Aired By BBC: 'Rwanda's Untold Story'."

33 Rwanda Media Commission, *The State of Media Freedom in Rwanda,* May 2015, 40, http://bit.ly/1PwYbot.

34 Freedom House consultant, May 2016; http://www.bbc.com/gahuza

35 Interview with journalist writers of *igihe.com* and *Kigali Today* who requested to stay anonymous

36 Two online news websites, *Umusingi* and *Umurabyo*, had reported experiencing such requests to delete content related to local political affairs and ethnic relations in previous years.

37 "Law No. 18/2010 of 12/05/2010, Relating to Electronic Messages, Electronic Signatures and Electronic Transactions, accessed October 24, 2014, http://www.wipo.int/wipolex/en/text.jsp?file_id=24315 .

38 Author interviews with anonymous journalists, May 2016.

commentary and manipulate online conversations.[39] Internet users typically avoid topics that can be construed as critical of the government or disruptive to national unity and reconciliation.[40]

When online journalists try to push the boundaries, their editors frequently contend with editorial interference by security officials and other go ernment authorities who impose redlines limiting what can be published.[41] Journalists say editorial decisions are heavily influenced by go ernment forces—including police office s, army office s, and powerful leaders—whose demands are colloquially known as, "I say this." Journalists self-censored in their coverage of the December 2015 constitutional referendum on presidential term limits,[42] deliberately suppressing stories in the public interest. One journalist reported witnessing the forced collection of signatures for a petition in support of the constitutional change.[43]

Given the even more restricted space for press freedom in the traditional media sphere, Rwandan media outlets are increasingly going online to bypass government control or suspension as well as heavy production costs.[44] However, independent outlets face economic challenges in comparison to their state-run counterparts, which receive income from government advertisements and direct subsidies.[45] Large businesses only advertise with state-owned or pro-government media outlets based on an unspoken rule.

Digital Activism

Digital activism over political and social issues is not common in Rwanda. Radio and television call-in programs were once a positive outlet for citizens with mobile phones to anonymously voice critical political or social viewpoints. However, given SIM card registration requirements, users have become reluctant to participate in critical or sensitive discussions out of fear of being identified. In the ast year, callers were less critical and more likely to praise the status quo.

Violations of User Rights

An investigative reporter and editor with the Ireme *news website was arrested in January 2016, a month after the site was blocked. He faces charges of sexual assault against a minor, which observers say were trumped up to silence his critical reporting.*

39 In 2014, an international journalist for Radio France Internationale, Sonia Rolley, was repeatedly harassed on Twitter by a user known as @RichardGoldston. Rolley had been reporting on the mysterious January 1, 2014 assassination of Patrick Karegeya, a former top intelligence official in Kagame s inner circle who had been living in exile in Johannesburg. It was later revealed on the official witter account of Paul Kagame's office (@Urugwi oVillage) that "@RichardGoldson was an unauthorized account run by an employee in the Presidency.

40 Katrin Matthaei, "Rwanda: Censorship or self-censorship?" *Deutsche Welle*, December 9, 2014, http://bit.ly/1G9oEGP.

41 "I know very well that people would really want to read an article about some malpractices that happened in a certain District in Southern Province, where agents voted for people who were not around and influenced oters just for a certain candidate to win as was already decided. However, I know that this can endanger my outlet," said one online journalist interviewed on February 24, 2016, who requested anonymity.

42 Johnson Kanamugire, "Kagame free to rule till 2034," The East African, October 31, 2015, http://www.theeastafrican.co.ke/news/Kagame-could-rule-until-2034/-/2558/2936826/-/a1385mz/-/index.html

43 Anonymous interview, March 2016.

44 "Rwanda: Why We Went Online: Media Icons Speak Out," Itangazamakuru, March 2012, http://bit.ly/18GUIy1.

45 In Rwanda, approximately 85 to 90 percent of advertisements come from the public sector, says Robert Mugabe, editor of the online news site Great Lakes Voice. "If you need to attract adverts, it's simple. Don't annoy government," he said. http://www.pambazuka.org/governance/advertising-and-censorship-east-africas-press

Legal Environment

The Rwandan constitution, adopted in May 2003, provides for freedom of the press and information along with other legislative instruments, including Law N° 02/2013 regulating media,[46] and Law No 04/2013 of relating to access to information.[47] In practice, the government maintains tight control over the media and information landscape. Amendments to the 2009 Media Law, passed in 2013,[48] provided the government with some scope to control the internet by giving the minister of ICTs unlimited powers to establish the conditions for local and foreign media companies to operate in Rwanda.[49] The Rwandan judiciary is not independent, and many journalists view the threat of imprisonment as a key constraint on their work.

While there are no laws that specifically estrict internet content or criminalize online expression, Rwanda's generally restrictive legal provisions governing the traditional media can be applied to the internet. Penalties for criminal defamation may also be applicable to online speech. Defamation of the president or other public officials carries a penalty f up to fi e years in prison.[50] October 2013 amendments to the law against "genocide ideology" similarly threatens freedom of expression both online and off, prescribing heavy prison sentences of up to 9 years and fines for any ffender "…who disseminates genocide ideology in public through documents, speeches, pictures, media or any other means."[51] The law also lacks a clear distinction between private and public speech.[52]

Journalists say the government has the ability to restrict the internet and infringe on user privacy under the pretext of protecting national security. One online journalist who requested anonymity said, "There is a difference between how laws are written and how they are put into practice. Ask me about what I face while exercising my profession and leave alone the laws. We have very well written and 'thought-about' laws, but their implementation has its own unwritten laws."

Prosecutions and Detentions for Online Activities

Citizens are periodically arrested for online activities in Rwanda, though the lack of critical commentary originating in the country and the high degree of self-censorship practiced by online journalists and ordinary users alike has resulted in fewer incidents. Cases may also be underreported given the government's strict controls of the media. One arrest was reported in the past year.

In January 2016, John William Ntwali, an investigative reporter and editor of the *Ireme* news website (which was blocked a month prior in December) was arrested and held for 13 days. He was charged with sexual assault against a minor in a case that could not be substantiated, leading observers to believe the charge was trumped-up in an effort to silence him for his critical reporting.[53]

46 Law N° 02/2013 of 08/02/2013 regulating media in Rwanda.

47 Law No 04/2013 of 08/02/2013 relating to access to information.

48 Article 19, "Proposed media law fails to safeguard free press," IFEX, January 5, 2012, http://bit.ly/1NfYemn.

49 Article 19, "Rwanda: Media law does not go far enough," press release, March 18, 2013, http://bit.ly/1LS2gUC.

50 Freedom House, "Rwanda," *Freedom of the Press 2013*, http://www.freedomhouse.org/report/freedom-press/2013/rwanda.

51 Art. 8, "Law No. 18/2008 of 23/07/2008 Relating to the Punishment of the Crime of Genocide Ideology," http://bit.ly/1LS2gUC.

52 Emmanuel R. Karake, "Gov't seeks to amend genocide ideology law," *The New Times*, November 3, 2012, http://bit.ly/1Pmb8T8.

53 "Newsletter: Freedom of Expression in East Africa," Article 19, March 7, 2016, https://www.article19.org/resources.php/resource/38282/en/newsletter:-freedom-of-expression-in-eastern-africa; "Investigation reporter freed provisionally after prosecutor reduces charge," Reporters Without Borders, February 10, 2016, http://bit.ly/2eOTus2

Surveillance, Privacy, and Anonymity

The sophistication of the Rwandan authorities' surveillance capabilities is unknown, but there is a strong sense that surveillance is pervasive. Exiled Rwandan dissidents have been attacked and murdered, despite their efforts to protect their identities, following threats from individuals inside or associated with the government.[54]

October 2013 amendments to the 2008 Law Relating to the Interception of Communications expanded the government's surveillance powers, authorizing high-ranking security officials to tap the communications of individuals considered potential threats to "public security," including online.[55] Under the amendments, communications service providers are required to ensure that their systems have the technical capability to intercept communications upon demand, though security officials also have the power to "intercept communications using equipment that is not facilitated by communication service providers," which de facto allows the authorities to hack into a telecommunications network without a provider's knowledge or assistance.[56] While the law requires government officials to apply for an interception warrant, warrants are issued by the national prosecutor, who is appointed by the justice minister. The national prosecutor can also issue warrants verbally in urgent security investigations, to be followed by a written warrant within 24 hours. There is no requirement to justify surveillance as necessary and proportionate to a legitimate aim.[57]

In July 2015, email leaks from the Italian surveillance firm Hacking Team revealed that the Rwandan government attempted to purchase sophisticated spyware known as Remote Control System (RCS) in 2012.[58] While the leaked emails did not confirm that a sale took place, they illustrate the government interest in acquiring technology that can monitor and intercept user communications.

The ability to communicate anonymously is compromised by mandatory SIM card registration requirements in place since 2013.[59] Under the regulation establishing SIM card registration, the ICT regulator RURA has unfettered access to SIM card databases managed by operators, while other "authorized" individuals or institutions may also be granted access.[60]

The various legal provisions that enable surveillance and limit anonymity are particularly troubling in the absence of a comprehensive data protection law to safeguard citizens' private data. A data protection law was drafted in July 2013, though the draft provided exceptions in the vaguely defined interest of national sovereignty, national security, and public policy, which could be abused to monitor individuals critical of the regime.[61] There was no movement on the passage of the law as of mid-2016.

54 Human Rights Watch, "Rwanda: Repression Across Borders," January 28, 2014, http://bit.ly/1i9HihM.

55 "Law Relating to the Interception of Communications" Official Gazette nº 41 of 14/10/2013.

56 Art. 7, "Law Relating to the Interception of Communications" Official Gazette nº 41 of 14/10/2013.

57 OpenNet Africa and Collaboration on Internet ICT Policy in East and Southern Africa, *Online Freedoms in Rwanda*, May 2014, http://bit.ly/1LovLbk.

58 WikiLeaks, "Hacking Team," July 8, 2015, http://bit.ly/1ReTbn0; Lorenzo Frankenstein, Twitter Post, July 9, 2015, 3:53 PM, http://bit.ly/1hIJLUs.

59 "Rwanda Flags Off SIM Card Registration Exercise," Chimp Reports, February 4, 2013, http://bit.ly/1jHd5fr.

60 See Regulations on SIM Card Registration, art. 13 and 15, http://bit.ly/1VWMjBw.

61 "Rwandan ICT experts discuss draft data protection policy," Telecompaper, July 16, 2013, http://bit.ly/1MtJkGd.

Intimidation and Violence

Critical journalists frequently face violence and harassment when attempting to cover news stories, leading many to flee the count y.[62] According to the Committee to Protect Journalists, Rwanda ranks among the top countries from which journalists seek exile.[63] There were no reported incidents of violence against online journalists and ordinary users during the coverage period, though high levels of censorship and self-censorship may result in underreporting.

Technical Attacks

There was no evidence of technical attacks against online news outlets or users in Rwanda during the period under study. The last reported attack occurred in April 2014, when the investigative news website, *Ireme*, experienced a seemingly targeted cyberattack from an unknown source.[64] *Ireme* was blocked in December 2015 (see Blocking and Filtering).

62 Human Rights Watch, "Rwanda: Repression Across Borders."

63 Committee to Protect Journalists, "452 Journalists Forced Into Exile Since 2010," accessed on October 13, 2016, http://www.cpj.org/exile/.

64 Reporters Without Borders, "Wave of intimidation of Kigali media."

Freedom House

Saudi Arabia

	2015	2016
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	15	14
Limits on Content (0-35)	24	24
Violations of User Rights (0-40)	34	34
TOTAL* (0-100)	**73**	**72**

* 0=most free, 100=least free

Population:	**31.5 million**
Internet Penetration 2015 (ITU):	**70 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- Internet penetration has risen on the back higher mobile broadband subscriptions (see **Availability and Ease of Access)**.
- Authorities throttled Telegram starting in January 2016 in order to prevent users from sharing images and files o er the popular messaging app (see **Blocking and Filtering**).
- The head of Riyadh's Committee for the Promotion of Virtue and the Prevention of Vice was dismissed after public outrage over a video of committee members harassing a girl outside of a mall (see **Digital Activism**).
- Abdulkareem al-Khadar, Abdelrahman al-Hamid, and Abdulaziz al-Sinedi were respectively sentenced to 10, 9 and 8 years in prison for online advocacy against human rights violations. Saudi's Supreme Court upheld a harsh verdict against liberal blogger Raif Badawi in June 2015, who had earlier been sentenced to 10 years in prison and 1,000 public lashes (see **Prosecutions and Detentions for Online Activities**).
- Mobile phone operators are now required to fingerprint cus omers when selling new SIM cards, limiting the ability of Saudis to use their phones anonymously (see **Surveillance, Privacy, and Anonymity**).

Introduction

Saudi internet freedom improved slightly in 2015-16 due to greater internet access, although the environment remains marked by pervasive censorship and severe punishments for online activism in support of human rights.

Amid fiscal t oubles, mounting tensions with Iran, and the ongoing Saudi-led airstrikes in Yemen, authorities in Saudi Arabia are on high alert for public expressions of dissent. The government continues to promote internet use as a tool for economic development and e-government services, where it is ahead of many countries in the region. Mobile broadband penetration continued to increase and Saudis remained some of the most active social media users in the world. But the country's highly centralized internet infrastructure facilitates state censorship, and restrictions on Voice-over-IP (VoIP) increase economic barriers for communication between Saudis and the outside world.

The internet is the least repressive space for expression in the country. Government ministers and public officials—such as the head f Riyadh's so-called morality police—have been dismissed from posts due to public uproar over viral videos of abuse on social media. Large numbers of Saudis use circumvention tools to access banned content and services, even if they are reluctant to express themselves due to strict legal penalties for political, social, or religious speech on certain topics.

Repression has been institutionalized under antiterrorism and cybercrime laws that have instilled fear into activists and ordinary social media users alike. Several well-known activists were sentenced to 8–10 years in prison over the past year, while ordinary citizens and migrant workers were also targeted for smaller online crimes. Social media is heavily monitored and law enforcement agencies have sought to break or bypass encryption in order to spy on users. While the internet has fundamentally changed the way that young Saudis interact with each other, the authoritarian tendencies of the country's political and religious establishments remain fully present in the minds of internet users, whose democratic aspirations remain blocked.

Obstacles to Access

Overall, infrastructure is not considered a major barrier to access except in remote and sparsely populated areas. Internet penetration is highest in major cities such as Riyadh and Jeddah, as well as in the oil-rich Eastern Province. Young Saudis make up the majority of the user population throughout the country.

Availability and Ease of Access

Saudis have enjoyed a rapid growth of internet and communications technologies (ICTs) in recent years. Access increased to 64.9 percent of the population in 2015, up from 41 percent in 2010.[1] Saudi Arabia is home to around 20 million internet users. Fixed broadband subscriptions stood at 45.3 percent of all households, with a majority using ADSL connections. Monthly expenditure on 4G broadband ranged from between SAR 55 (US$11) for a 2GB allowance to SAR 95 (US$25) for a 20GB

1 Communications and Information Technology Commission (CITC), *"ICT Indicators Charts: End of Q1 2015,"* 2016, https://bit.ly/1XIRceu.

allowance.[2] Household internet plus television bundles with fibe -optic connections range from SAR 300 (US$80) for speeds of 25 Mbps to SAR 800 (US$213) for 200 Mbps.[3]

Mobile broadband penetration has jumped from 94.5 percent in 2014 to 102 percent in 2015, with some 35 million mobile broadband subscriptions. Standard mobile phone subscriptions have reached to 51.8 million, resulting in a penetration rate of 167.7 percent.[4] Finally, 86.7 percent of mobile subscriptions are prepaid. The number of mobile subscriptions has dropped from a height of 56 million in 2011 as the government deported thousands of illegal workers and deactivated their prepaid mobile accounts.[5]

Restrictions on Connectivity

Saudi Arabia is connected to the internet through two country-level data services providers, the Integrated Telecom Company and Bayanat al-Oula for Network Services, up from a single gateway in years past. These servers, which contain a long list of blocked sites, are placed between the state-owned internet backbone and global servers. All user requests that arrive via Saudi internet service providers (ISPs) travel through these servers, where they can be fil ered and possibly blocked. International internet bandwidth increased from 318 Gbps in 2010 to 1321 Gbps in 2014.[6]

The country's regulator has taken an aggressive stance toward VoIP services that circumvent the country's regulatory environment and, by some indication, the surveillance apparatus. The use of Viber to make calls has been blocked since June 2013, while WhatsApp calling has been restricted since March 2015.[7] The authorities have also threatened to institute further restrictions on services such as Skype.[8]

ICT Market

The two country-level service providers offer services to licensed ISPs, which in turn sell connections to dial-up and leased-line clients. Broadband and mobile phone services are provided by the three largest telecommunications companies in the Middle East: Saudi Telecom Company (STC), Mobily (owned by Etisalat of the United Arab Emirates), and Zain (from Kuwait). Two newly licensed virtual operators have entered the market, operating on the infrastructure of existing companies: Virgin Mobile in October 2014 (operating with STC) and Lebara in December 2014 (operating with Mobily).

Several ISPs provide zero-rating services to consumers. For example, access to Wikipedia is provided free of charge by STC to all of its mobile data users,[9] while Zain provides unlimited access to YouTube as part of one of its prepaid mobile packages.[10]

2 Mobily, "Connect 4G," 2015, http://bit.ly/1tJ6Rch.

3 Mobily, "Package Prices," 2015, http://bit.ly/1sFClRf.

4 CITC, *"ICT Indicators Charts: End of Q1 2015,"* 2016, https://bit.ly/1XIRceu.

5 Matt Smith, "Saudi mobile subscriptions shrink on labor crackdown, hajj limits," *Al Arabiya News,* January 26, 2014 https://bit.ly/1HaGC9I.

6 CITC, *"Annual Report, 2014,"* 2015, https://bit.ly/1U9q2vL.

7 "WhatsApp's new call service to be blocked in KSA" *ITP.net*, March 17, 2015, http://bit.ly/2bPpYm0

8 "CITC blocks Viber", *Saudi Gazette*, June 5, 2013, http://bit.ly/1VLVW28.

9 Kul Wadhwa, "Wikipedia Zero reaches 230 million mobile users with Saudi Telecom partnership," *Wikimedia blog*, October 17, 2012, http://bit.ly/1NYU4gZ.

10 Zain, "Shabab Package," http://bit.ly/1NpWlWH.

Internet cafes, once prevalent, have become less popular in recent years due to the broad availability and affordability of home broadband access. Internet cafes are mainly used by youth from lower socio-economic backgrounds to congregate and socialize. Conversely, coffee shops have grown in popularity among business people, young adults, and single males, who enjoy free Wi-Fi access with their paid beverages.

Regulatory Bodies

Previously, all internet governance fell under the purview of the Internet Services Unit (ISU), a department of the King Abdulaziz City for Science & Technology (KACST). Established in 1998 and reporting directly to the Vice President for Scientific esearch Support of KACST, the ISU now only provides internet access to government departments, as well as Saudi research and academic institutions.[11] In 2003, the governmental Saudi Communication Commission was renamed to become the Communications and Information Technology Commission (CITC) and became responsible for providing internet access to the private sector, in addition to resolving conflicts among the private telecommunication companies.[12] The CITC is also responsible for controlling the price that telecommunications companies are allowed to charge for cross-network calls. For example, in February 2015, the maximum charge of local voice calls between different networks was lowered.[13] Furthermore, the CITC sends content removal requests to social networks in political cases (see "Content Removal" section below). The board of directors of the CITC is headed by the minister of communications and information technology.[14]

Limits on Content

The Saudi government continued to employ strict filtering of internet content throughout 2015 and early 2016. Self-censorship remains prevalent when discussing topics such as politics, religion, or the royal family. Nonetheless, high levels of social media use have driven an immense diversification of online content, offering Saudis a multitude of perspectives beyond state-controlled media. These tools have also been used by ordinary citizens and human rights activists to raise awareness of issues surrounding political reform, poverty, gender inequality, and corruption.

Blocking and Filtering

Popular social media and communication apps are not blocked in the country, although authorities have imposed restrictions on their use. For example, messaging app Telegram has faced throttling since January 9, 2016, when users reported severe bandwidth limitations preventing file- and image sharing.[15] Telegram's CEO confi med the issue, but said that the "reasons [behind the restrictions] are unknown."[16] VoIP services offered by popular apps have also been restricted (see "Restrictions on

11 CITC, "CITC Roles and Responsibilities", accessed March 2, 2013, http://bit.ly/1g9sAuI.

12 CITC, "Background," accessed on June 10, 2015, http://bit.ly/1KE1eLk.

13 "The Communication Commission Reduces the Charge Between Telecommunication Companies," [in Arabic] *Al Riyadh Newspaper*, February 22, 2015, http://www.alriyadh.com/1024133.

14 CITC, "Board of Directors", accessed on June 10, 2015, http://bit.ly/1OcShbq.

15 Amir-Esmaeil Bozorgzadeh , "UPDATED: Telegram's Troubled Times In The Middle East" *TechCrunch*, January 12, 2016, http://tcrn.ch/1PpVhhB.

16 Pavel Durov on *Twitter* https://bit.ly/1Qy2fHM, and The Telegram Team, "Voice Messages 2.0, Secret Chats 3.0 and..." *Telegram Blog*, February 12, 2016, https://bit.ly/1QWdTqr.

Connectivity").

Officiall , sites that are judged to contain "harmful," "illegal," "anti-Islamic," or "offensive" material are routinely blocked, including pages related to pornography, gambling, and drugs. Authorities also seek to disrupt violent networks and the dissemination of extremist ideology. Criticism of the Saudi royal family or that of other Gulf Arab states is not tolerated, and neither are sites that organize political opposition or question the ruling family's strict conception of Islam.[17] Websites that may be used to distribute copyrighted materials, such as the Pirate Bay,[18] are blocked.[19] In 2014, the Ministry of Communication and Information Technology (MCIT) blocked dozens of websites for failing to obtain an online publication license.[20] The practice continues, with the blockage of the London-based newspaper *Al-Araby Al-Jadeed* and its English equivalent *The New Arab* in January 2016.[21]

Websites and social media pages belonging to human rights or political organizations, such as the Saudi Civil and Political Rights Organization (ACPRA) and the Arab Network for Human Rights Information (ANHRI), are blocked.[22] Sites belonging to several Saudi religious scholars and dissidents are blocked,[23] as well as those related to the Shi'a religious minority, such as Rasid,[24] Yahosein, and Awamia.[25] Authorities also blocked the website of the Islamic Umma Party, the country's only underground (and illegal) political party, which has called for the royal family to step down.

Website mirroring is often used to circumvent blockage, but mirrors are often detected and blocked in a cat-and-mouse game. For example, authorities blocked the official ebsite for the "October 26th Women Driving campaign" on September 29th, 2013. One week later, a mirror site was also blocked.[26] The CITC has been developing blocking tools based on IP address, in order to prohibit websites from circumventing blockage by changing their domain name. Currently, this affects over 2,500 websites.[27] In one example, the CITC unblocked the website Mustamel after the owners complied with a request from the CITC to remove illegal advertisements.[28]

The CITC has also blocked individual social media pages that demand political reforms or civil rights. However, the move by many companies to standardize encrypted "HTTPS" communication has rendered much of this blockage useless, since it is technically very difficult for authorities o block individual pages on an HTTPS domain, rather than a standard HTTP domain. Authorities have occasionally moved to block entire online products and services for breaching the country's

17 "The censorship policy of websites that spread extremist ideologies has proven its success" [in Arabic] *Al Arabiya News*, December 22, 2012, https://bit.ly/1Fr25fm.

18 Ernesto, "Saudi Arabia Government Blocks The Pirate Bay (and More)," *TorrentFreak*, April 2, 2014, http://bit.ly/1KZwhQz.

19 "Ministry of Culture and Information blocks 52 websites for infringing the rights of authors," [in Arabic] *Al Riyadh Newspaper,* October 2012, https://bit.ly/1PrEspC.

20 Rory Jones and Ahmed al-Omran, "Saudi Arabia Plans to Regulate Local YouTube Content," *The Wall Street Journal*, April 24, 2014, http://on.wsj.com/1JQuBEu.

21 Jasper Jackson "Saudi Arabia, UAE and Egypt block access to Qatari-owned news website" *The Guardian*. 5 January 2016 https://bit.ly/1mzqvw2.

22 According to the Alkasir.com, which provides information on blocked websites, the URLs acpra6.org and anhri.net are blocked in Saudi Arabia: "Cyber-Censorship Map," Alkasir, accessed on March 2, 2013, https://alkasir.com/map.

23 Blocked websites of Saudi religious scholars include: www.almoslim.net, www.albrrak.net, and islamqa.info/ar;"Blocking some sites because they violate rules and spread bold ideas and theses" [in Arabic] *Al Arabiya*, April 6, 2012, http://bit.ly/1EUWChv.

24 Adala Center, "A list of blocked sites from within Saudi Arabia" [in Arabic] accessed on December 22, 2012, http://bit.ly/1NpMiAZ.

25 "Cyber-Censorship Map," Alkasir, accessed on March 2, 2013, https://alkasir.com/map.

26 Osama Khalid, "Saudi Authorities Block Women Driving Websites," *Global Voices*, October 8, 2013, http://bit.ly/1QmGLti.

27 CITC, *Annual Report 2014*, [in Arabic], pg 32 http://bit.ly/1L1xxCA.

28 "For the second time Haraj site blocked in Saudi Arabia" [in Arabic] *QBS News*, March 26, 2013, http://bit.ly/1VNpw7s.

strict laws. In September 2012, the government threatened to block all of YouTube if Google, the site's owner, did not restrict access to the controversial "Innocence of Muslims" video containing an offensive depiction of the Prophet Mohammed. Google later blocked the video in Saudi Arabia.[29]

The government responds to blockage requests from members of the public, who can use a web-based form to submit a complaint regarding undesirable material.[30] Once an individual submits the form, a team of CITC employees determines whether the request is justified. In 2014, the CI C received 466,863 blockage requests, and complied in 94.3 percent of cases. Pornographic content accounted for 85.6 percent of these requests. Sites can also be unblocked through a similar process.[31]

The government is somewhat transparent about what content it blocks. While the list of banned sites is not publicly available, users who attempt to access a banned site are redirected to a page displaying the message, "Access to the requested URL is not allowed!" In addition, a green background is displayed on sites blocked by the CITC, whereas sites blocked by the ministry of culture and information for licensing violations or copyright infringement have a blue background. The country's data service providers must block all sites banned by the CITC,[32] and failure to abide by these bans may result in a fine of up to SAR 5 million (US$1.33 million), according to Article 38 of the Telecommunication Act.[33] It should be noted, however, that many Saudi internet users have become savvy at using circumvention tools such as Hotspot Shield, which allows users to access a virtual private network (VPN) to bypass censorship,[34] but the websites of many other tools to circumvent blockage, such as Tor and the major VPN providers, are blocked by the government.[35]

Content Removal

Blocking and fil ering are compounded by the prior censorship that online news moderators and site owners must exercise. Gatekeepers frequently delete user-generated content that could be deemed inappropriate or inconsistent with the norms of society, as they can be held legally liable for content posted on their platforms.[36] This often results, for example, in keeping only progovernment user comments. It is unusual to find any antigo ernment comments on the websites of major Saudi newspapers, which do not reflect the di ersity of political views seen on social networks.

The CITC also sends requests to social networks to remove content. Facebook's Government Requests Report of the fi st half of 2014—the latest information available as of mid-2016—cites seven processed requests that were "reported by the Communications and Information Technology Commission (CITC) under local laws prohibiting criticism of the royal family."[37] Google report that removal requests jumped from zero to eight during the second half of 2015, with the majority of requests related to alleged religious offenses and ordered by executive agencies, rather than courts.

29 "YouTube blocks 'Innocence of Muslims' in Saudi Arabia", *Al Arabiya News*, September 19, 2012, http://bit.ly/1iv2VhN.

30 CITC, "Block Request Form, "Internet.gov.sa, http://web1.internet.sa/en/block.

31 CITC, "Unblock Request Form, "Internet.gov.sa, http://web1.internet.sa/en/unblock.

32 CITC, "General Information on Filtering Service", Internet.gov.sa, accessed on September 30,2012, http://bit.ly/1MbhO5y

33 Telecommunication Act of Saudi Arabia, [in Arabic], http://bit.ly/16Jzjj5.

34 Saudis refer to this circumvention tool as a "proxy breaker."

35 Examples include Hotspot Shield, Hide My Ass! and AirVPN.

36 "Raif Badawi's wife provides "Anhaa" with the list of charges against her husband and calls for his release [in Arabic] *Anhaa*, April 25, 2013, http://www.an7a.com/102662.

37 Facebook, "Saudi Arabia," *Government Requests Report,* January-June 2014, accessed on November 4, 2014, http://bit.ly/1VLX6ec.

Google complied in 14 percent of cases.[38] On the other hand, Twitter reported only one removal request from July 2015 to June 2016, which resulted in an account being reported.[39]

Copyright takedown requests have also been used to restrict political speech. In September 2014, an episode of a satirical show on YouTube called *Fitnah* was censored when the Saudi TV channel Rotana sent a Digital Millennium Copyright Act (DMCA) notice to take it down. The show used footage from the channel to criticize its owner, Prince Waleed Bin Talal, who was accused by the show of being responsible for the takedown request.[40] The video was later restored.[41]

Media, Diversity, and Content Manipulation

Social media users are increasingly careful about what they post, share, or "like" online, particularly after the passage of a new antiterrorism law in 2014. Users who express support for extremism, liberal ideals, minority rights, or political reforms, in addition to those who expose human rights violations, are closely monitored and often targeted by the government. Questioning religious doctrine is strictly taboo, particularly content related to the prophet Mohammed. Influential witter users are growingly fearful of expressing support for outspoken activists who have been recently sentenced to jail time. Government consultants have stopped contributing to foreign newspaper articles due to pressure from other government agency representatives.

With so much activity occurring on social networks, the Saudi government maintains an active presence online as a means of creating the illusion of popular support for its policies. It is believed the government employs an "electronic army" to constantly post progovernment views, particularly on social media. Progovernment trolls have taken to "hashtag poisoning," a method of spamming a popular hashtag in order to disrupt criticism or other unwanted conversations through a flood f unrelated or opposing tweets. Through the use of a "bot," such as those provided by Yoono.com, one individual can send thousands of tweets to a hashtag at the same time.[42] While the tweet may contain the same message, the bot sends the tweet on behalf of numerous fabricated accounts, created by combining random photos of faces with names culled from the internet. The government also influences online news eporting by offering financial suppo t to news sites such as *Sabq* and *Elaph* in return for coordination between site editors and the authorities.[43]

Whereas the authorities provide monetary support to progovernment websites, the owners of opposition websites can come under strong financial p essures as a result of the country's environment of censorship. Revenue from third-party advertisers can be heavily impacted by a government decision to block a website. The government can also request advertisers cancel their ads on a particular website in order to pressure the website to close. Restrictions on foreign funding further inhibit the sustainability of websites that are critical of the ruling system. Numerous sites

38 Google, "Saudi Arabia," Transparency Report, https://www.google.com/transparencyreport/removals/government/SA/?hl=en.

39 Twitter , "Saudi Arabia," *Transparency Report*, https://transparency.twitter.com/en/countries/sa.html.

40 "YouTube Blocks Fitna Show In Response to a Request from Rotana." [in Arabic] al-Tagreer, September 7, 2014. https://bit.ly/1Tb7KKZ [offline

41 Maira Sutton, "Copyright Law as a Tool for State Censorship of the Internet," Electronic Frontier Foundation, December 3, 2014, http://bit.ly/1rVSJmg.

42 "Fake accounts and drowning the hashtag in Twitter [in Arabic] *Osama Al Muhaya*, March 16, 2013, http://bit.ly/1Q13N8g.

43 "Othman Al-Omair in Turning Point 8-5" [in Arabic] YouTube video, 8:11, published by Alnahry2009, May 31, 2010, http://bit.ly/1LXn9um.

have been closed for copyright violations,[44] or for featuring advertisements for drugs.[45]

Arabic content is widely available, as are Arabic versions of applications such as chat rooms, discussion forums, and social media sites. While opposition blogs and online forums were once the main venue for discussing political and social matters, most Saudis now use social media instead. Similarly, Saudis are the largest adopters of Twitter in the Arab world.[46] In 2015, it was estimated that 53 percent of internet users in Saudi Arabia have accounts on Twitter.[47]

Saudi companies such as C3 (Creative Culture Catalyst) and Jeddah-based UTURN have sprung up to provide funding and support for video production in the kingdom, with great success. Fahad Albutairi, host of the YouTube show La Yekthar, touches on social and political issues, such as women's right to drive. Opposition figu es abroad use YouTube as a platform for distributing their audio and video content, since their websites are blocked within the country.[48] Omar Abdulaziz, founder of the Yakathah channel on YouTube, produces political commentary shows from Canada which are very critical of progovernment propaganda and call for political reform.

Digital Activism

Saudis have employed online tools for holding government officials accountable, mainly th ough the use of smartphones to capture videos of corruption or improper behavior. In February 2016, the head of the Committee for the Promotion of Virtue and the Prevention of Vice (CPVPV) in Riyadh was dismissed after a video showing members of the CPVPV chasing a girl outside a mall in the Saudi capital.[49] That same month, online uproar over the airing of a documentary about Hezbollah's leader by the Saudi-funded Al-Arabiya news channel led to the dismissal of its head, Turki al-Dukial.[50] Local media took both cases as gestures of the new king's intolerance for public officials' mo es to offend the "dignity" of citizens.[51]

Activists from the local LGBTI community have used digital tools to push back against online hate speech. By reporting account violations to YouTube and Twitter, activists took down popular local accounts such as the YouTube comedy channel Fe2aFala, which had called for the execution of all homosexuals in an episode featuring a reported same-sex wedding party in Riyadh, as well as the Twitter accounts of @_YAS8R_ for inciting violence against homosexuals and @I_mohdiary (which has over one million followers) for comparing homosexuals to animals. Some of these accounts have been restored after removing the offensive content.

The anonymous Twitter user @Mujtahidd, which was called "Saudi's Julian Assange,"[52] continues

44 "CITC closed down Haraj site after advertising half kilo Hashish," [in Arabic], *AlSharq Newspaper*, March 30, 2013, http://bit.ly/1LXn9um.

45 "Saudi Arabia closes 52 sites violated intellectual property copyrights," [in Arabic], *Ameinfo*, October 16, 2012, http://www.ameinfo.com/ar-248952.html [offline

46 Lori Plotkin Boghardt,"Saudi Arabia's War on Twitter," *Middle East Voices,* December 12, 2013, http://bit.ly/1hdwdd7.

47 Arab Social Media Report 2015, p34 http://bit.ly/1oDXLDB

48 Examples include Sa'ad Al-Faqih, Mohammad al-Massari and Mohammad al-Mofarreh.

49 "Saudi Arabia: The head of the Committee for the Promotion of Virtue and the Prevention of Vice in Riyadh Abdullah al-Fawaz was dismissed" *ArabianBusiness.com*, February 14, 2016, http://bit.ly/2boxEvh.

50 "A 'Saudi Version' of 'Hassan' Story'", *al-Araby al-Jadeed*, February 24, 2016, http://bit.ly/2fl7RI .

51 "Salman stands for the dignity of the nation, and protects the freedom of the press...," [in Arabic], *Sabq*, May 5, 2015, http://sabq.org/uO5gde.

52 "Saudi's 'Julian Assange' returns to Twitter," BBC, March 12, 2015, http://www.bbc.com/news/blogs-trending-31840424.

to criticize high profile membe s of the royal family[53] and to provide detailed descriptions of state corruption.[54] The popularity of the account has increased more than fourfold, from around 410,000 Twitter followers in June 2012 to over 1.8 million as of June 2015. In 2013, the user shared the tweets of dozens of users who defended the government using the exact same wording, thus illustrating the presence of a government Twitter "army."[55] In March 2015, the account was suspended several times over the course of two days, but was reinstated without explanation.

Following attacks by Islamic State militants on Shiite mosques in the Eastern Province in October 2015 and January 2016, large funeral marches were called for through Twitter and Facebook. These marches included explicit political statements, such as calling for the banning of hate speech. Similarly, after the execution of Shiite cleric Nimr al-Nimr on January 2, 2016, several small protests were organized in the Eastern Province, which were covered through Twitter and YouTube. However, numerous arrests and lengthy prison sentences have had an overall chilling effect on online activism.

Violations of User Rights

Saudi courts have delivered some of the harshest prison sentences against online users in the world, with numerous human rights defenders jailed for periods of 10 to 15 years for their online activities. The legal environment surrounding online expression remains a significant impediment to internet freedom, and it has only worsened over the past year. The 2014 antiterrorism law, which equates "insulting the reputation of the state" with terrorism, was used to prosecute peaceful activists.

Legal Environment

Saudi Arabia has no constitution. The Basic Law of Saudi Arabia contains language that calls for freedom of speech and freedom of the press, but only within certain boundaries. The 2000 Law of Print and Press also addresses freedom of expression issues, though it largely consists of restrictions on speech rather than protections. Online journalists employed at newspapers and other formal news outlets maintain the same rights and protections as print and broadcast journalists, and like their counterparts, are also subject to close government supervision. Similarly, laws designed to protect users from cybercrimes also contain clauses that limit freedom of expression. The 2007 Anti-Cyber Crime Law criminalizes "producing something that harms public order, religious values, public morals, the sanctity of private life, or authoring, sending, or storing it via an information network," and imposes penalties of up to fi e years in prison and a fine f up to SAR three million (US$800,000).[56]

The antiterrorism law, passed in January 2014, defines errorism in such vague terms as "insulting the reputation of the state," "harming public order," or "shaking the security of the state," effectively criminalizing a range of nonviolent speech.[57] Article 1 of the law defines calling for atheist thought in any form" as terrorism.[58] Article 4 prohibits support for banned groups by "circulating their

53 Robert F. Worth, "Twitter Gives Saudi Arabia a Revolution of Its Own," *The New York Times*, October 20, 2012, http://www.nytimes.com/2012/10/21/world/middleeast/twitter-gives-saudi-arabia-a-revolution-of-its-own.html.

54 "Saudi's 'Julian Assange' returns to Twitter," BBC, March 12, 2015, http://www.bbc.com/news/blogs-trending-31840424.

55 Assaflovhotmail, witter post, February 28, 2013, 7:04 PM, http://bit.ly/1EOATbn.

56 Kingdom of Saudi Arabia, Royal Decree No. M/17, Anti-Cyber Crime Law, March 2007, http://bit.ly/VWXEmI.

57 Human Rights Watch, "Saudi Arabia: New Terrorism Regulations Assault Rights," March 20, 2014, http://bit.ly/1d3mLN9.

58 Elliot Hannon, "New law in Saudi Arabia Labels All Atheists as Terrorists," *Slate*, April 1, 2014, http://slate.me/1ifyNk9.

contents in any form, or using slogans of these groups and currents [of thought], or any symbols which point to support or sympathy with them" through audio, visual, or written format, including websites and social media.[59]

Prosecutions and Detentions for Online Activities

Saudi Arabia's restrictive laws have been rigorously applied to silence critical voices and human rights defenders. Since traditional political organizing is banned in the country, many human rights activists conduct activities online given the reach of social media tools in the country. As a result, the authorities often prosecute activists for setting up websites, posting on Twitter, or appearing in YouTube videos documenting human rights abuses or calling for government action.

For example, in October 2015, the Specialized Criminal Court found human rights activist Abdelrahman al-Hamid guilty of inciting public opinion through Twitter, demanding a constitutional monarchy, and storing illegal materials. He was sentenced to nine years in prison, barred from traveling abroad for nine years after his release, and fined US$13,300. Al-Hamid is a co-founder f the Saudi Civil and Political Rights Association (ACPRA).[60]

Also in October, Prof. Abdulkareem al-Khadar, a co-founder of ACPRA, was sentenced to 10 years in prison and a subsequent 10-year travel ban.[61] Prof. al-Khadar had been detained since April 2013 and charges included uploading ACPRA statements and video lectures, although the final erdict was not published. Moreover, Abdulaziz al-Sinedi was sentenced to eight years in prison and barred from traveling for another eight years for inciting public opinion, questioning the independence of the judiciary, and describing Saudi Arabia as a police state.[62]

A court in Riyadh disbanded the ACPRA in March 2013 and sentenced two of its members, Abdulah al-Hamid and Mohammed al-Qahtani, to 11 years and 10 years of jail time respectively, in addition to a travel ban equal in length to their jail sentences.[63] Five years of their sentences were based on Article 6 of the Anti-Cyber Crime Law, relating to the creation of a website that could disturb social order.[64] Six founding members of ACPRA are currently in detention.[65] Two founding members of the Islamic Umma Party, al-Wahiby and al-Gamidi,[66] have been in prison since February 2011.[67] Both the ACPRA and the Islamic Umma Party base many of their operations online.

Raif Badawi, the co-founder of the Saudi Arabia Liberals website who has been imprisoned since June 2012, had his sentence increased from 7 to 10 years in jail and from 600 to 1,000 public lashes,

59 Human Rights Watch, "Saudi Arabia: New Terrorism Regulations Assault Rights," March 20, 2014, http://bit.ly/1d3mLN9.

60 "Nine years in prison for a citizen who incited the public opinion against the state and its security agencies using Twitter." *Al Riyadh,* October 16, 2015, http://www.alriyadh.com/1091447.

61 The Associated Press, "Saudi Arabia: Activist Professor Gets 10-Year Sentence" *The New York Times*, October 20, 2015, http://nyti.ms/1VAnJCa.

62 The Associated Press, "Saudi Arabia: 2 Activists Sentenced," *The New York Times*, October 14, 2015, http://nyti.ms/1RjtHWV.

63 "10 years jail for Al-Qahtani and 11 for Al-Hamid in the ACPRA case" [in Arabic], *Sabq*, March 9, 2013, http://sabq.org/onyfde.

64 CITC, "Anti-Cyber Crime Law," March 2007 http://bit.ly/VWXEmI.

65 Those members are Suliaman Al-Rushoody, Mansour Al-Awth, Mousa Al-Garni, Mohamed Al-Bijadi, Saleh Al-Ashwan and Fawzan Al-Harbi.

66 Islamic Umma Party, Twitter Page, accessed on December 22, 2012, http://twitter.com/islamicommapart.

67 Islamic Umma Party, Twitter Page, accessed on March 10, 2012, http://twitter.com/islamicommapart.

as well as a fine f SAR one million (US$266,000) in early May 2014.[68] Badawi was charged with "setting up a website that undermines general security" and "ridiculing Islamic religious figu es." On January 9, 2015, Badawi received 50 lashings outside a mosque in Jeddah, following Friday prayer. Footage of the punishment was uploaded to YouTube, resulting in a massive international backlash.[69] Further lashings have been postponed.[70] His case was heard by the Supreme Court, which upheld the verdict in June 2015.[71]

Samar Badawi, a human rights advocate and Raif's sister, was briefly ar ested in January 2016[72] and charged with managing her detained ex-husband's account on Twitter, @WaleedAbulkhair. She was released on the following day and ordered to report to a police station for further interrogation.[73]

Ashraf Fayadh, a Palestinian poet based in Saudi Arabia, has been detained since January 1, 2014 on apostasy charges after a complaint that he was spreading atheism through his poetry. He was also charged with violating Article 6 of the country's Anti-Cyber Crime Law for taking and storing photos of women on his phone.[74] On November 17, 2015, Fayadh was convicted of apostasy and sentenced to beheading.[75] However, his sentence was reduced to eight years in prison and 800 lashes on February 2, 2016.[76]

On March 25, 2016, columnist Alaa Brinji was sentenced to fi e years in prison, an eight-year travel ban, and a fine f SAR 50,000 (US$ 13,300) for tweeting in support of women's right to drive, human rights defenders, and prisoners of conscience.[77]

Authorities have stepped up arrests and prosecutions against ordinary citizens as well. Among some of the cases from the coverage period:

- A Saudi man was sentenced to 10 years in prison, 2,000 lashes, and a SAR 20,000 (US$ 5,300) fine for spreading atheism online" in February 2016 under the Anti-Cyber Crime Law for 600 "atheist" tweets.[78]
- In December 2015, a Twitter user was sentenced to fi e years in prison and a subsequent fi e-year travel ban for "calling for protests through Twitter", "retweeting posts by suspicious

68 Ludovica Iaccino, "Saudi Arabian Online Liberal Activist Raif Badawi Sentenced to 1,000 lashes," *International Business Times*, May 8, 2014, http://bit.ly/1NpU0Lu.

69 Press Association, "Prince Charles raises Raif Badawi case with Saudi king," *The Guardian,* February 10, 2015, http://gu.com/p/45yxv/stw.

70 AFP, "Saudi Arabia postpones flogging f Raef Badawi for third week," *The Guardian*, January 30, 2015, http://gu.com/p/45c4y/stw.

71 AP, "Saudi Arabia: Verdict on Blogger Stands," *The New York Times,* June 7, 2015, http://nyti.ms/1IwJwYE.

72 Ben Hubbard, "Saudi Arabia Arrests Samar Badawi, Human Rights Advocate" *The New York Times*, January 12, 2016, http://nyti.ms/1ZjnHiB

73 Ian Black and Jessica Murphy, "Sister of Saudi blogger Raif Badawi briefly detained in same prison" *The Guardian*, January 13, 2016, http://bit.ly/1OpQQ6H.

74 "Poet faces death for apostasy in Saudi Arabia: Ashraf Fayadh" Amnesty International, November 24, 2015, http://bit.ly/1lg3b5f.

75 Ben Hubbard, "Artist's Death Sentence Follows a String of Harsh Punishments in Saudi Arabia," *The New York Times,* November 22, 2015, http://nyti.ms/1mTUgah.

76 Ben Hubbard, "Saudi Court Spares Poet's Life but Gives Him 8 Years and 800 Lashes," *The New York Times,* February 2, 2016, http://nyti.ms/1Pz2EY8.

77 "Saudi Arabia: Journalist sentenced to fi e years in prison for tweets latest victim of crackdown," Amnesty International, March 25, 2016, http://bit.ly/2bjsWwA.

78 "Punishing a citizen for publishing 600 atheist tweets" *Al Watan*, February 27, 2016, http://bit.ly/2bhvDSy

accounts", and "destroying his phone to hide the evidence."[79]

- In January 2016, a physician and a pharmacist were respectively sentenced to 6 months in prison and 100 lashes, and 4 months in prison and 100 lashes, for the defaming the ministry of health on Twitter.[80]
- In March 2016, Abdul Sattar Makandar, an Indian laborer, was arrested for denouncing working conditions via a Facebook video. A crowdfunding campaign was started to cover his legal expenses and the cost of his flight home [81] As of August 2016, he was still detained.[82]
- In May 2016, the Specialized Criminal Court sentenced a Saudi woman to six years in prison, two of which were in accordance with the Anti-Cyber Crime Law for producing videos that call for the release of detainees and publishing them through Twitter.[83]

Online defamation has also grown. The overall number of defamation cases heard by courts reached over 350 in the period from October 2014 to October 2015; most of the cases are related to social media.[84]

Surveillance, Privacy, and Anonymity

Surveillance is rampant in Saudi Arabia, which justifies pe vasive monitoring of political, social, and religious speech under the pretense of protecting national security and maintaining social order. The authorities regularly monitor websites, blogs, chat rooms, social media sites, emails and mobile phone text messages. Evidencing the government's determination to monitor its citizens, the American security expert Moxie Marlinspike published email correspondence with an employee at Mobily who sought to recruit him to help the telecommunications fi m intercept encrypted data from mobile applications such as Twitter, Viber, Vine, and WhatsApp.[85]

The Ministry of Culture and Information requires that all blogs, forums, chat rooms, and other sites obtain a license from the ministry to operate, thus putting more pressure on online writers to self-regulate their content.[86] However, this rule is enforced only on popular online publications. Even anonymous users and writers who employ pseudonyms when making controversial remarks face special scrutiny from the authorities, who attempt to identify and detain them.

In January 2016, the CITC required mobile network operators to register the fingerprints f new SIM card subscribers, and announced that it would soon mandate existing subscribers to register their fingerprints as ell. The CITC said that the new requirement is meant to "limit the negative effects and violations in the use of communication services."[87] This added to the previous legal requirement

79 "Five year in prison for a citizen who called for protests on Twitter" [in Arabic] *Al-Riyadh Newspaper*, http://www.alriyadh.com/1111065

80 "Imprisonment and lashing for two employees for criticizing the health department in Najran" [In Arabic] *Makkah Newspaper* 10 January, 2016 https://bit.ly/1TBetQn.

81 "Let's Bring Abdul Sattar Home", Ketto, https://www.ketto.org/fundraiser/bringabdulhome.

82 Kundan Srivastava on Facebook http://bit.ly/2bOIMRK.

83 "Six years in prison for a citizen who tempted people in Unaizah," *Al Riyadh*, May 11, 2016, http://www.alriyadh.com/1502213.

84 "Riyadh is the highest in defamation cases with 41%" October 10, 2015 http://www.an7a.com/206507/.

85 Moxie Marlinspike, "A Saudi Arabia Telecom's Surveillance Pitch", *Thought Crime* (blog), May 13, 2013, http://bit.ly/101IYnw.

86 Reporters Without Borders, "Saudi Arabia," *Internet Enemies*, 2012, http://bit.ly/JrLevJ.

87 "Communication Commission mandates companies to register fingerpri ts before issuing cards " [in Arabic], *Al-Riyadh Newspaper*, January 22, 2015, http://bit.ly/1WEBQ9H

of registering subscribers' real names and identity numbers, and mandating the collection of ID numbers in order to recharge a prepaid mobile card,[88] which was often circumvented by a black market in which vendors sold new SIM cards and prepaid refill ca ds with pre-existing ID numbers.[89]

Intimidation and Violence

Progovernment Twitter accounts often defame and harass political and social activists using hashtags calling for their arrest. The anonymous accounts often show photos of the king or the interior minister as their avatars. For example, after *The Economist* released a YouTube interview with political activist Loujain al-Hathloul and social critic Fahad Albutairi,[90] Twitter and WhatsApp users accused them of treason and called for their arrest. Furthermore, as legal limits on the detention of suspects were removed, numerous Saudis are now arbitrarily detained for periods of months—and sometimes years—without charge.

Technical Attacks

On June 20, 2015, WikiLeaks announced the release of over 60,000 documents collected from Saudi Foreign Ministry emails. The documents contained top-secret correspondence between Saudi embassies and local parties in countries such as Egypt, Lebanon, Iraq, and Afghanistan.[91] The official Twitter account of the foreign ministry called on citizens not distribute the documents in order to avoid "aiding the enemies of the nation." A foreign ministry spokesman acknowledged that the documents were related to a recent electronic attack and claimed that many were "clearly fabricated," saying that those who distributed the documents would be punished under the country's cybercrime law.[92]

On February 16, 2016, the official, erified witter account of the minister of education, @aleissaahmed, was hacked. The hacker posted messages critical of the ministry's performance on issues such as the lack of care for handicapped students and the relocation of teachers to rural areas far from their families.[93] The account was later restored.

On May 22, 2016, the Twitter account of the ministry of labor was briefly hac ed, with one tweet posted stating: "The account was hacked. You need to enable security, Ministry of Labour."[94]

On June 3, 2016, hackers infiltra ed the website of a*l-Watan* newspaper and posted a fabricated statement by the crown prince condemning Saudi foreign policy in Yemen and Syria.[95] The editor-in-chief of the site accused Iran or the so-called Islamic State as being responsible.[96]

88 "User's ID number now required to recharge prepaid mobile phones", *Arab News*, July 4, 2012, http://bit.ly/1azmvzS.

89 Faleh Al-Buyani, "Black market for SIM cards with ID thriving", *Saudi Gazette*, December 31, 2012, http://bit.ly/1Q1amYu.

90 Arrested and jailed for driving in Saudi Arabia" *The Economist*, January 22, 2016, https://youtu.be/XsQaIdTph5Q.

91 Saeed Shah, "Saudi Officials Lin ed to Jihadist Group in WikiLeaks Cables" June 28, 2015 http://on.wsj.com/1Kjc6Md.

92 Ben Hubbard, "Cables Released by WikiLeaks Reveal Saudis' Checkbook Diplomacy" *The New York Times*, June 20, 2015, http://nyti.ms/1CkuFJb.

93 "The account of the Minister of Education was hacked" *Al Riyadh*, February 16, 2016, http://www.alriyadh.com/1129253.

94 "Official witter account of the Ministry of Labor was hacked," al-Sharq Portal, May 22, 2016, http://www.al-sharq.com/news/details/423081.

95 "Saudi Al Watan confi ms: it was hacked and 'dishonest statements' of Prince Mohammad bin Nayef where distributed," CNN Arabia, June 5, 2016, http://cnn.it/2bGwMTB.

96 "Saudi Al Watan Editor-in-Chief: Iran hacked the website," Al Arabiya, June 5, 2016, http://bit.ly/2bQnST2.

Freedom House

Singapore

	2015	2016
Internet Freedom Status	Partly Free	Partly Free
Obstacles to Access (0-25)	6	6
Limits on Content (0-35)	14	14
Violations of User Rights (0-40)	21	21
TOTAL* (0-100)	**41**	**41**

* 0=most free, 100=least free

Population:	**5.5 million**
Internet Penetration 2015 (ITU):	**82 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- The High Court ordered blogger Roy Ngerng to pay SGD 150,000 (US$106,000) in damages for defaming the prime minister (see **Prosecutions and Detentions for Online Activities**).
- The founder of *The Real Singapore* website was sentenced to ten months in prison under the Sedition Act for exploiting racial and xenophobic feelings (see **Prosecutions and Detentions for Online Activities**).
- Teenager Amos Yee, previously jailed for online video posts, was arrested again for wounding the feelings of religious groups (see **Prosecutions and Detentions for Online Activities**).
- Independent current affairs website *The Middle Ground* was asked to register its staff with the regulator and forego foreign funding (see **Media, Diversity and Content Manipulation**).
- The High Court ruled that the government cannot use a new antiharassment law to protect itself from criticism (see **Legal Environment**).

Introduction

The internet freedom environment saw no overall change in 2016, as website regulation and prosecutions for online speech continued at the same rate.

General elections held on September 11, 2015, were won handsomely by the ruling People's Action Party (PAP). The previous election, in 2011, had seen Singapore's tiny opposition make significant advances. Disaffection against the government had been mirrored—and to some extent catalyzed—by dissent on the internet, which has been largely free from prior restraints. In 2015, the PAP's share of the popular vote jumped from 2011's 60 percent (the lowest since Singapore became an independent republic in 1965) to an unexpectedly high 70 per cent. Observers credited the rebound mainly to the PAP's success in addressing key grievances, especially over housing affordability, and to the wave of national sentiment generated by the death of founding Prime Minister Lee Kuan Yew in March 2015.[1]

Changes in internet policy may have also contributed to the stronger PAP performance. While firmly committed to the internet as essential infrastructure for economic development, it has always been cautious of the technology's potential for enhancing democratic participation. Since 2012, it has launched a series of regulatory innovations and court actions to curb online dissent. The PAP also invested significantly in its own social media capacity. Whereas in 2011, internet opinion was dominated by antigovernment voices, the 2015 online terrain was much more evenly contested.

The internet remains Singapore's most important platform for alternative voices, as it is significantly freer than other media, and institutional or public spaces. However, the results of the 2015 general election show that the internet cannot be expected to usher in wider liberalization in the short term.

Obstacles to Access

As a wealthy and compact city-state, Singapore has highly developed information and communication technology (ICT) infrastructure. Its Intelligent Nation 2015 master plan for an ultra-high-speed, pervasive network achieved the target of 90 percent home broadband penetration. In addition, the national wireless network offers free public access. In late 2014, the government launched a high-level Smart Nation program that will include education and training to boost Singaporeans' skills in developing digital technologies and applications.

Availability and Ease of Access

Eighty-eight percent of resident households—and 98 percent of those with school-going children—had home internet access in 2014.[2] The International Telecommunication Union estimated individual internet penetration at 82 percent in 2015.[3] In mid-2015, there were almost 50 percent more mobile phone subscriptions than people in the country.[4] The fibe -based Next Generation Nationwide

1 Terence Lee and Kevin YL Tan (eds.), *Change in Voting: Singapore's 2015 General Election.* Singapore: Ethos Books, 2016.
2 Infocomm Development Authority of Singapore (iDA), https://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Facts%20and%20Figures/SurveyReport/2014/2014%20HH%20public%20report%20final.pd .
3 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1cblxxY.
4 iDA, "Statistics on Telecommunications Services," https://www.ida.gov.sg/Tech-Scene-News/Facts-and-Figures/Telecommunications/Statistics-on-Telecom-Services/Statistics-on-Telecom-Services-for-2015-Jan-Jun.

Broadband Network (Next Gen NBN) reached 95 percent of homes and businesses by July 2013. The national wireless network, Wireless@SG, offers free public access. In December 2015, there were 10,000 Wireless@SG hot spots at more than 3,000 locations. The government aims to double the number of hot spots by 2018. Speeds will be increased from 2Mbps to 5Mbps by the end of 2016.[5]

In late 2015, the Infocomm Development Authority started trials for a heterogeneous network (HetNet), a new wireless system that allows smartphone users to hop automatically across cellular and wifi net orks for smoother mobile internet use.[6]

The government's current IT masterplan, called Smart Nation, aims to integrate technologies more seamlessly and improve Singaporeans' skills in creating, as well as using, new technologies. A Smart Nation Programme Office has been set up under the prime minis er's office, in line with a "whole-of-Government, whole-of-nation approach."[7]

The digital divide cuts mainly along generational lines. While 99 percent of residents aged 15 to 24 reported in 2014 that they had used the internet in the past three months, the percentage was 31 percent for those aged 60 and older.[8] The government's Digital Inclusion Fund aims to make internet connectivity more accessible and affordable to older and lower-income Singaporeans.[9] Under its Silver Infocomm Initiative, it has set up hotspots and IT learning centers for senior citizens across the island.[10]

Restrictions on Connectivity

No known restrictions have been placed on ICT connectivity or access to social media or communication apps, either permanently or during specific e ents. The Singapore Internet Exchange (SGIX), a not-for-profit established by the Infocomm De elopment Authority of Singapore in 2009, provides an open, neutral and self-regulated central point for service providers to exchange traffic with one another directly instead of routing through international carriers, thus improving latency and increasing resiliency when there are cable outages on the international network.[11]

Singapore has adopted a National Broadband Network (NBN) structure, with the network built and operated by an entity that supplies telecommunications services on a wholesale-only, open-access, and non-discriminatory basis to all telecommunications carriers and service providers.[12] To develop Singapore's all-fiber Next Generation NBN, a structurally se arated network company has responsibility for the passive infrastructure, including the optical fibe . An operationally separate operating company is responsible for the active infrastructure, including routers, switches, and access network equipment. These are supposed to be separate from the retail service providers downstream, to avoid conflicts f interest. However, in 2013, the IDA approved the sale of the network company

5 Irene Tham, "Wireless@SG: 5Mbps speed by year end," *Straits Times,* April 12, 2016, http://www.straitstimes.com/tech/wirelesssg-5mbps-speed-by-year-end.

6 "HetNet trials at Jurong Lake District to start from Q3," August 22, 2015, http://www.channelnewsasia.com/news/business/hetnet-trials-at-jurong/1800288.html.

7 iDA, "Transcript of Prime Minister Lee Hsien Loong at Smart Nation Launch, 24 November 2014," November 24, 2015, http://bit.ly/1v88lB2.

8 iDA, "Infocomm Usage," https://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Facts%20and%20Figures/SurveyReport/2014/2014%20HH%20public%20report%20final.pd .

9 iDa, "Home Access," http://www.ida.gov.sg/Learning/Community-Development/Digital-Inclusion-Fund/Home-Access.

10 iDa, "Silver Infocomm Initiative," https://www.ida.gov.sg/Learning/Community-Development/Silver-Infocomm-Initiative.

11 Singapore Internet Exchange, "About Us," http://www.sgix.sg/about/.

12 iDA, "Building Singapore's Next Generation Nationwide Broadband Network, http://bit.ly/1LlvOnl.

OpenNet, which is responsible for building and operating the passive infrastructure, to a unit of government-linked Singapore Telecom (SingTel). Due to other players' concerns that the acquisition was anticompetitive, regulators required that SingTel sell off 75 percent of its stake in that unit by April 2018.[13]

ICT Market

The dominant internet access providers are also the mobile telephony providers: SingTel, Starhub, and M1. SingTel, formerly a state telecom monopoly and now majority owned by the government's investment arm, has a controlling stake in Starhub. The market is open to independent entrants. MyRepublic launched a broadband service in 2014. In October 2015, it started 4G trials to prepare for its bid for a telco licence.[14] ViewQwest, another new player in the broadband market, was launched in 2015.[15]

Regulatory Bodies

In January 2016, the government announced that its two main internet regulators would be restructured in the second half of the year. The Infocomm Development Authority of Singapore (IDA) has been responsible for internet infrastructure, while the Media Development Authority (MDA) oversaw content. They will be succeeded by the Infocommunications Media Development Authority (IMDA) and the Government Technology Organisation (GTO). IMDA will develop and regulate the converging infocommunications and media sectors.[16] Like the bodies that preceded it, it will be a statutory body of the Ministry of Communications and Information (MCI), taking instruction from the cabinet.

In planning the all-fiber Next Gen NBN, egulators have promised a competitive industry structure that would avoid conflicts f interest and allow retail service providers that offer services to end users to purchase bandwidth connectivity at nondiscriminatory and nonexclusive prices.

Limits on Content

The government has kept a 1996 promise not to block or filter any political content. During the coverage period, there was no repeat of the May 2015 order to shut down a political website, the only such case to date. A licensing system introduced in 2013 has been used to limit the growth of independent online news start-ups by restricting their funding options. During the coverage period, one more site was added to the list of those required to register. Despite such measures, the internet remains significantly more open than print or broadcasting as a medium for news and political discourse, which flow online largely unhindered. Restraints in online discourse are mainly due to fear of post-publication punitive action—especially through strict laws on defamation, racial and religious insult, and contempt of court (see Violations of User Rights).

13 . Tan Weizhen. "IDA approves OpenNet sale to CityNet, but with conditions," *Today*, November 21, 2013, http://www.todayonline.com/singapore/ida-approves-opennet-sale-citynet-conditions.

14 Irene Tham, "MyRepublic starts 4G trials as part of bid for fourth telco licence," *Straits Times,* October 23, 2015, http://www.straitstimes.com/tech/myrepublic-starts-4g-trials-as-part-of-bid-for-fourth-telco-licence.

15 Shivaanan Selvasevaran, "ViewQwest sets sights on smart home market," Channel News Asia, November 19, 2015, http://www.channelnewsasia.com/news/singapore/viewqwest-sets-sights-on/2275218.html.

16 Irene Tham, "Merger of IDA, MDA spurred by changes in tech," *Straits Times,* January 27, 2016, http://www.straitstimes.com/singapore/merger-of-ida-mda-spurred-by-changes-in-tech.

Blocking and Filtering

The Broadcasting Act has included explicit internet regulations since 1996. Internet content providers and internet service providers (ISPs) are licensed as a class and must comply with the act's Class License Conditions and the Internet Code of Practice. Under this regime, ISPs are required to take "all reasonable steps" to fil er any content that the regulator deems "undesirable, harmful or obscene."[17]

As a matter of policy, the MDA blocks a list of only 100 websites for the purpose of signposting societal values. This fl ating list has never been made public, but no political site has been blocked. Other than a few overseas sites run by religious extremists, the list is known to comprise pornographic sites.[18] Outside of this list, the Canada-based extramarital dating website, Ashley Madison, has been blocked since 2013, after it announced its plan to launch in Singapore.[19] No other site was subsequently singled out for similarly targeted blocking. The use of regulation to signpost social values has been linked to the influence f religious conservatives (mainly evangelical Christians) asserting themselves more in public morality debates.[20]

The Broadcasting Act empowers the MCI minister to prohibit disclosure of any directions to censor content.[21] This—together with the fact that most ISPs and large online media companies are close to the government—results in a lack of transparency and public accountability surrounding online content regulation.

Content Removal

Since the Class License system was introduced in 1996, it has been used once to ban a political site. In May 2015, the MDA declared that *The Real Singapore* (TRS) website had violated the Internet Code of Practice, and that its Class License was therefore suspended. The regulator said that several of its articles had "sought to incite anti-foreigner sentiments in Singapore." Some articles were "deliberately fabricated" and "falsely attributed." The site was taken down soon after.[22]

The information minister said that this was only the 27th intervention against online content since 1996. Previous cases apparently involved takedown notices for specific con ent, but these were not made public. However, in 2013, the minister informed parliament that most takedowns were for pornographic content or solicitation; others were related to gambling or drugs. He told parliament

17 Conditions of Class Licence, Section 2A (2), Broadcasting (Class Licence) Notification under the B oadcasting Act (Chapter 28) Section 9, last revised May 29, 2013, http://www.mda.gov.sg/RegulationsAndLicensing/Licences/Documents/Internet%20Services%20and%20Content%20Provider%20Class%20Licence/Class%20Licence%20%28Post%20ONLS%29.pdf.

18 "Internet," Media Development Authority Singapore, Regulations & Liscensing, accessed July 9, 2014, http://www.mda.gov.sg/RegulationsAndLicensing/ContentStandardsAndClassification/ ages/Internet.aspx.

19 "MCI's response to PQ on the Ashley Madison website," Ministry of Communications and Information Press Room, November 11, 2013, http://www.mci.gov.sg/content/mci_corp/web/mci/pressroom/categories/parliament_qanda/mci-s-response-to-pq-on-the-ashley-madison-website.html.

20 Terence Chong, "Christian Evangelicals and Public Morality in Singapore," *ISEAS Perspective* 17 (2014): 1-11, accessed July 9, 2014, http://www.iseas.edu.sg/documents/publication/ISEAS_Perspective_2014_17-Christian_Evangelicals_and_Public_Morality_in_Singapore.pdf.

21 Broadcasting Act (Chapter 28) Section 3(5).

22 Belmont Lay, "Media Development Authority statement on The Real Singapore," *Mothership,* May 3, 2015, http://mothership.sg/2015/05/media-development-authority-statement-on-the-real-singapore/. MDA statement: http://www.mda.gov.sg/AboutMDA/NewsReleasesSpeechesAndAnnouncements/Pages/NewsDetail.aspx?news=661.

that the MDA had never directed websites to take down content "just because it is critical of the Government."[23]

A separate notice-and-takedown framework exists for high-impact online news sites—those receiving visits from a monthly average of 50,000 unique IP addresses from Singapore. Introduced in June 2013, it removes the identified si es from the class license and subjects them to individual licensing, under which they are required to comply with any takedown notice within 24 hours. The sites are required to put up a "performance bond" of SGD 50,000 (US$35,600) as an incentive to exercise best efforts.[24] The bond is in line with the requirement for television niche broadcasters.[25]

Altogether, eleven news sites have been licensed under the new framework. The fi st ten to be covered included nine run by Singapore Press Holdings or MediaCorp—which, as newspaper and broadcasting companies, are already subject to discretionary individual licensing and traditionally cooperate with the government (see Media, Diversity and Content Manipulation). The only one on the original list not belonging to national mainstream media is Yahoo Singapore's news site. After it was licensed, Yahoo's reporters were granted the official acc editation that they had sought for several years.

One start-up was added within the coverage period. The independent site *Mothership* became the fi st individually licensed site not belonging to a major corporation.[26] Like the original ten news sites, it appears to have been targeted purely on the basis of having crossed the regulatory threshold of 50,000 visitors a month. Although it occasionally carries irreverent commentary, *Mothership* is considered moderate and not antiestablishment.

Another independent site, *The Middle Ground*, was ordered to take down an article reporting on a street poll of 50 voters ahead of a May 2016 by-election. The Parliamentary Elections Act prohibits the publication of election surveys during the official cam aign period. *The Middle Ground* said it was not convinced that its poll amounted to a survey, but it complied with the takedown order.[27]

Several bloggers have publicly acknowledged removing critical content under threat of criminal prosecution or defamation suits (see Prosecutions and Detentions for Online Activities), while others are widely believed to do the same behind the scenes.

Media, Diversity, and Content Manipulation

The online landscape is significantly mo e diverse than offline media. ouTube, Facebook, Twitter, and international blog-hosting services are freely available, and most bloggers operate openly. All

23 Chan Luo Er, "MDA was right to shut down The Real Singapore: Yaacob Ibrahim," Channel News Asia, August 22, 2015, http://www.channelnewsasia.com/news/singapore/mda-was-right-to-shut/1837480.html; "MCI's response to PQs on Licensing Framework for online news sites," Ministry of Communications and Information, July 8, 2013, http://www.mci.gov.sg/content/mci_corp/web/mci/pressroom/categories/parliament_qanda/mci_s_response_topqsonlicensingframeworkforonlinenewssites.html.

24 Broadcasting (Class Licence) Notification under the B oadcasting Act (Chapter 28) Section 9, revised May 29, 2013, G.N. No. S330/2013.

25 "Fact Sheet – Online news sites to be placed on a more consistent licensing framework as traditional news platforms," Media Development Authority Singapore, May 28, 2013, http://www.mda.gov.sg/AboutMDA/NewsReleasesSpeechesAndAnnouncements/Pages/NewsDetail.aspx?news=4.

26 "Mothership.sg to come under online news licensing framework," Channel News Asia, July 30, 2015, http://www.channelnewsasia.com/news/singapore/mothership-sg-asked-to/2017168.html.

27 "Our fi st take-down order from the MDA," *The Middle Ground,* May 6, 2016, http://themiddleground.sg/2016/05/06/fi st-take-order-mda/.

major opposition parties are active online. Several NGO sites contribute to debates within their respective spheres, such as TWC2 (promoting migrant worker rights) and Transitioning (opposing the PAP's immigration policies).[28] However, analysts observe a gradual "normalization" of online space, with the PAP's ideological dominance of the offline orld increasingly reflec ed online.[29]

The biggest online news players, in terms of resources and viewership, are the internet platforms of the mainstream newspaper and broadcast outlets of Singapore Press Holdings (SPH) and MediaCorp. MediaCorp is 80 percent government-owned, with SPH holding the remaining 20 percent. SPH is a listed company, but through the Newspaper and Printing Presses Act, the government can nominate individuals to its board of directors. Since the 1980s, every SPH chairman has been a former cabinet minister. The government is known to have a say in the appointment of chief executives and chief editors.[30] Their websites are subject to the notice-and-takedown framework, but the main avenue of control is the routine self-censorship that also afflicts their arent news organizations.

Most regulatory attention has focused on independent news and political commentary sites that are more impactful than individual blogs, but too small to come under the individual licensing framework (see Content Removal). These sites remain under the general class license framework but can be asked to register individually with the content regulator. During the coverage period, one more website, *The Middle Ground,* was made to register, joining two other prominent sites, *The Online Citizen* and *The Independent Singapore*.[31] The registration process does not involve a performance bond, but requires the provision of details about publishers, editors, and funding sources.

These registered political sites are also required to sign an undertaking not to receive funds from foreign sources other than subscription revenue and what the regulator deems bona fide comme - cial advertising. In effect, this shuts out grants and loans from foreign foundations, which have been essential for most independent political sites in the region. In March 2016, the MDA said The Opinion Collaborative—the fundraising arm of *The Online Citizen*—breached these funding rules in April 2015 by accepting SGD 5,000 in advertising revenue from Monsoons Book Club, a non-commercial British entity.[32] A Singaporean exile, Tan Wah Piow, is one of its directors.[33] The Opinion Collaborative said it would to contest the MDA order.[34]

Until 2011, anti-PAP voices dominated online spaces outside of the mainstream media's platforms. Since the 2011 general election, however, those spaces have come to approximate offline public opinion—moderate as well as pro-PAP content has grown much more prominent.[35] The proliferation of social media may have encouraged a previously silent mainstream to air their views more readily.

28 . Transient Workers Count Too, http://twc2.org.sg; Transitioning, http://www.transitioning.org.

29 Tan Tarn How, "The normalisation of the political cyberspace since the 2011 GE," *Today,* August 26, 2015, https://nus.edu/2eGv727.

30 Cherian George, *Freedom From The Press: Journalism and State Power in Singapore.* Singapore: National University of Singapore, 2012.

31 Wong Pei Ting, "MDA seeks registration of website The Middle Ground," *Today,* July 29, 2015, http://www.todayonline.com/singapore/mda-seeks-registration-website-middle-ground.

32 "The Opinion Collaborative Ltd ordered to return revenue to foreign advertiser," Channel News Asia, March 5, 2016, http://www.channelnewsasia.com/news/singapore/the-opinion-collaborative/2572626.html.

33 Martino Tan, "MDA asked TOC to return foreign money, so we asked (both of) them what happened," *Mothership,* March 4, 2016, http://mothership.sg/2016/03/mda-toc-foreign-funding/.

34 "The Opinion Collaborative intends to contest MDA's order," Channel News Asia, March 9, 2016, http://www.channelnewsasia.com/news/singapore/the-opinion-collaborative/2586894.html.

35 Tan Tarn How, Tng Ying Hui and Andrew Yeo, "Whispers, not shouts: A re-reading of the social media space," *Straits Times,* December 4, 2015, https://nus.edu/2fwli8k.

Individual ministers and government agencies have also ramped up and professionalized their social media capacity. Major government campaigns regularly and openly commission bloggers and creative professionals who are not ideologically opposed to such relationships.

In addition, mildly critical commercial startup sites catering to middle-of-the-road Singaporeans—*The Middle Ground* and *Mothership*—now match or better the audience of *The Online Citizen*, the leading online champion of democracy and human rights.[36] Sites occupying *The Online Citizen*'s niche in other countries have been able to rely on foreign foundation funding, which registered sites in Singapore are banned from receiving. *The Online Citizen* has struggled to remain viable, shedding all but one paid staff positions in early 2016.[37] The newer centrist websites are better able to attract investors and may be able to sustain themselves financiall .

Also contributing to the post-2011 pushback against online dissent are websites and Facebook pages attacking the opposition, including Fabrications About The PAP, Fabrications Led by Opposition Parties, FiveStarsAndAMoon, and Silent No More. Analysts have described "guerilla-type activism" emerging from these sites, with supporters responding quickly to anti-establishment comments online.[38]

There is no evidence of large scale deployment of cyber troops, or paid online commentators. However, in the 2015 general election, online rumors about an impending opposition landslide may have sufficiently spoo ed some swing voters to vote more conservatively.[39] The rumors were mainly in the form of bookies' odds, which gave detailed predictions of opposition victories in several constituencies. Several versions were circulated widely via WhatsApp within the nine-day campaign period.

Since election laws ban opinion polling, these supposed predictions were the only quantitative indicators of likely outcomes available to voters. Although their impact on voters may have been less than other factors, the case illustrates how political operatives might be able to manipulate voter sentiment in an environment where quality information is limited by regulatory constraints.

Digital Activism

The internet is regularly used for popular mobilization by groups across the political spectrum. The success of these efforts is constrained less by online regulation than by offline estrictions on fundraising and public assembly.

Online media were instrumental in shining a light on the January 2016 case of 14-year-old schoolboy Benjamin Lim who killed himself after being picked up from his school by police and questioned over complaints about his behavior.[40] Concerns were raised, including by the president of the Law

36 Tan Tarn How, Tng Ying Hui and Andrew Yeo, "Battle for Eyeballs: Online Media in the 2015 Election," September 11, 2015, http://www.ipscommons.sg/battle-for-eyeballs-online-media-in-the-2015-election/.

37 Walter Sim, "The Online Citizen now a one-man show," *Straits Times,* March 3, 2016, http://www.straitstimes.com/politics/the-online-citizen-now-a-one-man-show.

38 Tan Tarn How, "The normalisation of the political cyberspace since the 2011 GE;" Pearl Lee, "Supporters seek to amplify PAP voice online," *Straits Times*, September 20, 2015, http://www.straitstimes.com/politics/supporters-seek-to-amplify-pap-voice-online.

39 Jeanette Tan, "7 illuminating conclusions two political analysts made of the GE2015 results," *Mothership,* November 5, 2015, http://mothership.sg/2015/11/7-illuminating-conclusions-two-political-analysts-made-of-the-ge2015-results/.

40 Terry Xu, "Benjamin Lim's case would have died down if not for social media, says family," *The Online Citizen,* February 29, 2016, http://www.theonlinecitizen.com/2016/02/benjamin-lims-case-would-have-died-down-if-not-for-social-media-says-family/.

Society, about police procedures in dealing with minors. *The Online Citizen* published in full an open letter from Benjamin's father suggesting that the school and the police had treated the boy insensitively.

The case was discussed in Parliament, where Law and Home Affairs Minister K Shanmugam accused *The Online Citizen* of organizing "a planned, orchestrated campaign using falsehoods". He said the police had already promised a coroner's inquiry. "This is Singapore; there is no such thing as a cover-up," he added.[41] He also said that the government would reexamine the law to ensure that debates about incidents did not prejudice public hearings.

An online fundraising drive was launched by supporters of blogger Alex Au to help him meet the financial burden of being convicted for scandalizing the judiciary (see Prosecutions and Detentions for Online Activities). The campaign, carried out through the Generosity fundraising platform, exceeded its target of US$18,000.[42]

Violations of User Rights

The two years preceding the September 2015 general election saw a spike in government actions against online dissent, and many of those cases saw developments within the coverage period. While citizens remain free from major human rights abuses and enjoy high levels of personal security in Singapore, the government places a premium on order and stability at the expense of civil liberties and political opposition. The authorities are believed to exercise broad legal powers to obtain personal data for surveillance purposes in national security investigations.

Legal Environment

The republic's constitution enshrines freedom of expression, but also allows parliament wide leeway to impose limits on that freedom.[43] As the ruling party has consistently controlled more than 90 percent of seats in the legislature, laws passed tend to be short on checks and balances. The Newspaper and Printing Presses Act and the Broadcasting Act, which also covers the internet, grant sweeping powers to ministers, as well as significant scope for the administrati e branch to fill in the details through vaguely articulated subsidiary regulations, such as website licensing and registration rules (see Content Removal and Media, Diversity and Content Manipulation). Other laws that have been used against online communication, such as the Sedition Act and Political Donations Act, are open to broad interpretation by the authorities.

The Sedition Act, dating from colonial times, makes it an offense "to bring into hatred or contempt or to excite disaffection against the Government" or "to promote feelings of ill-will and hostility between different races or classes of the population of Singapore," among other things.[44] Punishments for fi st-time offenders could include a jail term of up to three years. Newer provisions in the penal code (Section 298) provide for jail terms of up to three years for offenders who act through any

41 "K Shanmugam slams 'falsehoods, politicisation' of Benjamin Lim case," Channel News Asia, March 1, 2016, http://www.channelnewsasia.com/news/singapore/k-shanmugam-slams/2561458.html.

42 "Fundraising for Yawningbread aka Alex Au's Case," via Generosity, https://www.generosity.com/fundraising/fundraising-for-yawningbread-aka-alex-au-s-case.

43 Constitution of the Republic of Singapore, Section 14.

44 Sedition Act (Chapter 290) Section 3.

medium with the "deliberate intention of wounding the religious or racial feelings of any person."[45] Singapore's fi st cases of imprisonment for online speech were under the Sedition Act in 2005, over postings insulting Muslims.[46] Police investigations into complaints of insult and offense appear to be a regular occurrence. In most known cases, police intervention at an early stage has been enough to elicit apologies that satisfy those who feel targeted by offending expression.

Defamation is criminalized in the penal code, but to date, no charges have been brought under this law to punish online speech.[47] Civil defamation law is fearsome enough. PAP leaders have been awarded damages in the range of SGD 100,000 to 300,000 each (US$71,000 to US$213,000) in defamation suits brought against opposition politicians and foreign media corporations.[48] Electronic media have been affected: In 2002, a libel suit was leveled at Bloomberg for an online column; it settled out of court and paid three leaders damages totaling SGD 595,000 (US$422,000). The offense of scandalizing the judiciary is another law that has been used to punish criticism of the court that in most democracies would be considered to fall within the norms of political debate. In 2008, a blogger was sentenced to three months in prison for this offense.[49]

A new Protection from Harassment Act came into force in 2014.[50] Under the law, a person who uses "threatening, abusive or insulting" expression likely to cause "harassment, alarm or distress" can be fined up o SGD 5,000 (US$3,500). Victims can also apply to the court for a protection order, which could include prohibiting continued publication of the offending communication. The government also inserted into the law a section providing civil remedies for "false statements of fact" published about a person. The affected party can seek a court order requiring that the publication of the falsehood cease unless a notice is inserted setting the record straight.

Although the Act was presented in parliament as a means of protecting ordinary citizens, it was quickly wielded by the government as a new instrument against critics: the Ministry of Defence applied for a court order against an article published in alternative news site *The Online Citizen*. Originally granted by a district court, the ministry's application was overturned by the High Court in December 2015. The court ruled that government departments could not be considered a "person" under the Act, and therefore could not apply for protection from harassment.[51] The Ministry of Defence is appealing against the decision.

Prosecutions and Detentions for Online Activities

A married couple behind *The Real Singapore* (see Content Removal) were imprisoned under the Sedition Act in 2016. The couple live in Australia but were arrested on a visit to Singapore. They

45 Penal Code (Chapter 224), Section 298.

46 Jaclyn Ling-Chien Neo, "Seditious in Singapore! Free speech and the offence of promoting ill-will and hostility between different racial groups," *Singapore Journal of Legal Studies* 2011: 351-372, http://law.nus.edu.sg/sjls/articles/SJLS-Dec11-351.pdf.

47 Penal Code (Chapter 224), Sections 499-500.

48 Michael Palmer, "Damages in Defamation: What is Considered and What is Awarded?" Law Gazette, May 2005, http://www.lawgazette.com.sg/2005-5/May05-feature3.htm.

49 Committee to Protect Journalists, "Blogger sentenced to three months in jail; newspaper faces possible contempt charge for criticizing judiciary," International Freedom of Expression Exchange, September 22, 2008, http://www.ifex.org/singapore/2008/09/22/blogger_sentenced_to_three_months/.

50 Protection From Harassment Act, http://statutes.agc.gov.sg/aol/download/0/0/pdf/binaryFile/pdfFile.pdf?CompId:5c68d19d-19ad-49d8-b1a9-5b8ca8a15459.

51 Selina Lum, "Government cannot invoke harassment Act to make website remove statements on Mindef: High Court," *Straits Times,* December 9, 2015, http://www.straitstimes.com/singapore/courts-crime/government-cannot-invoke-harassment-act-to-make-website-remove-statements-on.

were accused of using their site to exploit racial and xenophobic divisions in Singaporean society through posts attacking foreigners from the Philippines, India, and China. The prosecution said that the couple had invented sensational reports in order to attract readers and advertising revenue.[52] In March 2016, Australian national Ai Takagi was sentenced to ten months' imprisonment. Her husband, Singaporean Yang Kaiheng, received an eight-month sentence in June 2016, outside the coverage period of this report.[53]

In May 2016, a seventeen-year-old blogger, Amos Yee, was arrested on six counts of deliberately wounding religious feelings of Muslims and Christians under Section 298 of the penal code. It was the second time the teenager faced this criminal charge. In 2015, Yee served a four-week prison sentence. He had been found guilty of wounding Christians' feelings under Section 298 for an expletive-ridden video that likened the adulation of the late leader Lee Kuan Yew to Christians' worship of Jesus. He was also found guilty of obscenity under Section 292 of the penal code. Referencing a comment by the late British Prime Minister Margaret Thatcher that Lee was usually right, Yee had posted a manipulated image depicting the two politicians having sex. His appeal against these charges was dismissed by the High Court in October 2015.[54] Yee continued with his online commentary, including on religious themes. In court again near the end of this report's coverage period, the state prosecutor said Yee was "obviously escalating his offensive behavior in a bid to gain attention" and had "upped both the tempo and offensiveness of his posts."[55] He was released on bail, and his case was pending trial in mid-2016.

Other developments within the coverage period involved court decisions concerning earlier cases. In December 2015, the High Court ordered an activist blogger, Roy Ngerng, to pay damages of SGD 150,000 (US$106,000) to Prime Minister Lee Hsien Loong for a defamatory blogpost. The court had ruled in favor of Lee in November 2014. In January 2016, Ngerng was ordered to pay an additional SGD 29,000 (US$20,500) in costs.[56]

Bloggers have tended to retract offending posts and apologize when lawsuits are threatened. Ngerng's case was thus the first time an individual blogger was taken to court for defamation by a government leader. His blog, *The Heart Truths*, had regularly accused the government of providing citizens with inadequate returns from the Central Provident Fund (CPF), a national pension scheme built on compulsory contributions from employees and employers. Lee's lawyers said that one blog essentially claimed that the prime minister was guilty of criminal misappropriation of Singaporeans' money. They rejected Ngerng's initial apology and his offer of SGD 5,000 (US$3,500) in damages, pointing out that Ngerng emailed similar allegations to the media even after apologizing. Ngerng stood as a Reform Party candidate in the September 2015 general election.

Explaining how he set the damages in a 73-page decision, the Supreme Court judge noted that damages awarded to a prime minister for libel in the last 20 years have been much higher. However,

52 Elena Chong, "TRS ad revenue 'used to pay mortgage on couple's apartment'," *Straits Times,* March 29, 2016, http://www.straitstimes.com/singapore/courts-crime/trs-ad-revenue-used-to-pay-mortgage-on-couples-apartment.

53 Pearl Lee, "TRS co-founder Yang Kaiheng jailed 8 months for sedition," June 28, 2016, http://www.straitstimes.com/singapore/courts-crime/trs-co-founder-yang-kaiheng-jailed-8-months-for-sedition.

54 Global Freedom of Expression, Columbia University, "Public Prosecutor v. Amos Yee Pang Sang," https://globalfreedomofexpression.columbia.edu/cases/public-prosecutor-v-amos-yee-pang-sang/.

55 Lianne Chia, "Teenage blogger Amos Yee faces 8 new charges," Channel News Asia, May 26, 2016, http://www.channelnewsasia.com/news/singapore/teenage-blogger-amos-yee/2817976.html.

56 Walter Sim, "Blogger Roy Ngerng ordered to pay PM Lee Hsien Loong $150,000 for defamation," *Straits Times,* December 17, 2015, http://www.straitstimes.com/singapore/courts-crime/blogger-roy-ngerng-ordered-to-pay-pm-lee-hsien-loong-150000-for-defamation.

the influence and c edibility of the defamer had to be taken into account. A substantial reduction in damages was warranted because Ngerng did not have a significant standing among Singapo eans.[57]

In December 2015, the Court of Appeal upheld the conviction of blogger Alex Au, who had been fined SGD 8,000 (US$ 5,700) in April 2015 for scandalizing the judicia y. His offending 2013 blog had questioned the Supreme Court's handling of a constitutional challenge to Section 377A of the penal code, which criminalizes sodomy.[58]

Surveillance, Privacy, and Anonymity

Singapore has no constitutionally recognized right to privacy and law enforcement authorities have wide powers to conduct searches on computers without judicial authorization.[59] While many people try to communicate anonymously online in Singapore, their ability to conceal their identities from government is limited. Registration is required for some forms of digital interaction. Government-issued identity cards or passports must be produced when buying SIM cards, including prepaid cards, and buyers' details must be electronically recorded by vendors. Registration for the Wireless@SG public Wi-Fi network also requires ID.

Details about Singapore's surveillance capabilities and practices are unknown. However, according to the UK-based organization Privacy International, "it is widely acknowledged that Singapore has a well-established, centrally controlled technological surveillance system" including through internet monitoring. One analyst says that "few doubt that the state can get private data whenever it wants."[60] The government justifies its su veillance regime on security grounds. "Whether by compulsion or natural tendency, most Singaporeans appear to be relatively sympathetic to this rationale and do not protest the government's collection, monitoring, or even transfer abroad of data about them," says one recent study.[61]

Privacy International notes that law enforcement agencies are aided by sophisticated technological capabilities to monitor telephone and other digital communications. Surveillance is also facilitated by the fact that "the legal framework regulating interception of communication falls short of applicable international human rights standards, and judicial authorization is sidelined and democratic oversight inexistent".[62]

Under the sweeping Computer Misuse and Cybersecurity Act, the minister for home affairs can authorize the collection of information from any computer, including in real time, when satisfied that it is necessary to address any threat to national security.[63] Court permission need not be sought. Fail-

57 Global Freedom of Expression, Columbia University, "Lee Hsien Loong v. Roy Ngerng Yi Ling," https://globalfreedomofexpression.columbia.edu/cases/lee-hsien-loong-v-roy-ngerng-yi-ling/.

58 Selina Lum, "Blogger Alex Au loses appeal against conviction for contempt of court," *Straits Times,* December 1, 2015, http://www.straitstimes.com/singapore/courts-crime/blogger-alex-au-loses-appeal-against-conviction-for-contempt-of-court.

59 Privacy International, "The Right to Privacy in Singapore," Universal Periodic Review Stakeholder Report, 24th Session, June 2015, https://www.privacyinternational.org/sites/default/files/Singapo e_UPR_PI_submission_FINAL.pdf; M. Ravi, "At what cost of citizen's privacy, comes their freedom and security," *The Online Citizen*, May 12, 2016, http://www.theonlinecitizen.com/2016/05/at-what-cost-of-citizens-privacy-comes-their-freedom-and-security/.

60 Terence Lee, "Singapore an advanced surveillance state, but citizens don't mind," *Tech In Asia*, November 26, 2013, accessed July 10, 2014, http://www.techinasia.com/singapore-advanced-surveillance-state-citizens-mind/.

61 Columbia School of International and Public Affairs, "Singapore," in *Mapping Global Surveillance and Proposing Solutions to Respect Human Rights*, Spring 2015, https://pdfs.semanticscholar.org/36a9/5f793d87f54b23fb36a8bedf43a765860440.pdf.

62 Privacy International, "The Right to Privacy in Singapore."

63 Computer Misuse and Cybersecurity Act (Chapter 50A) Section 15A.

ure to comply with such orders is punishable with a fine f up to SGD 50,000 (US$35,000), a prison term of up to 10 years, or both.

Under the Criminal Procedure Code, police office s investigating arrestable offenses may at any time access and search the data of any computer they suspect has been used in connection with the offense.[64] No warrant or special authorization is needed. Penalties for non-compliance can include a fine f up to SGD 5,000 (US$3,500), six months in prison, or both. With authorization from the public prosecutor, police can also require individuals to hand over decryption codes, failing which they are liable to fines up o SGD 10,000 (US$7,000), jail terms up to three months, or both.

In mid-2016, police seized devices belonging to lawyer Teo Soh Lung from her home without a warrant after questioning her in relation to a Facebook post made prior to a May by-election. The police claimed Lung's post violated restrictions on political advertising in the Parliamentary Elections Act, which bars campaigning and election advertising from the day before polling.[65]

Website registration requirements, although imposed on only a small number of platforms, have raised concerns about unwarranted official intrusion in o their operations (see Media Diversity and Content Manipulation). In 2013, the owner of one site, the *Breakfast Network,* declined to register because the MDA required the names of anyone involved in the "provision, management and/or operation of the website," including volunteers.

Responding to a parliamentary question, the government said in October 2013 that, as part of the evidence gathering process, law enforcement agencies made around 600 information requests a year to Google, Facebook, and Microsoft between 2010 and 2012. Most were for Computer Misuse and Cybersecurity Act offenses, while the rest were for crimes such as corruption, terrorist threats, gambling, and vice. Although all requests were for metadata, agencies can request content data if required for investigating offenses, the government said.[66] The Personal Data Protection Act exempts public agencies and organizations acting on their behalf.[67]

From July 2015 to December 2015, Facebook reported receiving 214 requests for the details of 239 accounts from the Singapore government, and 198 requests for the data of 213 Facebook users. Facebook provided data in about three-quarters of cases.[68] From January to June 2015, Google received 1,408 requests to view 1,519 Google accounts.[69]

According to details leaked by former U.S. National Security Agency contractor Edward Snowden,

64 Criminal Procedure Code (Chapter 68) Section 39.

65 Terry Xu, "Teo Soh Lung visibly shaken from police raid involving 7-8 office s without search warrant," *The Online Citizen,* June 1, 2016, http://www.theonlinecitizen.com/2016/06/01/teo-soh-lung-visibly-shaken-from-police-house-raid-of-7-8-office s-without-search-warrant/.

66 "Singapore Government's Requests to Web Services Companies for User Data," Singapore Parliament Reports, October 21, 2013, http://bit.ly/1OZ07H7.

67 "Personal Data Protection Act Overview," Personal Data Protection Commission Singapore, last modified Februa y 28, 2014, http://www.pdpc.gov.sg/personal-data-protection-act/overview.

68 Facebook, "Singapore July 2015 to December 2015," in *Government Requests Report*, https://govtrequests.facebook.com/country/Singapore/2015-H2/.

69 Google Transparency Reports "Singapore, Requests for User Information," https://www.google.com/transparencyreport/userdatarequests/SG/.

SingTel has facilitated intelligence agencies' access to the traffic carried on the major unde sea telecommunications cable.[70]

Singapore has adopted a U.S. Defense Department concept, "Total Information Awareness," to gather electronic records en masse to look for digital footprints that might provide clues of impending security threats. The idea, which has proven controversial in the United States, has been incorporated into Singapore's Risk Assessment and Horizon Scanning program. According to one analyst, "Singapore has become a laboratory not only for testing how mass surveillance and big-data analysis might prevent terrorism, but for determining whether technology can be used to engineer a more harmonious society."[71]

Intimidation and Violence

There were no violent incidents targeting internet users in the past year. However the lack of protection for the expression of unpopular or dissenting views means that ICT users cannot be said to operate in an environment free of fear.

Technical Attacks

After several high-profile attacks on go ernment and private-sector websites in recent years, as well as growing concern about cybercrime, more attention is being paid to cyber-security. A Cyber Security Agency (CSA) was established in April 2015 to mitigate attacks and protect critical sectors such as energy, water, and banking. A new Cybersecurity Bill will be introduced in parliament in 2017 to give the CSA greater powers to manage incidents.[72] Cybersecurity expenditure will rise to at least 8 per cent of the government's IT budget.[73]

70 Phillip Dorling, "Australian spies in global deal to tap undersea cables," *Sydney Morning Herald Technology*, August 29, 2013, http://www.smh.com.au/technology/technology-news/australian-spies-in-global-deal-to-tap-undersea-cables-20130828-2sr58.html; *Malay Mail Online*, "Top-Secret expose: Singapore helping US spy on Malaysia," *Yahoo! News Singapore*, November 25, 2013, accessed July 9, 2014, https://sg.news.yahoo.com/top-secret-expos-singapore-helping-us-spy-malaysia-052600023.html.

71 Shane Harris, "The Social Laboratory," *Foreign Policy,* July 29, 2014, http://foreignpolicy.com/2014/07/29/the-social-laboratory/.

72 "Parliament: New Cybersecurity Bill to be tabled next year to strengthen Singapore's online defences," *Straits Times,* April 11, 2016, http://www.straitstimes.com/singapore/parliament-new-cybersecurity-bill-to-be-tabled-next-year-to-strengthen-spores-online.

73 "No one will be left behind in Smart Nation journey: MCI," Channel News Asia, January 21, 2016, http://www.channelnewsasia.com/news/singapore/no-one-will-be-left/2444684.html.

Freedom House

South Africa

	2015	2016
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	8	8
Limits on Content (0-35)	8	6
Violations of User Rights (0-40)	11	11
TOTAL* (0-100)	**27**	**25**

* 0=most free, 100=least free

Population:	**55 million**
Internet Penetration 2015 (ITU):	**52 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2016 Status:	**Partly Free**

Key Developments: June 2015 – May 2016

- Access to quality and relatively affordable internet in South Africa is growing, primarily among low income communities through government subsidized Wi-Fi projects across the country (see **Availability and Ease of Access**).
- Significan digital activism during the #FeesMustFall movement influence the government's decision in October 2015 to withdraw a proposal to increase tertiary education tuition fees (see **Digital Activism**).
- The Film and Publications Amendment Bill introduced in 2015 threatens to impose intermediary liability and a censorship regime on South Africa's online content, while new registration fees on video-streaming services may impede local content creation (see **Content Removal** and **Media, Diversity, and Content Manipulation**).
- The draft Cybercrimes and Cyber Security Bill has been criticized for its ambiguous language that threatens to infringe on freedom of expression, privacy rights, and access to information (see **Legal Environment**).

Introduction

South Africa's digital media environment is generally free and open. A culture of free expression exists online, and the online sphere remains diverse and vibrant. Access to the internet and related technologies is a core concern for government, civil society, and the private sector, which has led to collaborative efforts between public and private players to expand the information and communication technology (ICT) sector.

Digital activism was particularly notable during the coverage period, helping fuel the rise of the "Fees Must Fall" movement, the largest student movement since the Sharpeville massacre of 1960, in October 2015. Students took to social media to share information and organize massive protests against a proposed 10 to 12 percent increase in tuition fees for the 2016 academic year, using the hashtag #FeesMustFall. The movement ultimately influence President Zuma to withdraw the proposal on October 23, 2015, leaving tertiary school fees the same for the 2016 academic year. The protests and social media activism erupted anew in October 2016 when the government announced another proposal to raise tuition fees for the 2017 academic year.

While the South African government has not proactively restricted access to ICTs or internet content, increasing apprehension of the challenges and threats posed by ICT advancement has led several state actors, from the regulatory body to security agencies, to respond with policy and legislative proposals, some of which may impose restrictions on South Africa's internet freedom. For one, the Film and Publications Amendment Bill—drafted for the purpose of protecting children from racist, harmful, and violent content online—has been widely criticized for giving the government sweeping powers to censor content through an onerous classificatio system. The draft Cybercrimes and Cyber Security Bill has been criticized for its ambiguous language that threatens to infringe on freedom of expression, privacy rights, and access to information. Both bills were still under review as of October 2016.

In a worrisome development, South Africa voted against the UN Resolution for "the Promotion, Protection and Enjoyment of Human Rights on the Internet" in July 2016, siding with repressive countries including China, Russia, and Saudi Arabia, and based on concerns about the resolution's failure to consider hate speech.

Obstacles to Access

Access to quality and relatively affordable internet in South Africa is growing, primarily among low income communities through government subsidized Wi-Fi projects across the country. The majority of ICT infrastructure and services are privately-owned and enjoy a fair degree of self-regulatory independence, though a memorandum of understanding between the Independent Communications Authority of South Africa (ICASA) and the Film and Publications Board (FPB) may be the beginning of a new internet co-regulation regime.

Availability and Ease of Access

Internet penetration has expanded rapidly in South Africa, though many believe that the expansion has not kept up with the country's socioeconomic development. According to the latest data from the International Telecommunication Union (ITU), internet penetration reached 52 percent of the

South African population in 2015, up from 49 percent in 2014.[1] By contrast, mobile penetration reached 159 percent in 2015,[2] with 57 percent of internet users accessing the internet on their mobile devices.[3] Meanwhile, the country's average internet connection speed has improved from 3.2 Mbps in 2015 to 6.5 Mbps in 2016, above the global average of 6.3 Mbps, according to Akamai's first quarter "State of the Internet" report for 2016.[4]

In the General Household Survey 2015, the state's statistics agency reported that over 53 percent of South African households have at least one member who can access the internet at home, work, school, or internet cafes. The same survey found that nearly 10 percent of South African households are equipped with internet access at home, though home access is characterized by a significant urban-rural divide: 16 percent of households in metropolitan areas had home access, compared to approximately 1 percent in rural areas.[5] Another survey found that internet users were disproportionately white (50 percent), and speak either English (65.5 percent) or Afrikaans (39 percent).[6]

A monopoly in the fixed-line market remains a challenge to reducing overall fixed-line broadband costs, and there is a general perception that mobile operators overcharge to maximize profits. The passage of South Africa Connect—a new broadband policy that aims to connect the entire country by 2030—as well as a program providing tablets to schools suggest a positive trend in increasing internet access, especially for the poor. Several metropolitan areas including the cities of Tshwane, Johannesburg, and Cape Town, as well as the Ekurhuleni municipality[7] are piloting and expanding access to free public Wi-Fi infrastructure, providing users with access up to 500MB of data per day.[8] In October 2015, the city of Tshwane's Project Isizwe recorded 1 million unique users, a figure that is particularly significant given that the project services primarily low income areas within the city.[9]

Restrictions on Connectivity

The South African government does not have direct control over the country's internet backbone or its connection to the international internet. International internet connectivity is facilitated via five undersea cables—SAT-3, SAFE, WACS, EASSy, and SEACOM—all of which are owned and operated by a consortium of private companies.[10] Several operators oversee South Africa's national fiber networks, including partly state-owned Telkom and privately owned MTN, Vodacom, Neotel, and Fibre-Co, among others. Internet traffic between different networks is exchanged at internet exchange points (IXPs) located in Johannesburg, Cape Town, and Durban, which are operated by South Africa's nonprofit ISP Association (ISPA) and NapAfrica.[11]

In January 2016, the SEACOM cable experienced two interruptions caused by breakage of its under-

1 International Telecommunication Union, "*Percentage of Individuals Using the Internet*," 2000-2015, http://bit.ly/1cblxxY.

2 As a result of separate subscriptions for voice and data services and the use multiple SIM cards in order to make use of multiple product offerings, common among prepaid users. International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions," 2000-2014, http://bit.ly/1cblxxY.

3 'South Africa's big smartphone Internet uptake', *MyBroadband,* accessed 29 March, 2016, http://bit.ly/1Sj3fKQ

4 Akamai, "State of the Internet, Q1 2016 Report," https://goo.gl/TQH7L7.

5 Statistics South Africa, "General Household Survey, 2015," June 2016, http://www.statssa.gov.za/publications/P0318/P03182015.pdf

6 "South African Internet users: age, gender, and race," *MyBroadband*, September 19, 2014, http://bit.ly/XQtK5x.

7 'Free WiFi for Ekurhuleni', *ITWeb*, 10 November, 2016, accessed 29 March, 2016, http://bit.ly/1XZT5mH

8 'City of Tshwane doubles daily free WiFi data limit for residents', *HTXT.Africa*, 10 November, 2015, accessed 29 March, 2016, http://bit.ly/1ZI4eK8

9 'Tshwane free Wi-Fi hits one million device milestone', *TimesLIVE*, accessed 29 March, 2016, http://bit.ly/1XZT5mH

10 "This is what South Africa's Internet actually looks like," *MyBroadband,* March 9, 2014, http://bit.ly/1r5maRn.

11 Jan Vermeulen, "Here is who controls the Internet in South Africa," *MyBroadband*, July 17, 2014, http://bit.ly/1oQTm8p.

sea network, with users reporting slow international speeds due to congestion of traffi over redundant routes.[12]

ICT Market

There are hundreds of ISPs in South Africa, with ISPs belonging to the ISP Association (ISPA).[13] However, the fi ed-line connectivity market is dominated by Telkom,[14] a partly state-owned company of which the government has a 40 percent share and an additional 12 percent share through the state-owned Public Investment Corporation.[15] Telkom effectively possesses a monopoly, despite the introduction of a second national operator, Neotel, in 2006.[16] In the mobile market, there are fi e mobile phone companies—Vodacom, MTN, Cell-C, Virgin Mobile, and Telkom Mobile—all of which are privately owned except for Telkom Mobile, which falls under the partly state-owned Telkom.

Access providers and other internet-related groups are quite active in lobbying for better legislation and regulations. The ISPA was recognized as a self-regulatory body by the Department of Communications in 2009.[17]

In response to the rapid uptake of internet-based voice, messaging, and streaming (or over-the-top, OTT) services such as WhatsApp and Skype that have disrupted the traditional revenue streams of telecom companies, the Parliamentary Portfolio Committee on Telecommunications and Postal Services convened a meeting in February 2016 to discuss issues of governance and regulation of OTT services. Supporters of OTT regulation argue that such services profi at the expense of carriers that have invested in ICT infrastructure and must pay local taxes. Critics countered that any arbitrary limitations on services would stifl access to information and innovation that could potentially benefi the country. As of October 2016, the Portfolio Committee had not taken any formal position on OTT regulation.[18]

Regulatory Bodies

The autonomy of the regulatory body, the Independent Communications Authority of South Africa (ICASA), is protected by the South African constitution, although telecom observers contend that ICASA's independence has weakened as a result of various incidents over the past few years.[19] In May 2014, South Africa's ICT ministry was split into two departments—the Department of Communications (DoC) and the Department of Telecommunications and Postal Services (DTPS)— resulting in ICASA being engulfed by the DoC rather than the DTPS, which created confusion and concern that the government was seeking more control over the regulator.[20] Furthermore, ICASA lacks financia

12 South Africa internet hit by another Seacom outage. *Business Tech,* January 28 2016., http://bit.ly/25dD7d7

13 Internet Service Providers' Association, List of Members', accessed June 14 2015, http://ispa.org.za/membership/list-of-members/.

14 Quinton Bronkhorst, "SA's biggest ICT challenges," *BusinessTech*, December 26, 2013, http://bit.ly/1W2ySdR.

15 "Here is Government's shareholding in South African telecoms companies," *MyBroadband,* June 23, 2015, http://bit.ly/1MS4Vgf.

16 As reported in Freedom House 2013, Neotel has chosen to focus on providing wireless internet and telecom services, which has had minimal impact on last mile connectivity and the associated price of broadband.

17 Internet Service Providers Association, *See* http://ispa.org.za/about-ispa/

18 '*Regulation of OTT services'*, Portfolio Committee for Telecommunications and Postal Services, 16 March 2016, http://bit.ly/1RkuVT7

19 See: Freedom House, "South Africa," *Freedom on the Net 2012*, http://bit.ly/1LIYOOP; Open Society Initiative for Southern Africa, "South Africa," 2010, http://bit.ly/GzyPq8.

20 Martin Czernowalow, "Industry appalled at Zuma's ICASA edict," *ITWeb*, December 4, 2014, http://bit.ly/1LBbPCa.

control given its dependence on the Financial Treasury for funding and perennially cites poor resources as one of its primary challenges.[21]

The Film and Publications Board (FPB) traditionally regulates the distribution of films games, and other publications in South Africa but may soon regulate internet content under proposed amendments to the Film and Publications Act, 1996 (see "Content Removal"). In March 2016, the FPB signed a memorandum of understanding with ICASA to address regulatory overlaps created by the proposed amendments, which will effectively create co-jurisdiction over online content.[22]

Limits on Content

Commercial and user-generated content is not subject to arbitrary restrictions in South Africa, and the legal framework for takedown requests and intermediary liability are clearly articulated in law and established in practice. Nonetheless, the Film and Publications Amendment Bill introduced in 2015 threatens to impose intermediary liability and a censorship regime on South Africa's online content, while new registration fees on video streaming services may impede local content creation. In a positive step, significant digital activism during the #FeesMustFall movement influenced the government's decision to withdraw a proposal to increase tertiary education tuition fees.

Blocking and Filtering

Under the current legal and regulatory framework, neither the state nor other actors block or fil er internet and other ICT content, and there is no blocking or fil ering of content transmitted by mobile phones.

Content Removal

Between June 2015 and May 2016, there were no reported incidences of legal, administrative, or other means used to force the deletion of content from the internet in a way that contravenes international norms for free speech or access to information.

Section 77 of the Electronic Communications Act of 2002 (ECTA) requires ISPs to respond to takedown notices regarding illegal content such as child pornography, defamatory material, or copyright violations. Members of the ISPA—the industry representative body—are not held liable for third-party content that they do not create or select, though they can lose their protection from liability if they do not respond to takedown requests.[23] As a result, ISPs often err on the side of caution by taking down content upon receipt of a notice to avoid litigation, and there is no incentive for providers to defend the rights of the original content creator if they believe the takedown notice was

21 Bonnie Tubbs, "ICASA still fuzzy, one year on," *ITWe*b, May 27, 2015, http://bit.ly/1hQlegv; Siphiwe Hlongwane and Dumisani Moyo, "Regulatory Independence and the public interest," *Journal of African Media Studies* 1, no. 2 (2009) http://bit.ly/1GQSGtM; Bonnie Tubs, "ICASA's independence remains moot," *ITWeb*, July 8, 2015, http://bit.ly/1ZU4uXN.

22 'ICASA signs a Memorandum Of Understanding with the Film and Publication Board', Independent Communications Authority of South Africa, accessed 11 March 2016, http://bit.ly/1ZAg9tz

23 Section 73 of the Electronic Communications and Transactions Act of 2002 (ECTA) reaffi ms the limitation of service provider liability for information that is transmitted, stored or routed via a system under its control. *Electronic Communications and Transactions Act* of 2002, Government Gazette, Republic of South Africa , http://bit.ly/1pWWWGF

requested in bad faith. Meanwhile, any member of the public can submit a takedown notice, and there are no existing or proposed appeal mechanisms for content creators or providers.

User-generated content on news sites, social media platforms, and forums are regulated internally by content providers. There is no established best practice that has been adopted by South African content providers, and many are guided by internal policies that take into account the constitutional right to free expression and existing legislation, primarily the Promotion of Equality and Protection from Unfair Discrimination Act (PEPUDA). International platforms such as YouTube, Twitter and Facebook are guided by their respective policies. However, local private media platforms such as *Daily Maverick*, *Media24*, and the *Independent Online* are increasingly turning away from moderating comment sections and instead opting to close down public comments on selected sites and articles as a way to avoid dealing with hateful and harmful speech.[24]

In a worrisome development, the Film and Publications Amendment Bill introduced in 2015 threatens to impose intermediary liability and a censorship regime on South Africa's online content. The amendments are intended to give effect to the Online Regulation Policy proposed by the FPB in May 2016, which will in turn allow the FPB to pre-censor online content or take down existing content—including user-generated content—that fails to meet certain classificatio requirements.[25] Drafted for the purpose of protecting children from racist, harmful, and violent content online, the proposed policy has been widely criticized for giving the government "wide-sweeping powers to censor content on the internet."[26] Based on critical stakeholder feedback, the FPB released a revised Film and Publications Amendment Bill in October 2016, which is still up for discussion.[27]

Media, Diversity, and Content Manipulation

Online media in South Africa is vibrant, and online content represents a wide range of viewpoints and perspectives. Web-only news platforms, such as the *Daily Maverick*, have become particularly popular in recent years, with key news stories often broken online before print or broadcast, illustrating how online media is growing as a primary source of news in the country. In line with this development, recent anecdotal evidence suggests that the South African youth are increasingly reliant on the internet and radio for information and are less dependent on television and print news for current affairs.[28] Similarly, there are indications that in rural areas with internet access, the online versions of community newspapers are being accessed ahead of their print versions.[29] Nevertheless, while both English- and Afrikaans-language content is well represented online, 9 of South Africa's 11 officia languages are underrepresented, including on government websites.

New registration fees on video streaming services threaten to impede local content creation. In March 2016, the Film and Publications Board directed the video streaming service Netfli to pay a

24 Editorial: 'We tried. We really, really did', Daily Maverick, 11 January, 2016, http://bit.ly/1V0KL6K

25 Rebecca Kahn, "Scary new Internet censorship law for South Africa," *Huffington Post*, August 9, 2015, www.huffing onpost.com/rebecca-kahn/south-africa-might-get-th_b_8102720.html; "Scary new Internet censorship law for South Africa," *Mybroadband*, October 20, 2015, http://mybroadband.co.za/news/internet/142980-scary-new-internet-censorship-law-for-south-africa.html.

26 Paula Gilber, "Internet 'censorship' Bill may see changes," ITWeb, October 18, 2016, http://www.itweb.co.za/index.php?option=com_content&view=article&id=156791

27 The Film & Publications Board and online content regulation, Ellipsis Regulatory Solutions, http://www.ellipsis.co.za/the-film-publications-b_ard-and-online-content-regulation/

28 Suggested by Anton Harber, Professor of Journalism and Media Studies at the University of Witwatersrand.

29 Suggested in an access workshop held in East London in November 2013, run by Afesis-Corplan.

ZAR 795,000 (approximately USD 50,000) registration fee to distribute content under the self-classificatio criterion imposed on online distributors by the FPB.[30] The fee was criticized by industry stakeholders as unjustifiabl and prohibitive for smaller competitors providing content streaming services.[31]

Online self-censorship is low in South Africa, and the government does not actively try to limit or manipulate online discussions. Nevertheless, ANC-aligned businessmen have made significan inroads into the media landscape by acquiring or launching new media products over the past few years, leading to concerns over increasing progovernment bias among prominent media outlets.

Digital Activism

The internet has become a successful tool for online mobilization and democratic debate in South Africa, and the use of the internet and other ICTs for social mobilization has been mostly uninhibited by government restrictions.

In October 2015, the country witnessed the rise of the "Fees Must Fall" movement, the largest student movement since the Sharpeville massacre of 1960. The student movement began at the University of Witwatersrand in Johannesburg as a response to a proposed 10 to 12 percent increase in tuition fees for the 2016 academic year. Students took to social media—particularly Twitter—to share information and organize massive protests under the hashtag #FeesMustFall. As the hashtag trended on social media, the protests spread rapidly from the University of Witwatersrand to other universities and tertiary institutions across the country. The protests resulted in huge disruptions to the academic system, millions of Rand in damage to property, and at least one death,[32] but ultimately influence President Zuma to withdraw the proposal on October 23, leaving tertiary school fees the same for the 2016 academic year.[33]

The success of the #FeesMustFall protest movement proved short-lived upon the start of the 2017 academic year, when the government announced another proposal to raise tuition fees, this time by 8 percent.[34] Largescale protests erupted anew, once again facilitated by social media and the hashtag #FeesMustFall, and have been ongoing as of the time of writing in October 2016.[35]

Violations of User Rights

The draft Cybercrimes and Cyber Security Bill has been criticized by civil society for its ambiguous language that threatens to infringe on freedom of expression, privacy rights, and access to information. An unenforced ban on the hashtag #FeesMustFall may set a dangerous precedent that could restrict freedom of expression and digital activism in the future. Revelations of stingray "grabber" technology possessed by state security agencies led to increasing concerns over unchecked government surveillance.

30 Gareth van Zyl, ,EXCLUSIVE: FPB asks Netfli to pay R795k licensing fee, *FinTech24,* April 2016, http://bit.ly/1YUL2bz

31 Jan Vermeulen, Netfli – don't pay R795,000 to the FPB, *MyBroadband,* March 23, 2016, http://bit.ly/1XQcUPA

32 Coverage of Fees Must Fall movement since October 2015, http://ewn.co.za/Topic/Fees-must-fall

33 'South Africa: Jacob Zuma announces 0% university fee increase following Fees Must Fall protest', *International Business Times,* 23 October 2016, http://bit.ly/1ZIBmBu

34 "Why are South African students protesting?" BBC, October 4, 2016, http://www.bbc.com/news/world-africa-34615004

35 "Why are South African students protesting?" BBC, October 4, 2016

Legal Environment

The South African constitution provides for freedom of the press and other media, freedom of information, and freedom of expression, among other guarantees. It also includes constraints on "propaganda for war; incitement of imminent violence; or advocacy of hatred that is based on race, ethnicity, gender, or religion and that constitutes incitement to cause harm."[36] Libel is not a criminal offense, though civil laws can be applied to online content, and criminal law has been invoked on at least one occasion to prosecute against injurious material.[37] The judiciary in South Africa is generally regarded as independent.

In a worrisome development for internet freedom, South Africa voted against the UN Resolution for "the Promotion, Protection and Enjoyment of Human Rights on the Internet" in July 2016, siding with repressive countries such as China, Russia, and Saudi Arabia among the few objectors. In its opposition, South Africa's deputy permanent representative to the UN noted concerns that the resolution failed to take into account hate speech and incitement that pose unique challenges to freedom of expression in South Africa's post-apartheid society.[38]

Meanwhile, the draft Cybercrimes and Cyber Security Bill—published in August 2015 for public comment—has been criticized by civil society for its ambiguous language that threatens to infringe on freedom of expression. Section 17 of the draft bill criminalizes the "dissemination of [a] data message which advocates, promotes or incites hate, discrimination or violence," which could be broadly interpreted to include sharing such content on social media for the purposes of public discourse.[39]

The bill may also have far reaching implications on the right to access information and privacy. Critics have noted the bill's similarities to the controversial Protection of State Information Bill (POSIB), which was fie cely resisted by civil society and eventually vetoed in 2013 for placing harsh restrictions on the possession, distribution, or access of classifie state information, including online. Section 16 of the proposed cybercrime bill states, "Any person who unlawfully and intentionally–(i) possesses; (ii) communicates, delivers or makes available; or (iii) receives, data which is in the possession of the State and which is classifie as confidentia [by the State], is guilty of an offence," which observers worry will limit the ability of individuals, journalists, and society to hold those in authority to account.[40] As of October 2016, the bill is being redrafted by the Department of Justice with input from various stakeholders.[41]

Prosecutions and Detentions for Online Activities

Individuals were not prosecuted, detained, or sanctioned by law enforcement agencies for political, social, or religious speech online during the coverage period.

On October 19, 2015, the Western Cape High Court issued an interdict (a legal prohibition on an individual's actions) on several individuals and organizations, banning them from participating in the #FeesMustFall protest movement that was rocking the country, though none of the listed individuals

36 Constitution of the Republic of South Africa, Bill of Rights, Chapter 2, Section 16, May 8, 1996, http://bit.ly/1RUcGly.
37 See: Freedom House, "South Africa," *Freedom of the Net 2011*, http://bit.ly/1PEi9Oa.
38 http://www.fin24.com/ ech/News/why-sa-voted-against-internet-freedoms-at-the-un-20160705
39 http://www.justice.gov.za/legislation/invitations/cybercrimesbill2015.pdf
40 Freedom of Expression Institute, Submission on Cyber Crime and Cyber Security Bill (page 2-3), http://bit.ly/1VgycW6
41 Ellipsis Updates on Cybercrimes and Cybersecurity Bill, accessed October 26, 2016, http://bit.ly/1LXBs61

were arrested (see "Digital Activism"). In an unprecedented and bizarre move, the court interdict also included the hashtag #FeesMustFall, which meant that any use of the hashtag could lead to arrest.[42] While the interdict ultimately lacked enforcement and no social media users faced penalties for sharing the hashtag, the interdict set a dangerous precedent that could restrict freedom of expression and digital activism in the future.

Surveillance, Privacy, and Anonymity

Persistent concerns over government surveillance grew following reports that state security organizations possess stingray (or "grabber") technology that can mimic cell phone towers and capture cell phone metadata within a certain vicinity. In September 2015, Hlanwgani Mulaudzi, a spokesperson for the government investigation bureau known as the Hawks,[43] confi med that South African security official have access to grabber technology but noted that the technology was used specificall for national security matters only.[44] Nonetheless, consistent weaknesses in oversight mechanisms within the state security departments leave surveillance open to abuse. For example, the Offic of the Inspector-General of Intelligence has been vacant for over a year.[45]

According to Section 78 of the Electronic Communications and Transactions Act of 2002 (ECTA), service providers are not under any obligation to monitor data or actively seek circumstances indicating unlawful activity from data transmitted or stored on their information systems. The provision also recognizes the impracticality of generalized monitoring of user-generated content.

The Regulation of Interception of Communications and Provision of Communication-Related Information Act of 2002 (RICA) regulates the surveillance of domestic communications. Among its provisions, RICA requires ISPs to retain customer data for an undetermined period of time and bans any communications system that cannot be monitored, placing the onus and financia responsibility on service providers to ensure their systems have the capacity and technical requirements for interception.[46] While RICA requires a court order for the interception of domestic communications, the General Intelligence Laws Amendment Act (known locally as the "Spy Bill") passed in July 2013 enables security agencies to monitor and intercept foreign signals (electronic communications stemming from abroad) without any judicial oversight.[47]

RICA also compromises users' right to anonymous communication by requiring mobile subscribers to provide national identificatio numbers, copies of national identificatio documents, and proof of a physical address to service providers.[48] An identificatio number is legally required for any SIM card purchase, and registration requires proof of residence and an identity document.[49] For the many South Africans who live in informal settlements, this can be an obstacle to mobile phone usage. Meanwhile, users are not explicitly prohibited from using encryption, and internet cafes are not required to register users or monitor customer communications.

42 'High Court issues interdiction against a hashtag in #FEESMUSTFALL', *Htxt.Africa,* 20 October, 2015, http://bit.ly/1WUTaaS

43 The Hawks are South Africa's Directorate for Priority Crime Investigation (DPCI) which targets organized crime, economic crime, corruption, and other serious crime referred to it by the President or the South African Police Service

44 ITweb, 'Grabber used for 'national security", 8 September, 2015, http://bit.ly/1RDPadu

45 Times LIVE, 'ANC withdraws 'secretive' Cecil Burgess as spy inspector candidate' http://bit.ly/1WTVOOi

46 Section 30, Act No. 70, 2002, Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002, Government Gazette, 22 January 2003, http://bit.ly/1M5uQSD.

47 "Zuma passes 'spy bill,'" *News24*, July 25, 2013, http://bit.ly/1hQxVIf.

48 Chapter 7, "Duties of Telecommunication Service Provider and Customer," RICA, http://bit.ly/1W2EbKc.

49 Nicola Mawson, "'Major' RICA Threat Identified" *ITWeb*, May 27, 2010, http://bit.ly/16aWGqe.

Despite the legal framework for the interception of communications established under RICA, there have been worrying reports that the National Communications Centre (NCC)—the government body tasked with collecting intercepted signals—conducts surveillance without regard to RICA, thus extralegally. In June 2013, an investigative report by the *Mail & Guardian* revealed that the NCC monitors mobile phone conversations, SMS, and emails, "largely unregulated and free of oversight."[50] According to the *Mail & Guardian*, the NCC also has the technical capacity and staffin to monitor both SMS and voice traffi originating from outside South Africa. Calls from foreign countries to recipients in South Africa can ostensibly be monitored for certain keywords; the NCC then intercepts and records flagge conversations. While some interceptions involve reasonable national security concerns, such as terrorism or assassination plots, the system also allows the NCC to record South African citizens' conversations without a warrant and is subject to abuse without sufficien oversight mechanisms.[51]

The Protection of Personal Information (POPI) Act, signed into law in November 2013, provides measures to protect users' online security, privacy, and data. No law ensuring the constitutional right to privacy existed previous to POPI, which allows an individual to bring civil claims against those who contravene the act.[52] Penalties for contravening the law are stiff, including prison terms and fine of up to ZAR 10 million (approximately US$650,000). However, as of October 2016 the president has yet to appoint an Information Regulator and set a commencement date for the new legislation, after which point companies will have one year to begin compliance with the law.[53]

Intimidation and Violence

There were no cases of extralegal intimidation or violence reported against bloggers, journalists, or online users during the coverage period. However, at the beginning of 2016, Penny Sparrow, a realtor from Durban, was the subject of a social media storm after sharing a Facebook post wherein she described black beachgoers as monkeys.[54] After complaints were lodged at the Equality Court, Sparrow was ordered to pay a fin of ZAR 150,000 (approximately USD $10,000) to a local charity in June 2016 and as of October 2016 still faces charges of *Crimen Injuria* (offending the dignity of another).[55] The matter also drew attention to broader concerns on online harassment and personal privacy. Information on Penny Sparrow's personal contact details was posted on social media resulting in her receiving numerous undesirable messages and some even threatening her with imminent violence.[56]

Technical Attacks

South Africa is highly vulnerable to cybersecurity threats on many fronts, though independent news

50 Phillip de Wet, "Spy wars: South Africa is not innocent," *Mail & Guardian,* June 21, 2013, http://bit.ly/1jRPVD9.

51 Moshoeshoe Monare, "Every Call You Take, They'll Be Watching You," *Independent*, August 24, 2008, http://bit.ly/1RmaimM.

52 Lucien Pierce, "Protection of Personal Information Act: Are you compliant?" *Mail & Guardian*, December 2, 2013, http://bit.ly/1ZUn16t.

53 Update On the Protection of Personal Information Act (April 2016), accessed 30 October 2016, http://www.ellipsis.co.za/update-on-the-protection-of-personal-information-act/

54 Twitter erupts after KZN estate agent calls black people 'monkeys', *Mail & Guardian*, 4 January, 2016, accessed 29 March, 2016, http://bit.ly/1JozlH3

55 Penny Sparrow back in court. City Press, 12 September 2016, accessed 30 October 2016, http://www.news24.com/SouthAfrica/News/penny-sparrow-back-in-court-20160912-2

56 'Penny Sparrow: When racism backlash turns violent', *Mail & Guardian,* 6 January, 2016, accessed 29 March 2016, http://bit.ly/25uOdeL

outlets and opposition voices were not subject to targeted technical attacks during the coverage period. Government websites are often hacked.[57] Most of the hacks are perpetrated by amateur hackers with no apparent political motivations other than to advertise their skills, and consist of minor website defacements rather than incidents of data theft.

57 Through the use of a simple Google search trick, it is evident that a large number of websites have previously been "hacked" in some way or another. This can be emulated by googling the following: "hacked by" site:gov.za, or "hacked by" site:org.za. This will reveal the presence of the term "hacked by" in either governmental or NGO domains. The term is often used in the defacements. The search trick does not reveal up-to-date data, and many sites revealed have been fi ed since their indexing.

Freedom House

South Korea

	2015	2016
Internet Freedom Status	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	3	3
Limits on Content (0-35)	14	15
Violations of User Rights (0-40)	17	18
TOTAL* (0-100)	**34**	**36**

* 0=most free, 100=least free

Population:	**50.6 million**
Internet Penetration 2015 (ITU):	**90 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Partly Free**

Key Developments: June 2015 – May 2016

- An antiterrorism law passed in March 2016 grants the National Intelligence Service (NIS) powers to access private communication records and censor online content without judicial oversight during terrorism investigations (see **Surveillance, Privacy, and Anonymity**).
- In July 2015, leaked documents revealed that the NIS purchased spy tools from the Italian company Hacking Team ahead of the 2012 presidential election (see **Surveillance, Privacy, and Anonymity**).
- An amendment to the Newspaper Act, effective from November 2015, bars internet news agencies from fulfilling manda ory registration requirements if they employ fewer than fi e staff (see **Media, Diversity, and Content Manipulation**).
- Internet users continued to face prosecution for online activities; unlike many local residents, a Japanese journalist was acquitted of defaming President Park Geun-hye in December 2015 (see **Prosecutions and Detentions for Online Activities**).

Introduction

Internet freedom declined in 2015-16. The passage of an antiterrorism law with implications for privacy and free speech, and separate, tighter restrictions on news websites were among several issues of concern for internet freedom advocates.

Observers say that freedom of expression, both online and offline, has been unde mined since the conservative party returned to power in 2008. Three UN Special Rapporteurs shared concerns after visiting the country in 2010, 2013, and 2016, respectively, saying that the government's new laws, along with more restrictive interpretations and application of existing laws, affect citizens' rights to free speech, assembly, and association.[1]

During the coverage period of this report, Park Geun-hye of the conservative Saenuri Party entered the second half of her single, fi e-year presidential term. However, the investigation into the extent of online content manipulation by the National Intelligence Service (NIS), which was allegedly conducted to aid Park's victory in the 2012 election, was ongoing.[2] The NIS has been accused of political meddling and abuse of power, and concerns about their activities have extended to the digital realm. In 2016, news reports said NIS and other law enforcement agencies had repeatedly accessed telecommunications company data about labor rights activists and others without their knowledge, though they were not under investigation. Documents publicly leaked in July 2015 indicated that the NIS purchased spy tools from the Italian company Hacking Team for domestic surveillance purposes ahead of the 2012 election.[3] An antiterrorism law passed in March 2016 enables the agency to access personal communications and order the removal of online content without judicial oversight during terrorism investigations.[4]

Arrests and prosecutions continue to be documented on grounds of rumormongering and defamation, which South Korean law punishes more severely online than offline. tate prosecutors have sought heavy penalties in relation to online speech involving the sinking of Ferry Sewol in April 2014, a disaster that resulted in hundreds of deaths and widespread criticism of the Park administration's response. At least one person was also arrested for comments about an outbreak of the Middle East Respiratory Syndrome (MERS) in mid-2015.

1 Frank La Rue, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" (A/HRC/17/27/Add.2), 2011, http://bit.ly/1QgytnP; Margaret Sekaggya, "Report of the Special Rapporteur on the situation of human rights defenders" (A/HRC/25/55/Add.1), 2013, http://bit.ly/1oJBN1t; Maina Kiai, "Statement by the United Nations Special Rapporteur on the rights to freedom of peaceful assembly and of association at the conclusion of his visit to the Republic of Korea," 2016, http://bit.ly/1RfNJiy; see also Amnesty International, "Annual Report 2015/16 – South Korea," 2016, http://bit.ly/1DkoIB4.

2 Youngji Seo, "Controversy over the judges' favoritism towards Won Sei-hoon. Senior prosecutor leaves the courtroom in protest" (in Korean), *Hankyoreh*, November 1, 2015, http://bit.ly/1RD1JW1; for the case background information, see also Yoo Eun Lee, "South Korea's spy agency, military sent 24.2 million tweets to manipulate election," *Global Voices*, November 25, 2013, http://bit.ly/1jB00Sp; Chico Harlan, "In South Korea's latest controversies, spy agency takes a leading role," *The Washington Post*, July 6, 2013, http://wapo.st/1mO8QJQ; Aidan Foster-Carter, "Intelligence scandals, Seoul-style," *Asia Times*, November 12, 2013, http://bit.ly/1b0WGb4.

3 Bill Marczak & Sarah McKune, "What we know about the South Korea NIS's use of Hacking Team's RCS," *Citizen Lab*, August 9, 2015, http://bit.ly/1N5ctvi.

4 Steven Borowiec, "South Korean lawmakers try fi st filibus er since 1969 to block anti-terrorism bill," *Los Angeles Times*, February 24, 2016, http://lat.ms/1QpKNmV.

Obstacles to Access

South Korea boasts one of the world's highest broadband and smartphone penetration rates. The internet service sector is relatively diverse and open to competition, while the mobile market is subject to more state influence. Broadcasting and telecommunications activities are regulated by the Korea Communications Commission (KCC) and the content and ethical standards of such activities are monitored by the Korea Communications Standards Commission (KCSC). Both commissions are chaired by presidential appointees.

Availability and Ease of Access

South Korea is one of the most wired countries in the world, for both usage and connection speed.[5] Internet penetration was at 90 percent in 2015.[6] Counting access via mobile phone, television, and game consoles, an estimated 97 percent of households had access by 2012.[7]

Several factors have contributed to the country's high degree of connectivity. First, high-speed access is relatively affordable. Most residences have connections capable of reaching 100 Mbps for under KRW 30,000 (US$27) per month.[8] Second, the population is densely concentrated in urban areas. Roughly 70 percent of South Koreans live in cities dominated by high-rise apartment buildings that can easily be connected to fibe -optic cables.[9] Finally, the government has implemented a series of programs to expand internet access since the 1990s, including subsidies for low-income groups.[10]

Omnipresent and affordable cybercafes have also helped prevent a digital divide in South Korea. Known as *PC bang* ("computer rooms"), many offer broadband access for approximately US$1 per hour, and also serve as venues for social interaction and online gaming. There is no significant gap in access to information and communication technologies (ICTs) with respect to gender or income levels, although differences persist along generational and professional lines.[11]

Mobile phone penetration was at 118 percent in 2015—a sign that many users now have more than one device.[12] Moreover, the rate of smartphone ownership rose to 88 percent of the population by spring 2015, surpassing other advanced economies in global surveys.[13] Wi-Fi coverage has increased rapidly to accommodate smartphones and tablet computers. Free Wi-Fi is offered in over 2,000 public spaces across the country, including train stations, airports, libraries, health centers, and com-

5 Matthew Speiser, "The 10 countries with the world's fastest internet speeds," *Business Insider*, May 17, 2015, http://bit.ly/1Qppsqs.

6 International Telecommunication Union, "Percentage of individuals using the internet, 2000-2015," http://bit.ly/1cblxxY. A government index reported 81.6 percent penetration, excluding mobile access. http://bit.ly/1ESUBvJ.

7 South Korea has been on the top of the Organisation for Economic Co-operation and Development's (OECD) list of internet access rates in 34 member countries since 2000: OECD, "Households with access to the internet in selected OECD countries," *Key ICT Indicators*, July 2012, http://bit.ly/19Xqbzx.

8 John D. Sutter, "Why internet connections are fastest in South Korea," *CNN*, March 31, 2010, http://cnn.it/1mOyYUT; Edward Wyatt, "U.S. struggles to keep pace in delivering broadband service," *The New York Times*, December 29, 2013, http://nyti.ms/1cBCkJb.

9 J. C. Herz, "The bandwidth capital of the world," *Wired*, August 2002, http://wrd.cm/1f2ENfX.

10 Sutter, "Why internet connections are fastest in South Korea."

11 Ministry of Science, ICT and Future Planning, "The digital divide index, 2010-2014" (in Korean), *IT Statistics of Korea*, http://bit.ly/1e2FfNb.

12 International Telecommunication Union, "Mobile-cellular telephone subscriptions, 2000-2015," http://bit.ly/1cblxxY.

13 Jacob Poushter, "Smartphone ownership and internet usage continues to climb in emerging economies," *Pew Research Center*, February 22, 2016, http://pewrsr.ch/1RX3Iqq.

munity centers.[14] The Ministry of Science, ICT and Future Planning said it would extend this to 12,000 public hotspots by 2017.[15] Jeju, South Korea's biggest and most popular holiday island, will have 640 hotspots by the end of 2016, providing tourists with free and universal Wi-Fi access anywhere on the island.[16]

Restrictions on Connectivity

The country's internet backbone market is oligarchic, with Korea Telecom (KT) as the biggest provider. KT was founded in 1981 and remained state-owned until privatization in 2002. The network infrastructure is connected to the international internet predominantly from the southern cities of Busan and Keoje, through international submarine cables connecting to Japan and China. For national security reasons, police and the National Intelligence Service have oversight over the access points, but the government is not known to implement politically motivated restrictions on internet or mobile access.[17]

In January 2016, the independent investigative news site *Newstapa* and other media outlets reported that the Presidential Security Service routinely undertake blanket mobile phone jamming in the vicinity of the President's movements under a loose interpretation of the Presidential Security Act.[18]

ICT Market

The telecommunications sector in South Korea is relatively diverse and open to competition, with 94 internet service providers (ISPs) operating as of December 2015.[19] Nevertheless, it is dominated by three companies: Korea Telecom (41.5 percent), SK Telecom (25 percent), and LG Telecom (17 percent). The same fi ms also control the country's mobile service market, with 25 percent, 38 percent, and 23 percent market share, respectively.[20] All three companies are publicly traded, but they are part of the country's *chaebol*—large, family-controlled conglomerates connected to the political elite, often by marriage ties.[21] This has given rise to speculation that favoritism was at play in the privatization process and in the selection of bidders for mobile phone licenses.[22] Korea Mobile Internet (KMI), a consortium of mobile virtual network operators who rent capacity from the main players, made a sixth attempt to enter the market in 2014. The Ministry of Science, ICT and Future Planning rejected

14 Searchable at http://www.wifif ee.kr/en/service/map_search.jsp.

15 Ministry of Science, ICT and Future Planning, *Public Wi-Fi Free Service*, http://bit.ly/1EfmhKz; Inyoung Choi, "Significant expansion of free public Wi-Fi by 2017" (in Korean), *Yonhap News*, July 12, 2013, http://bit.ly/1GjEY5O.

16 Choong-il Choi, "Free Wi-Fi all around Jeju. Available regardless of carriers" (in Korean), *JTBC*, January 2, 2016, http://bit.ly/1oWUorr.

17 Interviews with ICT professionals, August 2015.

18 Eun-yong Lee, "'Mobile phone jamming' wherever the president visits. All phones must freeze" (in Korean), *Newstapa*, January 29, 2016, http://newstapa.org/31493.

19 Korea Internet & Security Agency, "ISP statistics" (in Korean), *Infrastructure Statistics*, http://bit.ly/1TPRXSz.

20 Ministry of Science, ICT and Future Planning, "Wire and wireless communication service subscribers, as of December 2015" (in Korean), *IT Statistics of Korea: Statistical Resources*, http://bit.ly/1RkOh6B.

21 Hyeok-cheol Kwon, "Is *Chojoongdong* one big family?" (in Korean), *Hankyoreh*, July 29, 2005, http://bit.ly/1lhqYQM.

22 Hyun-ah Kim, "KMI criticizes the selection criteria for the 4th mobile operator and issues an open inquiry" (in Korean), *e-Daily*, February 18, 2013, http://bit.ly/1fXe7y8.

their bid for a license for failing to meet financial equirements, which a KMI spokesman described as "excessively strict."[23]

Under the stated aim of easing the information asymmetry caused by the effective oligopoly of the mobile phone market, an act came into effect in October 2014 limiting service carriers' subsidies for consumers. However, it ended up hiking up the prices of mobile handsets and subscriptions, leading to a public furor, and is currently under reconsideration.[24]

Regulatory Bodies

The conservative Lee Myung-bak government, which was in power from February 2008 to February 2013, restructured the regulatory institutions overseeing the ICT sector. The Ministry of Information and Communication and the Korean Broadcasting Commission merged in February 2008 to create the Korea Communications Commission (KCC), tasked with overseeing both telecommunications and broadcasting to improve policy coherence between the two sectors.[25] The KCC consists of fi e commissioners, with the president appointing two (including the chairman) and the National Assembly choosing the remainder. The KCC struggled to earn credibility, as its fi st chairman, Choi See-joong, was a close associate of President Lee, causing some observers to view the restructuring as a government effort to tighten control over the media and ICT sectors.[26] Lee reappointed Choi as chairman in 2011, despite the objections of opposition lawmakers, who said that Choi's personnel choices politicized the agency and that his licensing decisions favored conservative-leaning media outlets. Choi resigned in 2012, and was later sentenced to two and a half years in prison and a fine f KRW 600 million (US$545,000) for influence peddling [27] Lee pardoned him at the end of his presidential term in January 2013.[28]

In 2013, President Park Geun-hye missed an opportunity to distance herself from this history of cronyism, naming her close aide and four-term lawmaker Lee Kyeong-jae to head the KCC.[29] She transferred the KCC's policy and strategy-related responsibilities to the new Ministry of Science, ICT and Future Planning. The KCC retains its regulatory remit and is currently led by a former judge, Choi Sung-joon.

The content of broadcasting and internet communications is qualitatively monitored by the Korea Communications Standards Commission (KCSC). Established in 2008, the KCSC is nominally an independent organization, but its nine members are appointed by the president and the National

23 Yoon-seung Kang, "Gov't nixes consortium's application for new mobile carrier license," *Yonhap News*, July 24, 2014, http://bit.ly/1uTA4aR;
Min-ki Kim, "Bidders for the position of the 4th mobile operator complain of high opening bid of $260 million" (in Korean), *Yonhap News*, January 20, 2014, http://bit.ly/1iy4Pf6.

24 Kwan-yul Cheon, "The birth of 'that law' that everybody hates" (in Korean), *SisaIN*, October 31, 2014, http://bit.ly/1Elq1vz.

25 Jong Sung Hwang & Sang-Hyun Park, "Republic of Korea," in *Digital Review of Asia Pacific 2009-2010,* eds. Shahid Akhtar and Patricia Arinto, (London: SAGE, 2009), 234-240.

26 Ji-nam Kang, "Who's who behind Lee Myung-bak: Choi See-joong the appointed chairman of the KCC" (in Korean), *Shindonga* 583, 2008, http://bit.ly/1aYiNCd.

27 Rahn Kim, "President's mentor gets prison term," *Korea Times*, September 14, 2012, http://bit.ly/1esLXak.

28 "South Korean president issues controversial pardons," *BBC News*, January 29, 2013, http://bbc.in/L3ce7o.

29 "Park appoints former veteran lawmaker as communications commission chief," *Yonhap News*, March 24, 2013, http://bit.ly/1gkauoV.

Assembly.[30] The current chair of the commission is Park Hyo-chong, a key figu e in the country's neo-conservative movement.

Limits on Content

Although South Korean cyberspace is vibrant and creative, there are a number of restrictions on the free circulation of information and opinions. Technical filtering and administrative deletion of content is particularly evident. Content that "praises or benefits" communist North Korea or that undermines the traditional social values of the country is blocked or deleted based on the recommendations of the Korea Communications Standards Commission. Systematic manipulation of online discussions is also being investigated. Won Sei-hoon, the former chief of the National Intelligence Service, was sentenced to three years in jail in February 2015 for directing an online smear campaign against the rival of the current president in the December 2012 election. The top court granted Won a retrial in July 2015.[31]

Blocking and Filtering

Censored content is classified by ca egories including gambling, illegitimate food and medicine, obscenity, violation of others' rights, and violation of other laws and regulations. The last category includes websites containing North Korean propaganda or promoting reunification, ased on Article 7 of the 1948 National Security Act, which bans content that "praises, promotes, and glorifies No th Korea."[32]

Censorship is predominantly carried out on the orders of the Korea Communications Standards Commission (KCSC). In 2008, its fi st year of operation, 4,731 websites or pages were blocked, and 6,442 deleted.[33] Its activities have steadily increased since then. In 2015, a total of 111,008 websites or pages were blocked and 27,650 deleted.[34]

A team of 20 to 30 monitoring office s flag possible ffenses, including threats to national security and public morals. The police and other authorities can refer matters to the KCSC, and individuals can also submit petitions. Commissioners meet every two weeks to deliberate over flagged cases, and then issue censorship orders to content hosts or service providers.[35] Noncompliant service providers face up to two years' imprisonment, or a fine f up to KRW 10 million (US$9,000), under the

30 Six members are nominated by the president and the party with a parliamentary majority, while three are nominated by the opposition.
Jeong-hwan Lee, "A private organization under the president? The KCSC's structural irony" (in Korean), *Media Today*, September 14, 2011, http://bit.ly/1aYr0GA.

31 Ju-min Park, "South Korea court orders retrial of ex-spy chief in vote-meddling case," *Reuters*, July 16, 2015, http://reut.rs/1pn7aiO.

32 OpenNet Initiative, "South Korea," August 6, 2012, http://bit.ly/19XA93S.

33 3,816 websites or pages were blocked for "encouraging gambling," 549 for "disturbing social order," and 366 for "obscenity;" 3,238 were deleted for "disturbing social order,"1,460 for "obscenity," 1,201 for "violating others' rights," 424 for "violence, cruelty, and hatred," and 119 for "encouraging gambling."

34 Among those blocked, 46,940 were for "encouraging gambling," 37,391 for "prostitution and obscenity," 18,027 for "illegitimate food and medicine," 4,932 for "violating other laws and regulations," and 3,718 for "violating others' rights." Among those deleted, 10,495 for "violating other laws and regulations," 8,106 for "prostitution and obscenity," 7,290 were for "illegitimate food and medicine," 1,661 for "violating others' rights, and 98 for "encouraging gambling." Statistics published quarterly by the Korea Communications Standards Commission at http://bit.ly/1iDTDgX (in Korean).

35 Author's interview with Park Kyung Sin, who served as a commissioner until his resignation in 2014, at the KCSC office, April 4, 2013.

Comprehensive Measures on Internet Information Protection issued by the KCC in 2008.[36] Observers criticize the KCSC's vaguely defined standa ds and wide discretionary power to determine what information should be censored, allowing the small number of commissioners to make politically, socially, and culturally biased judgments, often lacking legal grounds.[37]

Moreover, in many cases, the commission blocks entire sites even though only a small portion of posts are considered to be problematic. In March 2015, for example, the commission blocked the entire platform of an adult cartoon service, saying that part of its content was obscene. However, the service provider argued that the content was provided through an age-authentication system in compliance with the law. Faced with a public furor, the commission withdrew the shutdown order after only two days.[38] In May 2016, U.K. journalist Martyn Williams said he would legally dispute the KCSC's blocking of his website *North Korea Tech*, a media outlet that reports on technology in North Korea.[39]

Content Removal

Political and social content is subject to removal by private companies based on instructions from the KCSC and complaints from individuals, other government agencies, and the police. Individuals may also be requested to remove content. Since domestic companies do not publicize the amount or nature of items subject to removal, the impact on legitimate content is hard to gauge, but during the coverage period at least one candidate for parliamentary elections used takedown requests to delete online references to a compromising news story, indicating the scope for abuse.

The legal grounds for takedown requests was strengthened during the coverage period, when the National Assembly passed an antiterrorism law in March 2016, granting NIS agents the power to order the removal of any online content during terrorism investigations (See, Surveillance, Privacy, and Anonymity). The KCSC separately amended its regulations in December 2015 to receive takedown requests initiated by third parties—meaning other than the victims of the alleged violation—based on perceived defamation, despite opposition from civil society groups.[40]

On receiving a takedown request, the company must hide the content in question for 30 days.[41] The content is deleted if its owner does not revise it or appeal within that time. "Hundreds of thousands of online posts get deleted every year by such temporary removal requests, which in effect remove the posts permanently," according to the Associated Press.[42] Users and service providers were requested to delete 22,928 items on national security grounds between January 2013 and August

36 Ha-won Jung, "Internet to be stripped of anonymity," *Korea JoongAng Daily*, July 23, 2008, http://bit.ly/1eOpT9A.

37 Jillian York & Rainey Reitman, "In South Korea, the only thing worse than online censorship is secret online censorship," *Electronic Frontier Foundation*, September 6, 2011, http://bit.ly/1gkiKFw.

38 Sung-won Yoon, "Watchdog hit for excessive digital censorship," *Korea Times*, March 30, 2015, http://bit.ly/1IWCXcu.

39 Martyn Williams, "Lawsuit planned over South Korea's blocking of North Korea Tech website," *North Korea Tech*, May 11, 2016, http://bit.ly/28OGj84.

40 Young-joo Choi, "KCSC passes an amendment to its regulations on defamation" (in Korean), *PD Journal*, December 10, 2015, http://bit.ly/1Rlsmwd.

41 Kyung Sin Park, *Guilty of Spreading Truth* (in Korean), (Seoul: Dasan Books, 2012), 125-130.

42 Associated Press, "Online curbs limit South Korea pre-election speech freedoms," April 11, 2016, http://apne.ws/2cV37sl.

2014.[43] From 2010 to 2014, over 1.4 million posts on web portals were hidden based on takedown requests. There were around 454,000 such cases in 2014, up from 145,000 in 2010.[44]

Companies are also known to proactively delete content they judge to potentially violate the law to avoid legal liability, even without a complaint. Under Article 44(3) of the Information and Communications Network Act, intermediaries are encouraged to monitor and carry out proactive 30-day takedowns of irregular content.[45] Companies who can demonstrate proactive efforts to regulate content would be favorably considered by the courts, while those who do not are potentially liable for defamatory or malicious content posted on their platforms by users.[46] This potential liability encourages compliance with takedown requests even if they have no legal basis. In 2016, the KCSC also asked the web portal Naver to exercise "voluntary restraint" after it posted links to a video drama depicting homosexual themes.[47]

In the lead up to the April 2016 parliamentary election, one blogger told the Associated Press that Kakao deleted as many as two of his posts every day to comply with rules about political information online.[48] Although a ban on posting election-related commentary in the days before the polls was lifted after it was declared unconstitutional in 2011, content about candidates is still monitored by the National Election Commission, which has a remit to correct information published about candidates in news stories, online, and offline [49] In one case during the reporting period, the National Election Commission ordered companies to delete at least 600 online posts that referenced a news story alleging that conservative candidate Na Kyung-won's daughter had received special treatment during a college admissions program for disabled students in 2012. Na's campaign had complained to the election commission about a factual error in the story which was unrelated to the allegations.[50] The commission subsequently warned *Newstapa* for breaching Article 8 of the Public Official Election Act ("responsibilities of the press for fair reports")[51] Na separately filed a criminal lawsuit against the journalist responsible for the report in March 2016.[52]

In 2011, the KCSC expanded their remit to social media, mobile applications, and podcasts, creating a team to systematically monitor platforms such as Twitter and Facebook for illegal content. [53] The KCSC fi st warns users to voluntarily delete posts containing false or harmful information. In 2012, a former commissioner said social media cases amounted to roughly fi e percent of the total consid-

43 Chang, "66 years on, the National Security Act evolves into something for cyberland."

44 Jiyong Choi, "Portals screen 450,000 posts from view in 2014 – a threefold increase since 2010" (in Korean), *OhmyNews*, September 10, 2015, http://bit.ly/1Qq8qIP.

45 Yoo Eun Lee, "Is South Korea encouraging portal sites to self-censor?" *Global Voices*, November 23, 2013, http://bit.ly/1ff3EhD.

46 Hyeon-seok Kang, "Portal sites that neglected malicious comments liable for defamation" (in Korean), *Nocut News*, April 16, 2009, http://bit.ly/1kTPiqI.

47 Dong-hwan Ko, "Lesbian romance in Internet drama slammed," *The Korea Times*, March 28, 2016, http://bit.ly/1URtSMQ.

48 Associated Press, "Online curbs limit South Korea pre-election speech freedoms," April 11, 2016, http://apne.ws/2cV37sl.

49 People's Solidarity for Participatory Democracy, "Online campaigning permitted? The NEC's crackdown continues" (in Korean), *OhmyNews*, October 6, 2016, http://bit.ly/2dIPA6Z.

50 Associated Press, "Online curbs limit South Korea pre-election speech freedoms."

51 Kyunghyang Shinmun, "NEC warns Newstapa for reporting the illicit admission of Na Kyung-won's daughter" (in Korean), *Kyunghyang Shinmun*, April 2, 2016, http://bit.ly/28KONfp.

52 Hyeon-cheol Park, "Na Kyung-won files a lawsuit against Newsta a for the allegation of 'illicit admission' of her daughter" (in Korean), *Hankyoreh*, March 18, 2016, http://bit.ly/28Lx2Q0.

53 Matt Brian, "South Korea may begin censoring social networking, mobile apps from next week," *The Next Web*, December 1, 2011, http://tnw.co/1hFQkCf.

ered by the KCSC.[54] South Korean officials sent 129 con ent removal requests to Twitter in 2015, out of a worldwide total of 5,631, although the company did not comply with them.[55]

Until recently, a major cause for concern was that authors of blocked or deleted content were never notified f the KCSC's decision, though ISPs are legally required to notify authors that their content has been taken down. Affected users are allowed to challenge the commission's ruling in principle, but with no independent avenue for appeal available, only 0.07 percent of cases involving censorship have resulted in appeal. A legal amendment to Article 25(2) to the Act of the Establishment and Operation of the Korea Communications Commission was passed on December 29, 2014, to mandate notifying owners of censored content before and after deletion.[56]

A copyright law that restricts file sharing was assed in 2009. Often referred to as the "three strikes rule," it allows the Minister of Culture, Sports and Tourism, acting through the Korea Copyright Commission, to shut down an entire forum for failure to comply with a third warning to take down pirated content. Internet companies and civil liberties advocates say the law threatens fair use and free expression.[57] In 2013, a controversy arose when the commission and the KCSC blocked U.S.-based music-streaming site Grooveshark, among other overseas torrent sites.[58] Online freedom activists and some users of the site submitted an administrative litigation against the order in February 2014, but the case was dismissed in 2015.[59]

Media, Diversity, and Content Manipulation

South Korea's overall media environment is partly restricted.[60] In 2012, journalists launched a series of strikes against government interference and censorship for the fi st time since the country's transition to democratic rule in 1987.[61] In consequence, a variety of alternative and activist media outlets developed online, including *Newstapa*, a user-funded investigative journalism platform. It has accumulated more than 35,000 regular donors since its January 2012 launch, and its YouTube channel had been viewed more than 34 million times by early 2016.[62] It became a leading source of information on the electoral manipulation scandal in 2013,[63] and one of the fi st to allege systemic corruption and negligence behind the sinking of Ferry Sewol in 2014. In 2013, the KCC called the work of *Newstapa* and a handful of other independent news websites "pseudo journalism," warning their owners not to report on issues outside their remit.[64]

54 Interview with Kyung Sin Park; Ji-hyun Cho, "Criticism escalates over SNS censorship," *The Korea Herald*, January 29, 2012, http://bit.ly/1jC5NHk.

55 Twitter Transparency Report: Removal Requests, http://bit.ly/1mRNH87.

56 Open Net Korea, "The KCSC now mandated to notify affected content owners before and after censorship orders" (in Korean), January 7, 2015, http://opennet.or.kr/7974.

57 Cory Doctorow, "South Korea lives in the future (of brutal copyright enforcement)," *Boing Boing*, March 30, 2013, http://bit.ly/1fxo4jZ; "International human rights organizations in support for the abolition of the three-strike rule" (in Korean), *Open Net Korea*, April 1, 2013, http://opennet.or.kr/1529.

58 Minoci, "How 'Grooveshark' got blocked: Interview with the KCSC's Rights Violation Monitoring Team" (in Korean), *Slow News*, November 7, 2013, http://slownews.kr/15204.

59 Open Net Korea, "Submission of an administrative litigation against the shutdown of Grooveshark" (in Korean), February 3, 2014, http://opennet.or.kr/5695.

60 Freedom House, "South Korea," *Freedom of the Press,* 2015, http://bit.ly/22ZrciQ.

61 "No news is bad news: Reporters complain of being muzzled," *The Economist*, March 3, 2012, http://econ.st/1mPL1kL.

62 Newstapa's YouTube page, accessed March 2016, http://www.youtube.com/user/newstapa.

63 Newstapa, "South Korea spy agency's illegal campaigning on SNS" (in Korean), YouTube video, 15:34, January 6, 2014, http://bit.ly/1gVTjap; Yoo Eun Lee, "South Korean authorities discredit dissenting voices as 'not-real' news," *Global Voices,* January 2, 2014, http://bit.ly/1cpE2sy.

64 Yoo Eun Lee, "South Korean authorities discredit dissenting voices."

During the coverage period, legal measures introduced new obstacles for journalists seeking to operate in the digital media market. In November 2015, an amendment to the Newspaper Act stipulated that an online news agency must have more than fi e regular employees to be eligible to register, as part of a crackdown on "substandard" internet media.[65] The Korea Press Foundation estimated that this could cause at least one third of existing agencies to close down, including most citizen journalism sites; they were given until November 2016 to come into compliance.[66] All news organizations are required to register, and failure to do so is subject to up to one year of imprisonment or fines up o KRW 20 million (US$17,200), according to the Act. The constitutionality of the amendment was being challenged in the Constitutional Court in mid-2016.

The diversity of online content was negatively affected in the two weeks before the April 2016 parliamentary election when some media outlets closed their comment functions to comply with the Public Official Election Act, which ans anonymous online communication for 13 days before the polls (see Surveillance, Privacy, and Anonymity).[67]

Trials stemming from a scandal involving politicized manipulation of online comments by intelligence agents saw further developments in 2016. In December 2012, opposition lawmakers accused a National Intelligence Service (NIS) agent of manipulating 40 different online accounts to discredit opponents of then-presidential candidate Park Geun-hye. Police initially cleared the agent,[68] but in 2013, prosecutors indicted former NIS director Won Sei-hoon on charge of authorizing agents to post thousands of online comments and 1.2 million tweets characterizing members of the political opposition as sympathizers of North Korea.[69] Park Geun-hye denies ordering or benefiting f om digital manipulation.[70] Won and his successor, Nam Jae-joon, admitted having refuted North Korean propaganda in online forums, but denied political motives.[71] In December 2013, the Defense Ministry's cyber command unit, launched in 2010 to "combat psychological warfare in cyberspace," announced that some officials had pos ed inappropriate political content online during the same period, but without the knowledge of the unit heads. Like Won Sei-hoon, they denied the more serious charge of election meddling.[72]

In September 2014, the Seoul Central District Court gave Won a suspended sentence under a law that bars intelligence officials f om political activity, but acquitted him of trying to sway the elec-

65 Yonhap News, "Editorial from Korea Herald on Nov 21," *Yonhap News*, November 21, 2015, http://bit.ly/2dNJH8j.

66 Sang-geun Jeong, "Exclusive: Internet news agencies with less than 5 employees to be ousted" (in Korean), *Media Today*, November 3, 2015, http://bit.ly/1L6rAXg.

67 Associated Press, "Online curbs limit South Korea pre-election speech freedoms," April 11, 2016, http://apne.ws/2cV37sl.

68 In-ha Ryu, "Breaking news: Seoul Police already plots a scenario before releasing the interim report of investigation into the online comments scandal" (in Korean), *Kyunghyang Shinmun*, September 6, 2013, http://bit.ly/1aWCZkN; "Seoul Police warns Kwon Eun-hee, who claims the police investigation into NIS was 'downscaled and covered up'" (in Korean), *Chosun Ilbo*, September 26, 2013, http://bit.ly/1v85Yjn.

69 Harlan, "In South Korea's latest controversies, spy agency takes a leading role;" Dong-hyun Lee, "Won Sei-hoon ordered operations against opposition candidates in every election, says prosecution" (in Korean), *Joongang Ilbo*, June 6, 2013, http://bit.ly/1aYLChK; Sang-Hun Choe, "South Korean officials accused f political meddling," December 19, 2013, http://nyti.ms/1ohP89w.

70 Sang-Hun Choe, "Prosecutors detail attempt to sway South Korean election," *The New York Times*, November 21, 2013, http://nyti.ms/1hvtiyf; Lee, "South Korea's spy agency, military sent 24.2 million tweets to manipulate election;" Harry Fawcett, "South Korea's political cyber war," *Al Jazeera*, December 19, 2013, http://bit.ly/1cmfW86.

71 Ho-jin Song et al., "Nam Jae-joon says online posting is the NIS's legit work, insisting the allegation of election interference be a political set-up" (in Korean), *Hankyoreh*, August 5, 2013, http://bit.ly/1aDobNp.

72 Choe, "South Korean officials accused f political meddling; "Former chiefs of S. Korean cyber command charged with political intervention," *Shanghai Daily*, August 19, 2014, http://bit.ly/1v5n6pZ.

tion.[73] Both sides appealed. Despite the lower court's ruling, Won was sentenced in February 2015 to three years in jail for smearing political candidates,[74] but the Supreme Court granted him a retrial in July 2015.[75] In January 2015, the Supreme Court cleared the former chief of Seoul police, Kim Yong-pan, of covering up an investigation into the scandal.[76]

In the meantime, a sitting judge who had denounced Won's initial acquittal on an intranet was suspended for two months in December 2014.[77] State prosecutors involved in the investigation were also subjected to career setbacks. Chae Dong-wook resigned in September 2013, six months into his appointment as Prosecutor General in charge of the case, amid rumors of marital misconduct and political pressure. In January 2016, the Seoul High Court fined an NIS agent for illegally gathering personal information about Chae's eight-year-old extramarital son and leaking it to conservative news outlets as part of a smear campaign.[78] Other state prosecutors leading the case, Yoon Seok-yeol and Park Hyung-cheol, were subjected to a one-month suspension and a one-month salary reduction, respectively, for not following internal procedures. During the investigation for disciplinary action, Yoon testified that he was p essured not to "aid the opposition" while pursuing the investigation. They were later reassigned to non-investigative positions,[79] and Park resigned in January 2016.

In November 2015, an NIS field agent was arraigned o face charges for malicious comments allegedly made as part of the intelligence-orchestrated manipulation campaign. Prosecutors had identified the agent as the individual behind a no orious ID ("Hanging Commies") active in left-leaning online forums. A victim of his abusive posts pressed charges against him in October 2013.[80]

Digital Activism

South Koreans have embraced online technology for civic engagement and political mobilization. During the coverage period, an online community called Megalia used satire to draw attention to gender-based discrimination and violence and campaigned against a pornography platform known for hosting hidden camera footage taken without the subject's consent, causing it to be shut down.[81] The community also raised money to litigate against Facebook, which it accused of taking down their content, and to support victims of sexual assault.[82]

73 Sang-Hun Choe, "Former South Korean spy chief convicted in online campaign against liberals," *The New York Times*, September 11, 2014, http://nyti.ms/1qCE6xW.

74 "South Korea spy chief sentenced to three years in prison," *BBC News*, February 9, 2015, http://bbc.in/1dibHgP.

75 Park, "South Korea court orders retrial of ex-spy chief in vote-meddling case."

76 Rahn Kim, "Former Seoul police chief cleared of election law violation," *The Korea Times*, January 29, 2015, http://bit.ly/1yQwWx6.

77 "Sitting judge slams court ruling on ex-spy chief," *Global Post*, September 12, 2014, http://bit.ly/1BakDtA; Sohee, Park, "Criticizing Won Sei-hoon ruling, Judge Kim Dong-jin suspended for two months" (in Korean), *OhmyNews*, 3 December 2014, http://bit.ly/1dic3UC.

78 "Ex-presidential official fined for leaking info on ex op prosecutor's extramarital son," *Yonhap News*, January 7, 2016, http://bit.ly/1oZHkSb.

79 Won-il Cho, "Be in the good book or else. Independence of the state prosecution still a distant dream" (in Korean), *Hankook Ilbo*, January 16, 2016, http://bit.ly/1QMre4f.

80 In-ha Ryu, "Vicious comments on 12-year-old daughter by Jwaikhyosu: Victim of online comments files lawsuit against NIS agents," *Kyunghyang Shinmum*, October 22, 2013, http://bit.ly/1pqSfEd.

81 Hannah Cho, "Sora.net: When online conspiracies become a reality," *Columbia Journal of Transnational Law*, February 15, 2016, http://bit.ly/1QhMwX2; Bo-eun Kim, "Police shut down nation's largest porn site server," *The Korea Times*, April 7, 2016, http://bit.ly/28MBUSU.

82 The fundraising took place at https://tumblbug.com/mersgall4.

Violations of User Rights

South Koreans faced increasing challenges to online privacy during the coverage period. A new antiterrorism law granted the National Intelligence Service (NIS) powers to collect personal data and monitor individuals' online activity without judicial oversight. Publicly leaked materials in July 2015 also revealed that the NIS purchased spy tools from the Italian company Hacking Team ahead of the December 2012 presidential election for domestic surveillance purposes. Cases involving surveillance or arrest were ongoing in the aftermath of the 2014 Sewol ferry accident. A Japanese journalist was indicted for defaming President Park Geun-hye in 2014. Unlike many local residents, however, he was acquitted in December 2015.

Legal Environment

The South Korean constitution guarantees freedom of speech, the press, assembly, and association to all citizens, but it also enables restrictions, stating that "neither speech nor the press may violate the honor or rights of other persons nor undermine public morale or social ethics." South Korea has an independent judiciary and a national human rights commission that have made decisions upholding freedom of expression. Nonetheless, the prosecution of individuals for online activities has a chilling effect, generating international criticism (see Prosecutions and Detentions for Online Activities).

Several laws restrict freedom of expression in traditional media as well as online. The 1948 National Security Act allows prison sentences of up to seven years for praising or expressing sympathy with the North Korean regime. In 2010, the Ministry of Unification issued a notice reminding citizens that the 1990 Act on Exchanges and Collaboration between South and North Korea applies to online communications as well as offline [83] and that any active engagement with websites or pages maintained by people of North Korea must be reported to the government in advance.[84] Anyone failing to do so faces a fine of up to KRW one million (US$900).

Defamation, including written libel and spoken slander, is a criminal offense in South Korea, punishable by up to five years' imprisonment or a fine of up to KRW 10 million (US$9,000), regardless of the truth of the contested statement. Insult charges, which unlike defamation offenses must be instigated directly by a complainant, are punishable by a maximum KRW two million (US$1,800) fine or a prison sentence of up to one year. Defamation committed via ICTs draws even heavier penalties—seven years in prison or fines of up to KRW 50 million (US$45,500)—under the 2005 Information and Communications Network Act, which cites the faster speed and wider audience of online communication as a basis for the harsher sentencing.[85]

In May 2014, a month after the Sewol ferry disaster, conservative legislator Han Sun-kyo proposed amending the Information and Communications Network Act to criminalize rumormongering on social networking sites "in times of disaster," punishable by up to five years in prison or up to KRW 50 million (US$45,500) in fines. The proposed clause evolved from 47(1) of the 1983 Telecommunica-

83 Ministry of Unification, "Notice on the use of North Korean internet sites" (in Korean), April 8, 2010, http://bit.ly/1VVn7ad.

84 Reports of such contact, online and offline, are to be made through an online system at http://www.tongtong.go.kr/.

85 Act on Promotion of Information and Communications Network Utilization and Data Protection, Art. 61 amended December 30, 2005, http://bit.ly/LoN97A.

tions Business Act, which was ruled unconstitutional in 2009. The proposal remained under consideration at the time of writing this report.

Despite a nine-day filibus er by 38 opposition legislators, a draconian antiterrorism law (the Act on Antiterrorism for the Protection of Citizens and Public Security) was passed in the conservative-dominated National Assembly in March 2016, 14 years after it was fi st proposed (see, Surveillance, Privacy, and Anonymity).

Prosecutions and Detentions for Online Activities

Prosecutions against individuals expressing North Korean sympathies have increased under conservative rule. In the fi st year of the Park Geun-hye administration, national security arrests increased 19 percent and detentions 37.5 percent.[86] Between 2012 and 2014, 104 people were convicted for violation of the National Security Act in cyberspace, although a legislator of the ruling conservative party argued in April 2015 that the number should have been even larger, considering the increase in the number of offenses being committed online.[87]

Numerous online defamation cases have involved President Park Geun-hye since she took office in 2013. With public criticism of her response to the ferry disaster mounting, President Park told a cabinet meeting on September 16, 2014, that "profanity towards the president had gone too far" and that "insulting the president is equal to insulting the nation."[88] Two days after this remark, the public prosecutors' office set up a special in estigation unit for an enhanced monitoring of "online slanders and rumors."

Several prosecutions followed. In March 2015, the Supreme Court sentenced a 31-year-old citizen, Kim, to one year in prison for posting a fake screenshot of a messenger conversation suggesting that the Sewol rescue operation had been deliberately held back, although he deleted it within 10 minutes.[89] In May 2015, a man in his 50s named Wu, who had repeatedly posted a conspiracy theory about the ferry incident between August and November 2014, was sentenced to 18 months in prison for defaming the coast guard.[90] Civic activist Park Seong-soo was given a one-year suspended prison term in December 2015 for distributing fl ers and Facebook posts containing allegations about the president's negligence during the rescue operation, which had already been published in *Chosun Ilbo* in Korea and *Sankei Shimbun* in Japan.[91] In the same month, the Supreme Court found Seoul civil servant Kim Minho guilty posting "defamatory remarks" about President Park and other members of the conservative party in May 2014; he was fined KRW 2.5 million (US$2,780) and lost his position in the City Hall after 22 years.[92]

86 Hong-du Park, "In Park's fi st year, the number of violators of the National Security Act has leaped" (in Korean), *Kyunghyang Shinmun*, February 19, 2014, http://bit.ly/1fzIxmM; see also Amnesty International Report 2015/16.

87 "According to Cho Hae-jin, "Online violation of the NSA increasing dramatically but mostly going unpunished"" (in Korean), *Yonhap News*, April 10, 2015, http://bit.ly/1PzwA89.

88 Full text of the president's speech to the cabinet (in Korean) available at http://bit.ly/1ejqd8e.

89 "A white-collar man who had distributed a fake Kakaotalk on Sewol found to be guilty of cyber defamation" (in Korean), *Kyunghyang Shinmum*, March 1, 2015, http://bit.ly/1F0Ii0s.

90 "A man in his 50s sentenced for one and a half years for posting 'malicious rumors about Sewol' around 600 times" (in Korean), *Yonhap News*, May 16, 2015, http://bit.ly/1F1rBlB.

91 Miran Kim, "Civic activist Park Seong-soo found guilty for defaming Park Geun-hye's 'personal self'" (in Korean), *Gobal News*, December 22, 2015, http://bit.ly/1RsVHER.

92 Jong-cheol, Shin, "Supreme Court divests a civil servant of his office for defaming Chung Mong-joon and ark Geun-hye" (in Korean), *Law Issue*, December 28, 2015, http://bit.ly/1QxJI9d.

Unusually, even foreign reporters came under scrutiny. Japanese journalist Tatsuya Kato of the *Sankei Shimbun* newspaper was indicted for criminally defaming President Park in an August article that cited allegations about the president's whereabouts in the immediate aftermath of the ferry accident, although the same content was first published in a domestic daily, *Chosun Ilbo*, and spread across online media. The journalist was barred from leaving South Korea for eight months, and faced up to seven years in prison,[93] but was ultimately acquitted in December 2015.[94] Beyond national jurisdiction, two U.S.-based journalists received a complaint from the South Korean government for articles criticizing the Park Geun-hye administration's crackdowns on dissent.[95]

At least one similar case was reported after the Middle East Respiratory Syndrome (MERS) broke out in May 2015. At least 184 cases, including 33 deaths, were confirmed by the beginning of July.[96] On June 3, a 49-year-old man in Gyeonggi province named Lee was arrested on suspicion of defamation and obstructing business for forwarding a list of four hospitals he said were possibly affected by the outbreak to his contacts on the domestic instant messenger Kakaotalk the previous afternoon.[97] Police said the hospitals were unaffected.

In March 2016, the Supreme Court issued a positive ruling involving a 37-year-old doctor, Kim, who was prosecuted for insulting the Health Insurance Review and Assessment Service on his blog. The court ruled that swearwords do not constitute insults in the context of criticisms of government policies.[98]

Surveillance, Privacy, and Anonymity

The National Intelligence Service (NIS), the country's chief spy agency, has been at the epicenter of surveillance scandals in recent years. In July 2015, documents from the information technology company Hacking Team were leaked online, indicating that the NIS purchased surveillance software from the Italian company to monitor digital activity, especially on domestic mobile devices and Kakaotalk.[99] The agency acknowledged purchase of the software ahead of the 2012 presidential election, but maintained that it was only used to analyze material related to North Korea. In the wake of the revelations, on July 18, a senior intelligence agent was found dead in an apparent suicide, leav-

93 Roy Greenslade, "South Korea urged to drop libel charges against Japanese journalist," *The Guardian*, October 17, 2014, http://bit.ly/1xyYbZI; Nathan Park, "Is South Korea's criminal defamation law hurting democracy?" *The Wall Street Journal*, December 15, 2014, http://on.wsj.com/16u0CFE.

94 Sang-Hun Choe, "Court acquits journalist accused of defaming South Korean president," *The New York Times*, December 17, 2015, http://nyti.ms/1Yn8Z9I.

95 Whan-woo Yi, "Gov't hit for overreacting to foreign reports," *Korea Times*, December 7, 2015, http://bit.ly/1So4UDw; Se-Woong Koo, "War of words over the state of South Korea," *Korea Exposé*, December 10, 2015, http://bit.ly/1TEjgNx. The articles in question are: Se-Woong Koo, "South Korea's textbook whitewash," *The New York Times*, November 12, 2015, http://nyti.ms/1UF3sNu; Tim Shorrock, "In South Korea, a dictator's daughter cracks down on labor," *The Nation*, December 1, 2015, http://bit.ly/1NphwaD.

96 WHO, "Middle East respiratory syndrome coronavirus (MERS-CoV)—Republic of Korea," World Health Organization, July 3, 2015, http://bit.ly/28QuMJd.

97 "'Random hospital list' leads to the first arrest for spreading MERS rumors" (in Korean), *Yonhap News*, June 3, 2015, http://bit.ly/1TYxtHh.

98 Yonhap News, "According to the Supreme Court, swearing while criticizing government policies does not constitute an insult" (in Korean), March 9, 2016, http://bit.ly/28O6I5f.

99 Bill Marczak & Sarah McKune, "What we know about the South Korea NIS's use of Hacking Team's RCS," *Citizen Lab*, August 9, 2015, http://bit.ly/1N5ctvi; Yu-kyeong Jeong, "Everything you wanted to know about the NIS hacking scandal" (in Korean), *Hankyoreh*, July 23, 2016, http://bit.ly/23IiA2W.

ing a note denying that his team had ever used spyware on citizens.[100] An investigation into possible misuse of the equipment was subsequently dropped.

In the context of growing concerns over the NIS's political meddling and lack of accountability, it is anticipated that the new antiterrorism law, passed in March 2016, will further enhance the NIS's position and threaten individual privacy.[101] To advance terrorism investigations, the law enables the agency to use military means (Article 2), override any other law (Article 4), access individuals' travel records, financial ecords, private communications, location data, and any other personal information, on suspicion alone and without judicial oversight (Article 9). It also provides the agency with budgets that are not subject to audit, (Article 11), and allows it to have any items of expression removed from content online and offline, without judicial o ersight (Article 12).[102]

In activities not covered by that law, court-issued warrants are required to access the content of private communications. Service providers may "choose" to surrender individuals' metadata to the NIS and other investigative agencies without a warrant under Article 83(3) of the Telecommunications Business Act.[103] According to an official May 2015 p ess release, service providers fulfilled 508,511 requests for metadata in the second half of 2014, a six percent increase compared to the same period in 2013.[104] The number of affected citizens corresponds to roughly one fi th of the population.[105] Requests to access the content of private communications decreased, from 132,070 to 127,153 and from 337 to 192 respectively. User rights advocates say these figu es may be misleading, since one request can affect many individuals over a long period of time.[106] An amendment to the Presidential Enforcement Decree of the Network Act, effective from August 2015, shortened the legally permitted period for retaining users' personal data from three years to one year.

Service providers are also criticized for not fulfilling their legal duty f informing affected individuals,[107] leading internet users to share among themselves how to retrieve information about disclosures affecting their accounts.[108] Environment activist Lee Heon-seok, civil rights lawyer Yoon Jiyoung, and labor union representatives Park Byeong-woo and Kwak Yi-kyung are among dozens to discover after the fact that they were the subject of government requests to mobile carriers, though they were not under arrest or formal investigation at the time. The NIS and police retrieved Park's meta-

100 Jack Kim, "South Korea spy found dead with note denying agency targeted citizens," *Reuters*, July 19, 2015, http://reut.rs/1QyBC03; David Gilbert, "Hacking Team leak linked to South Korean spy suicide," *International Business Times*, July 20, 2015, http://bit.ly/1QwkU52.

101 Jun-beom Hwang, "Will passage of anti-terror bill turn the NIS into a monster?" *Hankyoreh*, March 3, 2016, http://bit.ly/1TUSjY4.

102 Steven Borowiec, "South Korean lawmakers try fi st filibus er since 1969 to block anti-terrorism bill," *Los Angeles Times*, February 24, 2016, http://lat.ms/1QpKNmV.

103 Metadata includes the user's name, RRN, postal address, telephone number, user ID, and dates of joining or leaving the service.

104 Tae-jin Kim, "Communication information handover increases—500,000 cases in the 2nd half of last year" (in Korean), *ZDNet*, May 21, 2015, http://bit.ly/1cRDcgu.

105 Kyung-sin Park, "50 times more frequent than in the US , why the current Korean practice of accessing communicator ID information is unconstitutional" (in Korean), *Slow News*, June 14, 2016, http://slownews.kr/55068.

106 Gwang Choi, "The public prosecutors access 67 accounts with one piece of document" (in Korean), *Money Today*, December 3, 2014, http://bit.ly/1ekA7Gy.

107 See also a public campaign by Open Net: "Reclaim the right to be informed when telecom companies disclose personal information" (in Korean), http://bit.ly/1GRAX6e.

108 PPSS, "How to find out whether the NIS and police rummage my mobile phone info mation?" (in Korean), PPSS, February 26, 2016, http://ppss.kr/archives/74772.

data ten times within four months and Kwak's 17 times over a year.[109] In response to requests from users, service providers have refused to provide grounds for complying with these demands.[110]

The 2014 ferry disaster also prompted accusations of privacy violations and government surveillance. The most telling development was a closed-door meeting that public prosecutors held with major service providers in September 2014 to discuss how to curb rumormongering, including on Kakaotalk, the country's most popular mobile messaging application.[111] The company dismissed public concern about its cooperation with law enforcement agencies, saying its compliance was prescribed by law.

Public trust in Kakaotalk, however, was undermined in October 2014 during a press conference by Jung Jinwoo, a vice representative of the Labor Party charged with "causing public unrest" during a post-Sewol protest. Jung said prosecutors had accessed two months' worth of his private Kakaotalk conversations, along with the personal details of his 3,000 contacts, as part of the investigation.[112] Public prosecutors responded by asking the court to cancel Jung's bail.[113] Yong Hye-in, a university student who initiated a silence protest to show support and solidarity for Sewol victims and their families, also turned out to be subject to surveillance on Kakaotalk.[114] In a February 2016 court case, Yong successfully contested the validity of the surveillance warrant executed against her on grounds that she was not appropriately informed, but prosecutors appealed the case to the Supreme Court.[115]

Some 400,000 users left the service for foreign alternatives perceived to be beyond the influence f the South Korean government, such as Telegram, a Germany-based messaging service that advertises encrypted connections.[116] In order to regain user trust, Kakaotalk held a press conference in October 2014, where its CEO, Lee Sir-goo, vowed to reject future data requests from the authorities, even those with warrants.[117] The following month, it was reported that seven warrants were pending due to the company's noncompliance. A year later, in October 2015, Kakaotalk announced that it would resume complying with law enforcement requests. More users, including politicians and activists, were reported to be switching messenger clients from Kakaotalk to Telegram, and using iPhones, the only smartphone device known to have failed to meet the NIS requirements,[118] after the antiterrorism bill was passed in March 2016.[119]

109 Hyung-kyu Kim, "NIS digs around the communication records of environmental activists, union representatives, and lawyers" (in Korean), *Kyunghyang*, March 4, 2016, http://bit.ly/1Sp9n8O.

110 Junho Bang, "When asked why my 'communication information' was looked at, service providers refuse to answer, saying they have 'no legal obligation'" (in Korean), *Hankyoreh*, March 13, 2016, http://bit.ly/1Th3R6J.

111 Jae-seob Kim, "KakaoTalk managers present at prosecutors' meeting on countering 'defamation of the president'" (in Korean), *Hankyoreh*, October 2, 2014, http://bit.ly/1vzr6Oy.

112 "Jung Jinwoo: Police surveillance over 3,000 of my family and acquaintances" (in Korean), *JTBC News*, October 2, 2014, http://bit.ly/1PAH0nY.

113 "Public prosecutors says Vice rep Jung Jinwoo's 'Kakaotalk press conference' caused public unrest" (in Korean), *Yonhap News*, October 19, 2014, http://bit.ly/1F5I3lu.

114 Myeong-soo Seon, "How was Kakaotalk surveillance 'legally' possible?" (in Korean), *Pressian*, October 1, 2014, http://bit.ly/1LkpBJJ.

115 Junho Bang, "Kakao chat surveillance victims stage citizens' filibus er," *Hankyoreh*, February 26, 2016, http://bit.ly/21KAlha.

116 Sam Judah & Thom Poole, "Why South Koreans are fleeing the count y's biggest social network," *BBC News*, October 10, 2014, http://bbc.in/1MimzbB.

117 Peter Micek, "South Korean IM app takes bold stand against police abuses," *Access*, October 16, 2014, http://bit.ly/1Q1as1f; "Seven warrants for Kakaotalk monitoring still disobeyed and prosecutors looking to enhance law" (in Korean), *Yonhap News*, November 12, 2014, http://bit.ly/1R9P8JC.

118 Nayoung Shim, "iPhone fails at the NIS's security compatibility assessment" (in Korea), *Asia Economy*, November 12, 2012, http://bit.ly/1QA7YYy. The full description of the NIS's Security Verification Scheme can be found he e: http://eng.nis.go.kr/EAF/1_7_1_1.do

119 Hyung-kyu Kim, "'2nd wave of cyber exodus' with the anti-terrorism bill now passed. Ruling party members joining too" (in Korean), *Kyunghyang Shinmun*, March 4, 2016, http://bit.ly/1QA8Ps9.

In November 2015, Kakaotalk CEO Lee stepped down to face criminal charges for failing to prevent teenagers from sharing lewd photos of themselves on the service, in contravention of Article 17(1) of the Children and Youth Protection Act. Though the charge carries a possible two-year prison sentence, few observers expect him to be convicted, and he took a position with a media group soon after his resignation. Nevertheless, since holding a CEO personally liable for user activity is unprecedented in South Korea, critics suspected that the real goal was "to punish him for resisting government surveillance efforts and refusing to curb users' opinions critical of the government."[120] During a parliamentary filibus er in February 2016, opposition legislator Hong Jong-hak reported that Kakaotalk was subjected to comprehensive tax audits three times within the last seven years, a level of scrutiny reserved for just 0.06 percent of corporate bodies. According to Hong, the audits took place during periods of heightened public criticism of the government, including after the Sewol ferry disaster in 2014 and the MERS outbreak in 2015. The 2015 audit lasted 137 days, three times longer than the average 36 days.[121]

Within South Korea, anonymous communication was long compromised by the so-called "internet real-name system" fi st adopted in 2004 as part of an amendment to the Public Official Election Act.[122] Users were required to verify their identities by submitting their Resident Registration Numbers (RRNs) to join and contribute to web portals and other major sites. An RRN is a 13-digit number uniquely assigned to a Korean citizen at birth. In 2007, the real-name system was expanded to apply to any website with more than 100,000 visitors per day under Article 44(5) of the Information and Communications Network Act.

In 2012, the Constitutional Court ruled Article 44(5) of the Network Act unconstitutional, citing privacy vulnerabilities from cyberattacks among other factors.[123] In 2011, a cyberattack allegedly originating from China targeted the popular portal Nate and its social networking service Cyworld. Hackers reportedly stole the personal details of 35 million users, equivalent to 70 percent of the population, including names, passwords, RRNs, mobile phone numbers, and email addresses. The portal's parent company, SK Communications, said RRNs and passwords were encrypted,[124] but the incident renewed public concern about internet users' right to privacy.[125]

The Personal Information Protection Act was amended in 2013 to reflect the Constitutional Cou t's 2012 ruling. Website administrators are now prohibited from collecting users' RRNs, and must destroy those already on record. Effective from August 2014, failure to protect an individual's RRN is punishable by fines f up to KRW 500 million (US$455,000).[126] Mobile service providers still require users to provide their RRNs.

Other laws, such as the Public Official Election Act, the Child en and Youth Protection Act, the Game Industry Promotion Act, and the Telecommunications Business Act, separately require internet users

120 "South Korea targets dissent," *The New York Times*, November 19, 2015, http://nyti.ms/1jah3N0; Simon Mundy, "Freedom fears as South Korea targets chat app chief," *Financial Times*, November 17, 2015, http://on.ft.com/1OVl2p4.

121 Slides that he used during his speech on February 29, 2016, are available for downloads at his official blog: http://bit.ly/1L7u4ol.

122 The amendment became Article 82, Provision 6.

123 Kyung Sin Park, "Korean internet identity verification rule struck down unconstitutional; 12 highlights f the judgment," *K.S. Park's Writings* (blog), August 25, 2012, http://bit.ly/1nevLB7.

124 AP, "Nate, Cyworld hack stole information from 35 million users: S Korea officials" *Huffington Post*, July 28, 2011, http://huff.to/1k9aiaf.

125 Eric Pfanner, "Naming names on the internet," *The New York Times*, September 4, 2011, http://nyti.ms/1ffDiLz.

126 Yun-ji Kang, "Hide your RRN away! Ban on online collection of user RRNs" (in Korean), *Policy News* (blog by the Ministry of Culture, Sports and Tourism), February 21, 2013, http://bit.ly/1eefGaD.

to verify their identities.[127] In July 2015, the Constitutional Court confi med that it is appropriate for the Public Official Election Act o require people to use their real names online during election periods (22 days before a presidential election and 13 days before a general election).[128]

To ensure compliance with these laws, the KCC is exploring other identity verification methods, such as Internet Personal Identification Numbe s (i-PINs, overseen by the Ministry of Government Administration and Home Affairs), authenticated certifica es (issued by banks and other organizations permitted to collect RRNs by Article 23 of the Network Act), and SMS verification. Ho ever, large-scale hacking attacks into the i-PIN system in February 2015, generating 750,000 counterfeit numbers, called for rethinking of the security framework at a more fundamental level.[129]

Following the 2011 Cyworld hack, around 2,900 users together filed suit for damages, but the Seoul High Court ruled in favor of the company in March 2015.[130] Fifteen citizens also filed a lawsuit o change their RRNs, but the Seoul Administrative Court and the Seoul High Court ruled against them. However, in December 2015, the Constitutional Court ruled that disallowing people to change their RRNs was unconstitutional and advised that the Resident Registration Act be revised accordingly by December 31, 2017.[131]

Intimidation and Violence

There have been no reports of physical violence against online users in South Korea.

Technical Attacks

Reported violations of electronic data tripled between 2010 and 2013, from 54,832 incidents to 177,736, but decreased to 152,151 in 2015, according to official statistics [132] Local officials alleged that the North Korean government was behind the attacks on major banks and broadcasting stations in March 2013,[133] those on nuclear power plants in December 2014,[134] and remote controlling of a large university hospital network over 8 months between 2014 and 2015,[135] among many other such threats,[136] which highlight vulnerabilities in the country's ICT infrastructure. Attacks were ongoing during the reporting period, though they did not succeed in disabling as many high-profile institutional targets.

127 Bora Jeong, "Internet real-name system and its lingering remains" (in Korean), *Bloter.net*, September 13, 2013, http://bit.ly/1jKR4Hx.

128 Kyung-min Lee, "Online real name system during election periods constitutional: court," *The Korea Times*, July 30, 2015, http://bit.ly/28QNHnH.

129 Sang-wook Ahn, "Hacking attacks result in 750,000 counterfeit public i-PINs" (in Korean), *Bloter*, March 5, 2015, http://bit.ly/1AoxYne.

130 Jihoon Kim, "Court says SK Comms has no responsibility to compensate users for Cyworld personal information hack" (in Korean), *Newsis*, March 20, 2015, http://bit.ly/1F1vB5o.

131 Hyun-ju Ock, "Court allows changes to national IDs," *Korea Herald*, December 23, 2015, http://bit.ly/1OVgcZ8.

132 Statistics Korea, "Incidents of personal information violation" (in Korean), *e-National Indicators*, http://bit.ly/1fcGxBK.

133 Agence France-Presse, "S. Korea probe says North behind cyber attack," *The Straits Times*, April 10, 2013, http://bit.ly/1jKAUAt; CrowdStrike, *CrowdStrike Global Threat Report*, January 22, 2014, p.25, http://bit.ly/1ffcUUB.

134 Jeyup S. Kwaak, "North Korea blamed for nuclear-power plant hack," *Wall Street Journal*, March 17, 2015, http://on.wsj.com/1EYLbnB.

135 Chang-wook Kang, "North Korea's remote controlling over the entire network of a large university hospital in Seoul goes unnoticed for 8 months" (in Korea), *Kukmin Ilbo*, August 13, 2015, http://bit.ly/1RMH2XU.

136 Ju-min Park & Jack Kim, "South Korea says suspects North Korea may have attempted cyber attacks," *Reuters*, January 26, 2016, http://reut.rs/1QBm7rW.

Freedom House

Sri Lanka

	2015	2016
Internet Freedom Status	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	14	14
Limits on Content (0-35)	13	12
Violations of User Rights (0-40)	20	18
TOTAL* (0-100)	**47**	**44**

* 0=most free, 100=least free

Population:	**21 million**
Internet Penetration 2015 (ITU):	**30 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- Internet freedom continued to improve under President Maithripala Sirisena, though free speech advocates criticized his reactivation of the draconian Press Council (see **Media, Diversity, and Content Manipulation**).
- In an isolated incident, one political website was reported to have been blocked by a telecommunications provider (see **Blocking and Filtering**).
- The government withdrew draft legislation to criminalize hate speech after political and civil society opposition (see **Legal Environment**).
- Digital activism increased and activists used social media to spur public engagement with political issues (see **Digital Activism**).

Introduction

Following the defeat of Mahinda Rajapaksa in the January 2015 presidential election, internet freedom has improved considerably in Sri Lanka. During the coverage period of this report, there were no reports of attacks, arrests or intimidation for online activities, in contrast to previous years.

Despite securing a nomination to run in the August 2015 parliamentary election, Rajapaksa and his supporters were unable to defeat the incumbent government. The United National Party (UNP)-led United National Front for Good Governance (UNFGG) secured 106 seats in a 225-member legislature, but fell short of a majority.[1] After negotiations, the UNP signed a two-year memorandum of understanding with the Sri Lanka Freedom Party (SLFP) to form a government.[2]

For the most part, internet freedom continued to improve under President Maithripala Sirisena and Prime Minister Wickremesinghe.[3] All websites blocked by the previous government continue to be accessible, including the exile-run news website *TamilNet,* which had been blocked since 2007 for reporting on the military campaign against the Liberation Tigers of Tamil Eelam (LTTE).[4] Digital activism continues to strengthen. In the lead up to election, activists launched voter education campaigns on Facebook and Twitter, and news websites adopted mobile messaging platforms like WhatsApp to keep citizens informed.

However, in a move that went against his election promises, President Sirisena reactivated the draconian Press Council in July 2015 despite civil society opposition, chilling media freedom including online. Separately, the government's attempt to introduce legislation to criminalize hate speech (even though such a law already exists) was thwarted by civil society groups and opposition parties who argued that the proposed law could be used to target government critics. In one isolated case, supporters of Mahinda Rajapaksa said their website had been blocked in advance of the election.

Legal and regulatory reform is still needed to consolidate the opening for internet and media freedom. At the end of the coverage period of this report, an amended Right to Information bill was still under discussion, a public consultation process on transitional justice was underway, and a constitutional reform process had just begun.

Obstacles to Access

Internet penetration in Sri Lanka continues to increase every year due to the affordable rates offered by ISPs. Moreover, an increasing segment of the population has turned to smartphones in order to access the web. According to the Department of Census and Statistics, Sri Lanka's digital literacy rate increased from 20 percent in 2009 to 25 percent in 2014. Regulatory reform to ensure independence and transparency is a pressing need as Sri Lanka's Telecommunications Regulatory Commission (TRC)

1 "Sri Lanka's PM defeats ex-president in elections", Al Jazeera, August 19, 2015, http://www.aljazeera.com/news/2015/08/sri-lanka-elections-150818133605788.html

2 "UNP and SLFP reach a two-year agreement", NewsFirst, August 21, 2015, http://newsfi st.lk/english/2015/08/unp-and-slfp-reach-a-two-year-agreement/107750

3 Siobhan Hagan, "Rights advocates welcome promised changes in Sri Lanka", International Press Institute, January 13, 2015, http://www.freemedia.at/newssview/article/press-freedom-advocates-welcome-promised-changes-in-sri-lanka.html

4 "TamilNet Blocked in Sri Lanka", BBC Sinhala, June 20, 2007, http://bbc.in/1YfSL5b.

continues to operate under the authority of President Sirisena, with his permanent secretary as its chairman.

Availability and Ease of Access

The International Telecommunication Union estimated internet penetration at 30 percent in 2015, up from 26 percent in 2014, as a continually expanding economic sector and a growing youth population drove demand for online services.[5] Mobile penetration was reported at 112 percent.[6] The Central Bank of Sri Lanka reported that mobile internet connections grew 22.2 percent, while fi ed-line connections grew by 12.6 percent during 2015.[7]

Free access to the internet was a key campaign promise of President Sirisena and it was featured in his manifesto for the presidential election. A few months after his election victory, the interim government announced the availability of free Wi-Fi at 26 public locations around the country.[8] The Information Communications and Technology Agency (ICTA), a state agency responsible for implementing the plan, announced that free Wi-Fi would be available at over 2000 public locations by the end of 2016.[9] The government's 2016 Budget proposals included a plan to provide free internet to state universities.[10]

Internet connectivity is becoming more affordable, with Sri Lanka Telecom's cheapest broadband connections priced at just under US$3 a month,[11] and Dialog's only slightly more.[12] In addition, increasingly affordable handsets and data packages have boosted mobile internet use, particularly among young people.[13] The overall growth rate for the market has been consistent year on year. In early 2016, according to the Minister of Telecommunication and Digital Infrastructure, smartphone penetration stood at 26 percent,[14] up from an estimated 20 percent at the end of 2014.[15] Technology company Huawei described Sri Lanka as the fastest growing smartphone market in South Asia

5 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1cblxxY.

6 International Telecommunication Union citing Telecommunications Regulatory Commission data, "Mobile-cellular subscriptions, 2000-2015," http://bit.ly/1cblxxY. The Central Bank of Sri Lanka reported 116 percent. See, Economic and Social Statistics of Sri Lanka 2015, http://www.cbsl.gov.lk/pics_n_docs/10_pub/_docs/efr/annual_report/AR2015/English/7_Chapter_03.pdf, 79.

7 The bank reported a slightly lower overall penetration rate, at 19.5 percent. Economic and Social Statistics of Sri Lanka 2015, Central Bank of Sri Lanka, http://www.cbsl.gov.lk/pics_n_docs/10_pub/_docs/efr/annual_report/AR2015/English/7_Chapter_03.pdf, 79.

8 The Official Go ernment News Portal of Sri Lanka, "Free Wi-Fi from today at 26 public locations in Sri Lanka," news release, March 30, 2015, http://bit.ly/1KjuEJj.

9 "ICTA plans ambitious digital infrastructure, Google Loon by March", LBO, November 6, 2015, http://www.lankabusinessonline.com/icta-plans-ambitious-digital-infrastructure-google-loon-by-march/

10 Azhar Razak, "Summary of 2016 Budget proposals", November 20, 2015, The Nation, http://nation.lk/online/2015/11/20/summary-of-2016-budget-proposals.html

11 Sri Lanka Telecom's cheapest broadband package offers 3.5GB at about $3 a month with a monthly rental fee of $1 and additional $3 startup fee. SLT also offers a concessionary package for students that costs about $2.50 with the same start-up fee and monthly rental fee as other packages. SLT, Broadband packages, https://www.slt.lk/en/personal/internet?item_id=104, accessed May 31, 2016

12 Dialog's cheapest broadband package offers 5GB at about $4 a month and an additional one-time connection fee of $26. Dialog, 4G Home Broadband, http://www.dialog.lk/browse/plansFixedBroadband.jsp?categoryId=onlinecat3800057&utm_source=dialoglk&utm_medium=homeIcons&utm_content=HomeBB&utm_campaign=dialoglk-Home, accessed May 31s 2016

13 Bandula Sirmanna, "Smart phones catch the eye of Sri Lankan Youth", *The Sunday Times*, October 20, 2013, http://bit.ly/1QIHp4G.

14 "Via Google Loon, Sri Lanka to be world's fi st with 4G-LTE coverage," March 8, 2016, Opportunity Sri Lanka, http://opportunitysrilanka.com/via-google-loon-sl-to-be-worlds-fi st-with-4g-lte-coverage/

15 "Sri Lanka's mobile phone shipments reached 1mn units in 3Q: Smart phone shipments up 100 pct: Report", LBO, December 25, 2014

in 2015.[16] Monthly subscriptions for mobile data packages can cost less than $1 a month whilst users can also access data services through pay-as-you-use packages.[17] Mobitel also offers 24-hour internet plans costing as little as LKR 3 (US$0.02) for 17MB of data.[18] Sri Lanka's average monthly household income is over $300,[19] making the cost of internet and mobile data packages relatively affordable given the range of pricing options.

However, accessibility to internet services, in terms of greater coverage, continues to be a priority for the incumbent government. The ICTA signed an agreement with Google to start testing Project Loon—a balloon-powered high-speed internet service—with the aim of connecting more of the population to the internet. Three balloons launched by Project Loon entered Sri Lanka's airspace in February 2016.[20] It is expected that service providers will be able to extend coverage and also provide higher speeds through the balloons.[21] The Minister of Telecommunications has stated that internet penetration will increase to 50 percent as a result of the project and other developments.[22] After the initial media blitz on the project in 2015, there have been limited updates. News reports said Google would work with existing ISPs and share the frequencies after testing is complete.[23] Some form of a joint venture is expected to be established to take the project forward.

While Wi-Fi coverage appears to be increasing every year, telecommunications experts have voiced concerns about the reliability of speeds delivered through public Wi-Fi spots.[24] ISPs are attempting to address the issue of speed with new and improved services. SLT introduced carrier-grade public Wi-Fi technology, allowing enterprises, institutions and other private sector entities to access island-wide hotspots with a username and password.[25] In July 2015, Dialog Broadband announced the start of its LTE Advanced Pilot Network, which would provide data speeds in excess of 100 Mbps for home broadband users, initially within selected areas of Colombo.[26] As of March 2016, Dialog operated over 2,500 pay-to-use Wi-Fi hotspots around the country with tiered subscription rates.[27] SLT reported over 70 Wi-Fi nationwide hotspots for its broadband subscribers and prepaid access.[28]

Low digital literacy represents a major barrier to ICT use. Although Sri Lanka's literacy rate is approx-

16 "Sri Lanka, one of the fastest growing markets in South Asia", News.lk, October 1st, 2015, http://www.news.lk/news/sri-lanka/item/10045-sri-lanka-one-of-the-fastest-growing-markets-in-south-asia.

17 Mobile Broadband – Postpaid, http://www.dialog.lk/mobile-knktd-data-packages/, accessed May 31, 2016

18 Mobitel, Broadband, http://www.mobitel.lk/internet-chooti, accessed May 31st, 2016

19 Household Income and Expenditure Survey – 2012/13, Department of Census and Statistics, June 2013, http://www.statistics.gov.lk/hies/hies201213buletineng.pdf

20 "Project Loon: Google balloon that beams down internet reaches Sri Lanka", The Guardian, February 16, 2016, http://www.theguardian.com/technology/2016/feb/16/project-loon-google-balloon-that-beams-down-internet-reaches-sri-lanka

21 Uditha Jayasinghe, "Google's 'Project Loon' Balloon Internet Experiment Floats into Sri Lanka", February 16, 2016, http://blogs.wsj.com/indiarealtime/2016/02/16/googles-project-loon-balloon-internet-experiment-fl ats-into-in-sri-lanka/

22 "Sri Lanka looks to LTE, Project Loon to double internet penetration", Mobile World Live, April 11, 2016, http://www.mobileworldlive.com/asia/asia-news/sri-lanka-looks-to-lte-project-loon-to-double-internet-penetration/

23 Gopiharan Perinpam, "Google Loon is Here – What Does This Mean For Sri Lanka", Roar.lk, May 5, 2016, http://tech.roar.lk/insights/google-loon-is-here-%E2%80%92-what-does-this-mean-for-sri-lanka/

24 Rohan Samarajiva, "Morning after: Thinking through Sri Lanka President's free Wi-Fi promise," LirneAsia, February 28, 2015, http://bit.ly/1iRO7Kr; Yudhanjaya Wijeratne, "Why Yahapalanaya's Train Wi-Fi might not be as cool as you think," *Readme*, February 28, 2015, http://readme.lk/free-wifi-train-stations .

25 "WLT Wi-Fi hotspots for the fi st time in Sri Lanka", *The Sunday Times*, May 25, 2014, http://bit.ly/1KTB73m.

26 "Dialog launches customer trial in Colombo with 100 Mbps Home Broadband", Dailymirror.lk, July 15th, 2015, http://www.dailymirror.lk/79677/dialog-launches-customer-trial-in-colombo-with-100-mbps-home-broadband

27 "Wi-Fi Hotspots in Sri Lanka", Dialog, http://www.dialog.lk/personal/broadband/wi-fi ; "Dialog's Giving Everyone Free Wi-Fi. For 30 Days," *Readme*, September 22, 2014, http://readme.lk/dialogs-giving-free-wi-fi-30-days .

28 SLT, Wi-Fi Coverage, https://www.slt.lk/en/personal/broadband/wi-fi/co erage

imately 91 percent,[29] only 20 percent of the population was comfortable using computers in 2009.[30] However, this increased to 27 percent in 2015, according to the Department of Census and Statistics (DCS).[31] The department reported that a higher percentage of young people use computers (57 percent for ages 15-19; 52 percent for ages 20-24; and 43 percent for ages 25-29). Older age groups had a lower rate of digital literacy (26 percent for ages 35-39 and 16 percent for ages 40-49).[32] Digital literacy was higher in urban areas (40 percent) and lower in rural areas and among Up-Country communities (24 percent and 7 percent respectively) where the high cost of personal computers limits access for lower-income families, and schools with digital facilities lack corresponding literacy programs. The ICTA has promoted digital literacy in rural areas by establishing community-based knowledge centers, e-libraries, and e-learning centers to promote ICT access and services,[33] though some local journalists criticized aspects of the initiative in the past.[34] The Department of Census and Statistics has also reported climbing computer acquisition rates, with almost 67 percent of households acquiring a fi st computer between 2010 and 2014.[35] The acquisition rate was 70 percent in the rural sector and 56 percent in the urban sector.

The civil war caused severe lags in infrastructure development for the northern and eastern provinces. Since its conclusion in 2009, the government has made up some of this ground, thereby boosting the regions' economic growth, though development was also criticized for causing issues with respect to land ownership that threatened to further marginalize the local Tamil community, among others in the region.[36] There has been some progress following the change in government. In April 2015, the military confi med that it had released 1,000 acres of land from high-security zones (HSZs) in the Northern province.[37] In March 2016, the Navy released over 177 acres of land in Sampur, which is in the Eastern province, to rightful owners who had been previously displaced due to the conflict and the occu ation of their lands.[38] However, militarization and the existence of other HSZs remain a serious concern.[39] More positively, census data identified heavy in ernet usage in post-war minority districts in 2011 and 2012, citing Vavuniya in the Northern Province as the district with the country's highest household internet usage.[40] In 2014, the Northern Province had the second highest percentage of households reporting internet and email usage in the entire country (11 and 8 percent

29 UNICEF, "Sri Lanka Statistics," accessed July 2013, http://www.unicef.org/infobycountry/sri_lanka_statistics.html.

30 Department of Census and Statistics, "Computer Literacy Survey – 2009," http://www.statistics.gov.lk/CLS/BuletinComputerLiteracy_2009.pdf.

31 Computer Literacy Statistics – 2015, Department of Census and Statistics, January – June 2015, http://www.statistics.gov.lk/samplesurvey/ComputerLiteracy-2015Q1-Q2-final%20.pd

32 Computer Literacy Statistics – 2015, Department of Census and Statistics, January – June 2015, http://www.statistics.gov.lk/samplesurvey/ComputerLiteracy-2015Q1-Q2-final%20.pd

33 Nenasala, "Establishment of Nenasalas," accessed July 2013, http://bit.ly/1W4XODp.

34 "ICTA Responds to Business Times report on e-government project," *The Sunday Times*, January 6, 2013, http://bit.ly/1bmHPwO.

35 Computer Literacy Statistics – 2015, Department of Census and Statistics, January – June 2015, http://www.statistics.gov.lk/samplesurvey/ComputerLiteracy-2015Q1-Q2-final%20.pd

36 M.A. Sumanthiran, "Situation in North-Eastern Sri Lanka: A series of serious concerns," *dbsjeyaraj* (blog), October 23, 2011, http://bit.ly/1Ozd3Cs.

37 "Sri Lanka releases 1000 acres of land from high security zones in Jaffna," ColomboPage, April 11, 2015, http://www.colombopage.com/archive_15A/Apr11_1428691768CH.php

38 "Navy hands over 177 acres of land in Sampur to legitimate owners," DailyFT, March 28, 2016, http://www.ft.lk/article/533374/Navy-hands-over-177-acres-of-land-in-Sampur-to-legitimate-owners

39 "Sri Lanka accused of waging 'silent war' as Tamil land is appropriated by army," *The Guardian*, May 28 2015, http://www.theguardian.com/global-development/2015/may/28/sri-lanka-army-land-grabs-tamil-displacement-report-oakland-institute

40 Rohan Samarajiva, "Sri Lanka census data show heavy household Internet use in post-conflict minority districts" LirneAsia, December 30, 2013, http://bit.ly/1W4YqJh.

respectively). In 2015, this encouraging trend continued. Vavuniya had the country's second highest rate of internet usage (18 percent); Jaffna had the fourth highest (17 percent).[41]

Restrictions on Connectivity

Sri Lanka has access to multiple international cables, but the majority of the landing stations for these cables is controlled by Sri Lanka Telecom (SLT), the majority government-owned ISP.[42] Lanka Bell, a private operator, controls one landing station. SLT does not allow other telecommunications companies to connect to landing stations using their own fiber net ork and instead imposes price barriers by making competing players lease connectivity at significantly high prices [43] The state's control over the internet architecture in the country is problematic, especially when non-price barriers emerge, such as delays in responding to private companies' requests for increased capacity.

In May 2016, however, Dialog announced that Sri Lanka was now connected to the Ultra High Capacity BBG Submarine Fibre Optic Cable through its cable landing station located in the south of Colombo.[44] The connection will boost speeds by providing over 6 Tbps of international bandwidth. It is reported that Dialog will allow other operators to buy bandwidth and directly compete with its data prices.

SLT also announced the opening of a new cable landing station for SEA-ME-WE-5 in the south of Sri Lanka in early 2016.[45] In 2014, SLT entered into a partnership with 15 international telecom operators and formed a consortium to build the SEA-ME-WE 5 undersea cable system to connect 17 countries in Southeast Asia, the Middle East, and Western Europe.[46]

There were no large-scale connectivity interruptions during the coverage period of this report, although they have occurred in the past. SLT temporarily severed internet and 8,000 mobile phone connections in the predominantly Tamil-speaking north and east in 2007, then the center of the conflict with the TTE.[47]

ICT Market

SLT commanded more than 41 percent of the total fi ed-line market in 2013, which is substantially

41 Computer Literacy Statistics – 2015, Department of Census and Statistics, January – June 2015, http://www.statistics.gov.lk/samplesurvey/ComputerLiteracy-2015Q1-Q2-final%20.pd

42 Sri Lanka Telecom PLC, Update Report, Fitch Ratings, January 21, 2013, http://bit.ly/2fn0vlk.

43 Helani Galpaya, *Broadband in Sri Lanka: Glass Half Full or Half Empty?* (Washington, D.C.: infuse/The World Bank, 2011), http://bit.ly/1izou0Y.

44 "Dialog Connects Sri Lanka to Ultra High Speed 100G-Plus Submarine Cable", Dialog, May 30, 2016, https://www.dialog.lk/dialog-connects-sri-lanka-to-ultra-high-speed-100g-plus-submarine-cable

45 "SLT introduces SEA-ME-WE 5 submarine cable system and fi st tier 4 ready data station", The Island, February 1, 2016, http://www.island.lk/index.php?page_cat=article-details&page=article-details&code_title=139608

46 Raj Moorthy, "Facebook and Google to enter Sri Lanka in June this year", *The Sunday Times*, February 7, 2016, http://www.sundaytimes.lk/160207/business-times/facebook-and-google-to-enter-sri-lanka-in-june-this-year-181941.html

47 "Cutting off Telecoms in Sri Lanka Redux...," *Groundviews*, January 30, 2007, http://bit.ly/1OzcQ29.

lower than the 87 percent it held in 2004.[48] President Sirisena appointed his brother as the chairman of Sri Lanka Telecom in January 2015.[49]

With over 10.5 million subscribers,[50] Dialog Axiata is the largest mobile service provider, followed by Mobitel (over 5 million),[51] Etisalat (3.8 million), Airtel-Bharti Lanka (1.8 million), and Hutchison Telecommunications (1.4 million).[52] So far, only Dialog Axiata, Mobitel, Sri Lanka Telecom and Lanka Bell offer 4G LTE broadband services.[53]

Regulatory Bodies

Regulatory reform continues to be a pressing issue. The Telecommunications Regulatory Commission (TRC) was established under the Sri Lanka Telecommunications (Amendment) Act, No. 27 of 1996, which states that the Secretary to the Minister of Telecommunications will also be Chairman of the TRC.[54] Over the years, the TRC's interventions to restrict online content and pronouncements on strengthening online regulation have been partisan, extralegal, and repressive.[55]

During Rajapaksa's presidency, the Ministry was placed under his authority for a period of time and his secretary, Lalith Weeratunga, served as Chairman. In February 2015, after Rajapaksa's defeat in the presidential election, a businessman lodged a complaint at the Financial Crimes Investigation Division (FCID) against Lalith Weeratunga and Anusha Palpita, the former director-general of the TRC, for the alleged misappropriation of LKR 620 million (US$4 million) in TRC funds for the former president's election campaigns.[56] In May 2016, the Attorney General's Department filed indictments b - fore the High Court against Weeratunga and Palpita under the Public Property Act and the Sri Lanka Telecommunications Regulatory Commission Act for the alleged criminal misappropriation of public funds.[57] This news came in the same month that Palpita was appointed as Additional Secretary to the Ministry of Home Affairs, increasing skepticism about the incumbent government's commitment

48 "Lanka's ICT literacy, penetration below global averages, remains a focus in macro development agenda – Sri Lanka Telecom Group CEO Greg Young," The Island, November 4, 2012, http://www.island.lk/index.php?page_cat=article-details&page=article-details&code_title=65313; Sri Lanka: Telecommunication Sector," JKSB Research, December 2008, http://www.jksb.keells.lk/newjksb/research%5CTelecom%20Sector%20-%20December%202008.pdf.

49 http://www.asianmirror.lk/news/item/6618-president-s-brother-kumarasinghe-sirisena-appointed-as-telecom-chairman

50 Dialog Axiata PLC, https://www.dialog.lk/fact-sheet, accessed May 31, 2016

51 "Mobitel finalizes erms of Hutch takeover, report says," *TeleGeography*, February 11, 2014, http://bit.ly/1izpDpo.

52 The customer base figu es for Etisalat, Airtel and Hutchison received from sources in each company (according to customer churn rates for June/July 2015).

53 "Dialog launches fi st mobile 4G-LTE service in Colombo," *Daily FT*, April 2, 2013, http://bit.ly/1gukvRx; Duruthu Edirimuni Chandrasekera, "Etisalat to head start on 4G," *The Sunday Times*, February 10, 2013, http://bit.ly/1KswESY; "Lanka Bell Launches 4G Connectivity", *Explore Sri Lanka*, April 2014, http://exploresrilanka.lk/2014/04/lanka-bell-launches-4g-connectivity/.

54 Sri Lanka Telecommunications (Amendment) Act, No.27 of 1996, http://www.trc.gov.lk/images/pdf/legislation/Act%2027%20of%201996.pdf, Section 3 (1) (a)

55 "Colombo Telegraph blockade: TRC clueless," *Daily FT*, August 27, 2013, http://www.ft.lk/2013/08/27/colombo-telegraph-blockade-trc-clueless/; Sarath Kumara, "Sri Lankan government prepares new Internet restrictions," *World Socialist Web Site*, February 15, 2010, http://bit.ly/1QkpyA3.

56 "Sri Lanka; Lalith Weeratunga summoned to Presidential Commission of Inquiry," September 16, 2015, http://www.colombopage.com/archive_15B/Sep16_1442379869CH.php

57 "Indictments filed against 16 including Basil , Daily News, May 20th, 2016, http://www.dailynews.lk/?q=2016/05/20/law-order/82286

to its own political program of *yahapalanaya*, or good governance. Civil society organizations opposed the appointment,[58] and he was subsequently removed.[59]

President Sirisena, like his predecessor, appointed his permanent secretary, P. B. Abeykoon, as the Chairman of the TRC.[60] President Sirisena also appointed M. M. Zuhair, a former Member of Parliament, diplomat and current President's Counsel, as the TRC director-general.[61] These political appointees, who lacked the necessary experience and expertise, were cause for concern given the TRC's interventions in the past. In October 2015, not long after their appointment, M. M. Zuhair and the board of directors were fi ed by President Sirisena for violating TRC financial egulations.[62] Zuhair was replaced by Sunil S. Sirisena, a retired, senior member of the Sri Lanka Administrative Service.[63]

Limits on Content

During the coverage period of this report, a website belonging to former President Rajapaksa's information center was reportedly blocked under an order from the TRC. Other websites that were previously blocked under former President Rajapaksa's government continue to be accessible. Digital activism remains vibrant in Sri Lanka, with a number of citizen media sites and news sites freely publishing content on political and socioeconomic issues in the country.

Blocking and Filtering

President Sirisena moved quickly to dismantle the censorship regime imposed up until 2015 by his predecessor. Prime Minister Ranil Wickremesignhe assured journalists that they would be free to report without fear of harassment and that authoritarian practices like internet censorship would not occur under the new government.[64] Previously inaccessible content became accessible across ISPs, including the exile-run news website *TamilNet,* censored since 2007 for its support of the Tamil rebels.[65] As with the previous government, the current government continues to restrict access to many pornography websites.[66]

There was one apparent exception to an otherwise strong record since January 2015. In September 2015, the *Colombo Telegraph* reported that Mobitel, a subsidiary of Sri Lanka Telecom,[67] had re-

58 "Statement on Anusha Palpita's Appointment", Centre for Policy Alternatives, May 27, 2016, http://www.cpalanka.org/wp-content/uploads/2016/05/statement_on_anusha_palpita_s_appointment.pdf

59 "Anusha Palpita removed from Home Ministry post", adaderana.lk, May 31, 2016, http://adaderana.lk/news/35493/anusha-palpita-removed-from-home-ministry-post

60 Telecommunications and Regulatory Commission of Sri Lanka, "Chairman and the Director-General Assume Duties," http://bit.ly/1Qkqq7P.

61 "M.M. Zuhair appointed Director General of TRC", News.lk, January 29, 2015, http://www.news.lk/news/politics/item/5952-m-m-zuhair-appointed-director-general-of-trc

62 Niranjala Ariyawansha, "DG and Board of TRC fi ed by President", October 18, 2015, https://www.ceylontoday.lk/51-106844-news-detail-dg-and-board-of-trc-fi ed-by-president.html

63 "Mr. Sunil S. Sirisena is the new Director General of the Telecommunication Regulatory Commission of Sri Lanka", TRC, http://www.trc.gov.lk/mr-sunil-s-sirisena-is-the-new-director-general-of-telecommunications-regulatory-commission-of-sri-lanka.html

64 Jason Burke and Amantha Perera, "Sri Lanka's new president promises 'no more abductions, no more censorship'," *The Guardian*, January 10th, 2015, http://gu.com/p/44n3t/stw.

65 Local internet users reported it was patchily accessible through some fi ed-line and mobile broadband networks during that time. See, Sanjana Hattotuwa, "Tamilnet.com Accessible Once More in Sri Lanka via SLT ADSL".

66 Indika Sri Aravinda, "Police seek mobile porn ban," *Daily Mirror*, May 12, 2010, http://bit.ly/1YgcC4b.

67 Subsidiaries, SLT.lk, https://www.slt.lk/en/about-us/profile/subsidarie , accessed May 2016

peatedly blocked the website Mahinda.info, run by supporters of Mahinda Rajapaksa. The website administrators reported it was blocked several times prior to and after the parliamentary election in August, and said that Mobitel had informed them the blocking was implemented in response to a TRC order.[68] The nature of that alleged order remains unclear, but the possibility that an opposition candidate was censored in advance of elections was troubling, and highlighted the need for legal reform.

Between 20017 and 2015, dozens of websites were blocked at different times, censorship which lacked a legal framework or judicial oversight.[69] Blocks were not properly coordinated or comprehensive, with some targeted websites available at times on one or more ISPs and at other times completely inaccessible. Officials ci ed ill-defined national security measu es to legitimize these measures, though websites were blacklisted for publishing information related to human rights issues, government accountability, corruption, and political violence, including content by Human Rights Watch and Transparency International.[70] During Mahinda Rajapaksa's presidency, censors targeted blogs,[71] opposition and independent news, including Tamil websites, sites run by Sri Lankans in exile, and citizen journalism platforms.

The system that enables website blocking, which has largely operated outside of the law, remains intact. Whilst officials ha e the power to direct the TRC to blacklist content, previous blocks have not had any legal basis and it is not clear whether they were the result of official di ectives or unofficial requests.[72] Under the telecommunications act, ISPs must apply to the Ministry of Telecommunications for a license according to specifications laid out by the T C, who can make recommendations regarding whether or not a license is granted. The ministry can also impose conditions on a license, requiring the provider to address any matter considered "requisite or expedient to achieving" TRC objectives.[73] It is not clear if the TRC can impose other financial or legal penalties on uncooperati e telecommunications companies since the conditions, if imposed, are not transparent. To date, however, no company is known to have challenged the TRC's requests or sought judicial oversight.[74]

There is no independent body in Sri Lanka that content providers can turn to if they are censored. Instead, they must file a fundamental rights application with the Sup eme Court to challenge blocking or other restrictions. Under Rajapaksa's presidency, the lack of trust in the country's politicized judiciary and fear of retaliatory measures represented significant obstacles for the petitione .[75] In December 2011, one settled out of court, agreeing to several TRC conditions—such as removing links to blocked content—in return for restored access.[76]

68 "Mahinda's Webiste Unblocked; Mobitel Says TRC Ordered Blockade", Colombo Telegraph, September 14, 2015, https://www.colombotelegraph.com/index.php/mahindas-website-unblocked-mobitel-says-trc-ordered-blockade/

69 Centre for Policy Alternatives, "Chapter 4: Restriction of Content on the Internet" in *Freedom of Expression on the Internet*, (November 2011), http://bit.ly/1F4D1Mf.

70 Reporters Without Borders, *Internet Enemies*, March 12, 2009, http://bit.ly/tus9bB.

71 Sanjana Hattotuwa, "More websites including ghs.google.com blocked in Sri Lanka?", ICT4Peace, July 29, 2009, https://ict4peace.wordpress.com/2009/07/29/more-websites-including-ghs-google-com-blocked-in-sri-lanka/

72 Insights – Verité Research, "Is blocking websites making telecom share prices vulnerable?," Daily Mirror Business, July 31, 2014, http://www.dailymirror.lk/50418/is-blocking-websites-making-telecom-share-prices-vulnerable

73 Centre for Policy Alternatives, *Freedom of Expression on the Internet*, 30.

74 'Dialog CEO Hans Wijesuriya: "No surveillance program in Sri Lanka, but telecoms have to comply"', *The Republic Square*, September 28, 2013, http://bit.ly/1QkqZOZ.

75 International Crisis Group, "Sri Lanka's Judiciary: Politicised Courts, Compromised Rights," *Asia Report No.172*, June 30, 2009, http://bit.ly/1KsA8oz.

76 S.S. Selvanayagam, "Website previously blocked now permitted to operate by SC," *DailyFT*, December 16, 2011, http://bit.ly/1NFYH3Q.

Content Removal

Documented cases of content removal are few and far between. According to Google's *Transparency Report*, the previous government made four requests for the removal of content over a fi e-year period. The most recent request was submitted in December 2014.[77] Google reported that were no requests for content removal from the current government from January 2015 to May 2016.

Media, Diversity, and Content Manipulation

Despite a history of censorship, there are still diverse, accessible sources of information online in English, Sinhala, and Tamil, including on socioeconomic and political issues. YouTube, Facebook, Twitter, and international blog-hosting services were accessible and widely-used for the anonymous or pseudonymous critique of governance, development, and human rights abuses during the coverage period of this report. Both the presidential and parliamentary elections in 2015 spurred greater activity on social media, particularly as Facebook and Twitter were used to discuss political news, debate key issues and spread awareness about topics pertaining to corruption and governance. Some commentators described the 2015 presidential election as "Sri Lanka's fi st cyber-election" given the increased activity on social media platforms.[78]

The 2015 elections were also noted for how politicians used social media to influence and engage users. The personal pages of President Sirisena and Mahinda Rajapaksa had over 700,000 "likes" after the 2015 parliamentary election. Mahinda Rajapaksa led the way with over 470,000 engaged users (with engagement meaning comments, clicks, shares, post likes, and video plays).[79] During the presidential election Twitter was used most effectively by journalists and one politician – Mahinda Rajapaksa.[80] However, when it came to the parliamentary election in August 2015, politicians published less content on Twitter than journalists and commentators, according to one analysis.[81]

Citizen media site *Groundviews* and its sister site *Vikalpa* feature opinion, news, investigative reports, photography, art, and short videos generated by citizens, covering content that would otherwise not be covered by the mainstream media.[82] In 2014, *Groundviews* announced the launch of *Maatram*, a new citizen journalism initiative that publishes content aimed at Tamil readers across Sri Lanka and the diaspora.[83] The past two years have seen journalism initiatives utilizing mobile messaging platforms to reach new audiences. As a natural progression of its reporting initiative during the elections

77 Google, "Sri Lanka," *Google Transparency Report*, accessed April 13, 2016, https://www.google.com/transparencyreport/removals/government/LK/?hl=en

78 Nalaka Gunawardene, "Social media and General Elections 2015", Daily Mirror, September 2, 2015, http://www.dailymirror.lk/85811/social-media-and-general-elecations-2015

79 "Mapping election influence on social media: art Two – Facebook", Icaruswept (blog), August 19, 2015, http://icaruswept.com/2015/08/19/mapping-election-influence-on-social-media- art-two-facebook/

80 Yudhanjaya Wijeratne, "Who's Been Running the #PresPollSL?", Readme.lk, January 14th, 2015, http://readme.lk/running-prespollsl/

81 "Mapping election influence on social media: art one – Twitter", Icaruswept (blog), August 17, 2015, http://icaruswept.com/2015/08/17/the-general-election-on-social-media-part-one-twitter/

82 "#UPRLKA: Complete Tweet Archive and Related Visualisation Around Sri Lanka's UPR Review," *Groundviews*, November 2, 2012, http://bit.ly/1gupD89.

83 "Announcing the launch of Maatram: Citizen journalism in Tamil," *Groundviews*, January 20, 2014, http://bit.ly/1W52ngY.

in 2014 and 2015,[84] *Groundviews* started enabling mobile updates through WhatsApp in order to publish article updates, audio clips, and pictures.[85]

Other curated websites, largely recent startups, contribute to the country's diverse online media landscape. For example, Readme.lk offers news on technology and Roar.lk, a social content start-up, offers "Sri Lankan content" that it describes as "credible, accessible, readable and shareable."[86] Yamu.lk, a popular city guide, produces short videos on popular culture as well as on socio-economic and political issues, which are viewed and shared widely on social media. Yamu's viewership on Facebook has reportedly doubled every month, from 44,000 views in its fi st month to 720,000 views in February 2016.[87]

During Rajapaksa's presidency, the media ministry issued a directive requesting all "news" websites to register, and a registration fee was ultimately approved at cabinet level in the previous government at LKR 25,000 (US$190) with an annual renewal fee of LKR 10,000 (US$75) and proposed as an amendment to the Press Council Act.[88] These costs threatened to inhibit the emergence of new websites and force existing ones out of operation.[89] While the amendment was never passed, the previous UPFA government still imposed the registration fee through the Ministry of Mass Media without any legal basis.

Despite its explicit media freedom guarantees, the current government made a fresh call for websites to register. In a notice published in the *Daily News*, the government announced that all websites had to be registered with the Ministry of Parliamentary Reforms and Mass Media by March 31, 2016; websites failing to do so would be considered "unlawful."[90] Media freedom activists noted that there is still no legal basis for websites to register with the government. Following considerable pushback from the media and activists, the Acting Minister of Parliamentary Reform and Mass Media Karu Paranavithana stated that the registration drive was not intended to control digital media, but to offer official acc editation, giving web journalism the same recognition as mainstream outlets.[91] Yet Paranavithana undercut this conciliatory message when he justified the go ernment's action with reference to a 2012 Supreme Court ruling, which stated that registration was required in order to prevent the publication of defamatory material on websites, and that freedom of expression was not an absolute right (see Legal Environment).[92]

In May 2014, former President Rajapaksa reaffi med his intent to regulate social media and stated that the government would take the necessary steps to prevent the internet from being used to

84 Sanjana Hattotuwa, "Social media and elections: Sri Lanka's Parliamentary Election, August 2015, *ICT for Peacebuilding*, August 31st, 2015, https://ict4peace.wordpress.com/2015/08/31/social-media-and-elections-sri-lankas-parliamentary-election-august-2015/

85 "Groundviews: Now on Whatsapp", Groundviews, February 23rd, 2016, http://groundviews.org/2016/02/23/groundviews-now-on-whatsapp/

86 Roar.lk, http://roar.lk/about-us/

87 "YAMU TV reports exponential growth in web video", YAMU, April 18, 2016, https://www.yamu.lk/yamu-tvs-press-release/

88 Office f the Cabinet of Ministers – Sri Lanka, "Registration of News Casting Websites – Amendment to the Sri Lanka Press Council Act No 05 of 1973," press brief, August 8, 2012, http://bit.ly/1W53wFf.

89 "Rs.100,000 to be Charged from News Websites," *Daily Mirror*, July 12, 2012, http://bit.ly/1KoO9zk.

90 "Sri Lanka's new regime revives Rajapaksa's censorship of websites," Economy Next, March 2nd, 2016, http://www.economynext.com/Sri_Lanka_s_new_regime_revives_Rajapaksa_s_censorship_of_websites-3-4392-10.html

91 Disna Mudalige, "Not intended to control but to give recognition for web journalists," Daily News, March 3rd, 2016, http://www.dailynews.lk/?q=2016/03/03/local/not-intended-control-give-recognition-web-journalists

92 "IFJ Disappointed by Sri Lanka's Supreme Court Decision on Internet Restrictions", IFJ, May 17, 2012, http://www.ifj.org/nc/fr/news-single-view/browse/255/backpid/237/category/europe-1/article/ifj-disappointed-by-sri-lankas-supreme-court-decision-on-internet-restrictions/

cause "social and political unrest."[93] Under President Sirisena and the new interim government, no attempts have been made to regulate social media as of May 2016.

During Rajapaksa's presidency, officials acti ely encouraged self-censorship "on matters that would damage the integrity of the island," and many mainstream news websites complied, increasing the importance of citizen journalism and exile-run sites in the media landscape.[94] Online platforms of the main state-run newspaper and broadcasting networks supported former President Rajapaksa when he was in power and the UPFA government.[95] These and official go ernment websites have waged smear campaigns against UPFA critics in the past.[96] Under President Sirisena, however, some traditional and new media outlets have become vocal critics of both sides of the political divide, freely expressing opinions and publishing reportage that would have never been tolerated under Rajapaksa's administration. Overall, the practice of self-censorship by journalists and media institutions appears to be diminishing in response to the government's commitment to media freedom, although the media still stay clear of reporting on certain topics, such as controversial issues concerning the military, for fear of reprisals.

While media ethics and responsible reportage are critical issues that need to be addressed, some politicians are quick to criticize media institutions, particularly when inconvenient truths are revealed. For example, in reaction to reports published about the government and the economy, the Minister of Finance Ravi Karunanayake requested media institutions and journalists to avoid abusing the "media freedom that prevails under the new government."[97] A history of government intervention in media freedom meant such statements were cause for concern, even though some of the criticism had foundation. For example, in February 2016, Prime Minister Wickremesinghe threatened to take action against electronic media in response to an offensive description of a performer in a televised opera, especially since licenses to broadcast are issued by the government.[98] Separately, in May 2016, he stated that the greatest threat to media freedom comes from within the media itself. The statement was issued in the context of media reports about the Leader of the Opposition and Tamil National Alliance (TNA) MP, R. Sampanthan, allegedly entering an army camp by force.[99] The TNA said Sampathan only visited private land the camp was located on, which was occupied by the army during the war.[100] The media was criticized for erroneous reporting, including online.

Many pages on Facebook publish offensive material targeting Muslims and other groups.[101] In early

93 P.K. Balachandran, "Social Media To Come Under Watch in Sri Lanka," *The New Indian Express,* May 23, 2014, http://bit.ly/1KsDtE1.

94 Dinidu de Alwis, "Media should exercise self-censorship-Lakshma Yapa," *Ceylon Today*, March 23, 2012, http://bit.ly/1F4G9HU.

95 Milinda Rajasekera, "Namal's disclosure of family embarrassment," *The Island*, December 21, 2011, http://bit.ly/1FPJgy8.

96 World Organization Against Torture, "Sri Lanka: Smear campaign against Ms. Sunila Abeysekara, Ms. Nimalka Fernando, Dr. Paikiasothy Saravanamuttu and Mr. Sunanda Deshapriya," March 27, 2012, http://bit.ly/1LAs55A; Committee to Protect Journalists, "In Sri Lanka, censorship and a smear campaign," July 14, 2009, http://cpj.org/2009/07/in-sri-lanka-censorship-and-a-smear-campaign.php.

97 "Don't abuse the prevailing media freedom – Ravi," *Daily Mirror*, May 26, 2015, http://bit.ly/1FPJB3K.

98 "Ranil condemns Derana TV for calling a woman a 'bitch'; describing the way she sang Danno Budunge", The Island, February 13th, 2016, http://www.island.lk/index.php?page_cat=article-details&page=article-details&code_title=140349

99 "Some media groups pose threat to media freedom: Ranil", The Sunday Times, May 1, 2016, http://www.sundaytimes.lk/160501/news/some-media-groups-pose-threat-to-media-freedom-ranil-191723.html

100 "TNA Says Sampanthan Did Not Forcefully Enter 'Army Camp', Colombo Telegraph, April 27, 2016, https://www.colombotelegraph.com/index.php/tna-says-sampanthan-did-not-forcefully-enter-army-camp/

101 Shilpa Samaratunge and Sanjana Hattotuwa, "Liking Violence: A study of hate speech on Facebook in Sri Lanka," Centre for Policy Alternatives, September 2014, 67-202, http://www.cpalanka.org/liking-violence-a-study-of-hate-speech-on-facebook-in-sri-lanka/.

2013, hate speech against the Muslim community spread online when a Sinhala Buddhist extremist group gained a considerable following on social media.[102] The group's violent rhetoric led to attacks on mosques and Muslim-owned businesses, as well as isolated incidents of assault.[103] No legal action was taken against the group's members, and prominent public officials—including the P esident Rajapaksa's brother, Defense Secretary Gotabhaya Rajapaksa—openly supported them.[104] Some of the relevant social media pages have since been removed, and the intensity of online hate speech declined during the coverage period of this report, though without stopping altogether.

Digital Activism

The web has provided wide scope for robust digital activism and engagement on political issues in Sri Lanka. In the lead up to the January 2015 presidential election, #IVotedSL was launched on Facebook and Twitter – a campaign that called on people to exercise their franchise on election day.[105] Twitter and Facebook profile pho os as well as digital posters were developed and shared by thousands of users, publicizing the campaign and encouraging other users to take the pledge. This campaign continued into the August 2015 parliamentary election with hundreds of people uploading #iwillvote photos on Facebook, Instagram and Twitter. For the fi st time, Facebook allowed all of its users based in Sri Lanka to update their statuses around the August 2015 parliamentary election to indicate whether they were going to vote or had voted on election day.[106]

Following the conclusion of the Presidential election, another independent campaign was initiated by citizens on Facebook and Twitter—#icanChangeSL and #wecanChangeSL—to sustain a meaningful dialogue about shaping a new country.[107] Other interesting initiatives were launched during the coverage period of this report. In March 2016, *Groundviews* launched an initiative to highlight street-based sexual harassment around the country by mapping it on Google Maps and publishing the story behind each incident.[108] Similarly, the Center for Policy Alternatives, a leading public policy institute, launched "Right to the City," an online initiative seeking to broaden the discussion on development, housing, and displacement in Sri Lanka, and anchored to the institute's research and advocacy work on development and rights.[109]

In May 2016, massive floods and landslides caused an estima ed $2 billion worth of damage and claimed 200 lives.[110] The Disaster Management Center (DMC), the main institution responsible for managing disasters, has no active social media presence and still disseminates updates via fax and press releases. Despite having the technology to send SMS alerts to all mobile subscribers in the

102 Sanjana Hattotuwa, "Anti-Muslim hate online in post-war Sri Lanka, "*Sanjana Hattotuwa* (blog), February 1, 2013, http://bit.ly/1F4GA53.

103 Charles Haviland, "The hardline Buddhists targeting Sri Lanka's Muslims," *BBC*, March 25, 2013, http://bbc.in/1UYKiEe.

104 D.B.S. Jeyaraj, "Defence Secretary Gotabhaya Rajapaksa Openly Supportive of "Ethno Religious Fascist" Organization Bodhu Bala Sena," *dbsjeyara* (blog), March 10, 2013, http://dbsjeyaraj.com/dbsj/archives/17939.

105 "#IVotedSL | Exercise your vote on the 8th!," *Groundviews*, January 2, 2015, http://groundviews.org/2015/01/02/ivotedsl-exercise-your-vote-on-the-8th/.

106 Nalaka Gunawardene, "Social Media and General Elections 2015," Dailymirror.lk, September 2, 2015, http://www.dailymirror.lk/85811/social-media-and-general-elecations-2015

107 "icanChangeSL & #wecanChangeSL: Shaping a new Sri Lanka," *Groundviews*, February 4, 2015, http://bit.ly/1zerhBo.

108 Raisa Wickrematunge, "Mapping Street Harassment This Women's Day," March 8, 2016, http://groundviews.org/2016/03/08/mapping-street-harassment-this-womens-day/

109 Center for Policy Alternatives, "Right to the City", https://www.facebook.com/righttothecitysl/

110 Amantha Perera, "After devastating floods and landslides, Sri Lanka plans new building code , IRIN, May 26, 2016, https://www.irinnews.org/news/2016/05/26/after-devastating-floods-and-landslides-sri-lanka-plans-new-building-cod .

country, the DMC has hardly used it.[111] Observers criticized the DMC for missing the opportunity to use digital media to advance its mission, and for failing in its duty to protect the public.[112]

Citizens and organizations, by contrast, used digital tools to organize flood elief efforts, solicit donations, and disseminate information about rescue operations. For example, Sri Lanka Red Cross used its social media accounts to disseminate information regarding floods and landslides; taxi service apps like PickMe introduced a flood elief button for donations and also an SOS button that allowed existing customers trapped in flood-affec ed areas to mark their location for rescue;[113] and Dialog, one of the largest mobile service providers, allowed its customers to donate their loyalty points to flood elief efforts, which the company pledged to double with its own financial contrib - tion. Dialog reported that over LKR 50 million (US$330,000) was donated for flood elief as a result of this initiative.[114]

Violations of User Rights

There were no significant reports of intimidation, prosecution or assault during the coverage period of this report. Physical attacks and threats against journalists, including many linked to government actors, gradually decreased in the aftermath of the civil war. Whilst the failure to investigate past incidents cast a long shadow during President Rajapaksa's rule, the new government under President Sirisena has promised to initiate investigations into the murder and disappearance of journalists. The progress of these investigations has been described as "agonizing."

Legal Environment

While the right to freedom of speech, expression, and publishing is guaranteed under Article 14(1) (a) of Sri Lanka's constitution, it is subject to numerous restrictions for the protection of national security, public order, racial and religious harmony, and morality. There is no constitutional provision recognizing internet access as a fundamental right or guaranteeing freedom of expression online. A culture of impunity, circumvention of the judicial process through arbitrary action, and a lack of adequate protection for individuals and their privacy, compound the poor enforcement of freedom of expression guarantees.

The Supreme Court has called freedom of expression from "diverse and antagonistic sources" indispensable to democracy.[115] In May 2012, however, it rejected a fundamental rights petition brought by members of the local Free Media Movement questioning the media ministry's right to block websites for failure to register.[116] After a complaint was made to the Human Rights Commission of Sri Lanka about the blocking of two websites in May 2014, the commission said it would investigate, but that freedom of expression was subject to constitutional limits.[117]

111 Amantha Perera, "With Social Media, we could have saved more lives", Reuters, May 25, 2016, http://in.reuters.com/article/sri-lanka-landslide-socialmedia-idINKCN0YG13C

112 "Arming against disasters", *Daily News*, June 10, 2016, http://www.dailynews.lk/?q=2016/06/10/features/84270

113 "PickMe's SOS feature breaks new ground", *The Island*, May 24, 2016, http://island.lk/index.php?page_cat=article-details&page=article-details&code_title=145788

114 Dialog, Flood Relief, http://sm.dialog.lk/relief/

115 Centre for Policy Alternatives, *Freedom of Expression on the Internet in Sri Lanka,* (August, 2010), 54, http://bit.ly/1gutuCa.

116 Bob Dietz, "Sri Lanka Supreme Court slams door on websites," *Committee to Protect Journalists* (Blog), May 17, 2012, http://cpj.org/x/4bb2.

117 Waruni Karunarathne, "HRC To Study Complaint on Websites", *The Sunday Leader*, May 25, 2014, http://bit.ly/1W55qWs.

Several laws with overly broad scope lack detailed definitions and can be abused o prosecute or restrict legitimate forms of online expression. Computer crimes and intellectual property rights laws allow information contained within computers to be admissible in civil and criminal proceedings. Publishing official sec ets, information about parliament that may undermine its work, or "malicious" content that incites violence or disharmony could result in criminal charges.[118]

The Press Council Act No.5 of 1973 had lain dormant under previous administrations until the Rajapaksa regime reactivated it after the end of the war.[119] The act prohibits the publication of profanity, obscenity, "false" information about the government or fiscal polic , and official sec ets. It also allows the president-appointed council to impose punitive measures on the violators of its provisions, including possible prosecution. Six months after his victory at the presidential election, President Sirisena used his executive powers to reactivate the Press Council and appoint three members to it.[120] The move was criticized by publishers, media activists, editors and journalists, who argued that it contradicted President Sirisena's election promise to protect media freedom.[121] Since 2009, local and international media rights organizations have constantly opposed the Press Council Act.[122]

In April 2015, President Sirisena proposed legislation in order to ban hate speech and material that could "exacerbate religious and ethnic tensions."[123] The UN High Commissioner for Human Rights has encouraged the government to address hate speech and religious violence.[124] The Minister of Justice tabled two new bills in parliament, which added a new offence regarding hate speech into the Sri Lankan Penal Code and the Criminal Procedure Code. However, an existing law, the International Covenant of Civil and Political Rights (ICCPR) Act No. 56 of 2007, already prohibits anyone from advocating national, racial, and religious hatred that might be an incitement to discrimination, hostility, or violence.[125] In addition, the new offence outlined in the bills replicates Section 2(1)(h) of the Prevention of Terrorism Act (PTA) of 1979,[126] which was used by Rajapaksa's government to prosecute critics like J.S. Tissainayagam, who was detained for over a year and sentenced to 20 years' imprisonment hard labor in 2009 on charges of causing racial hatred and raising money for terrorism.[127] Moreover, the overbroad provisions of the legislation left it open to manipulation to restrict legitimate forms of expression. The Tamil National Alliance (TNA), the Human Rights Commission

118 Respective legislation: Official Sec ets Act No. 32 of 1955; Parliament (Powers and Privileges) (Amendment) 1997; Prevention of Terrorism (Temporary Provisions) Act No. 48 of 1979.

119 "Press Council Reactivated", *The Sunday Times*, June 14th, 2009, http://www.sundaytimes.lk/090614/News/sundaytimesnews_10.html

120 "Media groups slam Sirisena for bringing back Press Council", *The Sunday Times*, July 5, 2015, http://www.sundaytimes.lk/150705/news/media-groups-slam-sirisena-for-bringing-back-press-council-155671.html

121 "Media Release on Press Council Act". Sri Lanka Press Institute, January 21st, 2016, http://www.slpi.lk/media-release-on-press-council-act/

122 "IFJ, Sri Lankan media rights organizations object to reactivation of Press Council", IFJ, July 6, 2015, http://www.ifj.org/nc/news-single-view/browse/3/backpid/33/article/ifj-sri-lankan-media-rights-organizations-object-reactivation-of-press-council/

123 Sanjaya Jayasekera, "Sri Lankan government to pass laws banning "hate speech"," *World Socialist Web Site*, April 20, 2015, http://bit.ly/1YglQxt.

124 "Statement by UN High Commissioner for Human Rights Zeid Ra'ad al Hussein via videolink to the Human Rights Council", OHCHR, September 15th, 2015, http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=16539&LangID=E

125 Section 3, International Covenant on Civil and Political Rights Act No. 56 of 2007, November 16, 2007, http://www.documents.gov.lk/Acts/2007/International%20Covenant%20on%20Civil%20&%20Political%20Rights%20%28Iccpr%29%20-%20Act%20No.%2056/English.pdf

126 Section 2(1)(h) of the Prevention of Terrorism Act of 1979 states "(h) by words either spoken or intended to be read or by signs or by visible representations or otherwise causes or intends to cause commission of acts of violence or religious, racial or communal disharmony or feelings of ill-will or hostility between different communities or racial or religious groups" shall be guilty of an offence under the act.

127 "Sri Lankan president pardons convicted Tamil editor", BBC News, May 3rd, 2010, http://news.bbc.co.uk/2/hi/south_asia/8657805.stm

and civil society groups opposed the proposed laws.[128] Petitions were also filed with the Sup eme Court in order to challenge the laws.[129] After considerable opposition, the government withdrew the bills.[130] Legal scholars argue that enforcing the ICCPR Act, which abides by international standards, is adequate enough for "advancing justice and preventing future religious violence."[131]

The current government also announced that it would be drafting new laws to respond to the growing rate of cybercrime. In the fi st seven months of 2015, there were over 2,000 complaints regarding fake social media profiles. The Compu er Crimes Division of the Criminal Investigations Department (CID) has investigated over 100 internet-related crimes, which includes cases of defamation, obscene content, and email hacking.[132]

After months of political bargaining, Parliament passed the 19th Amendment to the Constitution in April 2015. The amendment strengthened checks and balances on the executive presidency, restored term limits to the presidency, revived the Constitutional Council, and empowered independent commissions.[133] In January 2016, the Public Representations Committee (PRC), appointed by the Cabinet of Ministers to receive public representations on constitutional reform, began its public sittings around the country and published a final eport in May 2016.[134] The Prime Minister also presented a resolution to convert Parliament into a Constitutional Assembly for the purpose of enacting a new Constitution.[135] In April 2016, Parliament convened for the fi st time as the Constitutional Assembly in order to discuss the fi st steps required to draft a new Constitution.[136]

Following the passage of a resolution titled "Promoting Reconciliation, Accountability and Human Rights in Sri Lanka", which it co-sponsored at the United Nations Human Rights Council, Sri Lanka initiated a transitional justice process with the appointment of the Consultation Task Force on Reconciliation Mechanisms (CTF) in January 2016. It will present a report in October 2016.[137]

Right to Information (RTI) is another legislative development that has been undertaken by the Government during the coverage period of this report. The fi st RTI bill was proposed in 2003, but was ultimately rejected by parliament. As part of President Sirisena's 100-day program, the new government promised to introduce RTI legislation in order to entrench good governance and transparency. Whilst the passage of the 19th Amendment to the Constitution recognizes RTI as a fundamental

128 "TNA wants new 'hate speech' legislation withdrawn", *Daily News*, December 16, 2015, http://www.dailynews.lk/?q=2015/12/16/political/tna-wants-new-hate-speech-legislation-withdrawn

129 "Two petitions filed in SC against Govt. amendments o Penal Code on hate speech", *DailyFT*, December 16, 2015, http://www.ft.lk/article/509053/Two-petitions-in-SC-against-Govt--amendments-to-Penal-Code-on-hate-speech

130 "Govt backs away from bills claimed to bar free speech", The Sunday Times, December 20, 2015, http://www.sundaytimes.lk/151220/news/govt-backs-away-from-bills-claimed-to-bar-free-speech-175994.html

131 Gehan Gunatilleka, "Hate Speech in Sri Lanka: How a New Ban Could Perpetuate Impunity", OHRH, January 11, 2016, http://ohrh.law.ox.ac.uk/hate-speech-in-sri-lanka-how-a-new-ban-could-perpetuate-impunity/

132 Nushka Nafeel, "New laws to curb cyber crimes", Daily News, November 6, 2015, http://www.dailynews.lk/?q=2015/11/05/features/new-laws-curb-cyber-crimes-0

133 "A Brief Guide to the Nineteenth Amendment to the Constitution", May 2015, Centre for Policy Alternatives, https://www.cpalanka.org/wp-content/uploads/2015/05/A-Brief-Guide-to-the-Nineteenth-Amendment.pdf

134 Report on Public Representations on Constitutional Reform, May 2016, http://www.yourconstitution.lk/PRCRpt/PRC_english_report-A4.pdf

135 T. Ramakrishnan, "Resolution passed to convert Sri Lankan Parliament into Constitutional Assembly", *The Hindu*, March 10, 2016, http://www.thehindu.com/news/international/resolution-passed-to-convert-sri-lankan-parliament-into-constitutional-assembly/article8332294.ece

136 "Sri Lanka parliament appoint members to committees at the fi st sitting of Constitutional Assembly", *Colombo Page*, April 6, 2016, http://www.colombopage.com/archive_16A/Apr06_1459923593CH.php

137

right, Parliament had yet to pass the legislation for it.[138] In December 2015, the cabinet approved the "Right of Access to Information" bill—following which, the government announced that the bill would be gazetted, circulated amongst the provincial councils and tabled in parliament during the fi st quarter of 2016.[139] The bill is expected to strengthen accountability, improve governance and increase transparency within public institutions. In March 2016, the government finally tabled the TI bill in parliament.[140]

Civil society activists flagged serious conce ns about the drafts,[141] notably for lack of consideration for information surrounding victims of enforced disappearances.[142] In April 2016, Transparency International Sri Lanka said it supported the current version of the bill, while identifying six areas that could be further strengthened.[143]

However, also in April 2016, multiple fundamental rights petitions were filed with the Sup eme Court, challenging the constitutionality of several clauses in the bill.[144] Civil society activists also filed fund - mental rights petitions in defense of the bill. After hearing all of the petitions,[145] the Supreme Court determined that fi e sections of the bill were inconsistent with the Constitution of Sri Lanka.[146] The Government stated that it would consider the Court's determination before moving ahead. Soon after, the Government announced that it would be accepting all amendments to the RTI bill stipulated by the Supreme Court since they further strengthened the bill.[147] In May 2016, the amended RTI bill had not yet been taken up for further debate in Parliament.

Prosecutions and Detentions for Online Activities

No detentions for online activity were reported during the coverage period of this report. Detentions for legitimate online activity were documented during Rajapaksa's presidency. In one egregious 2012 example, CID officials raided the ffices f the *Sri Lanka Mirror* and *Sri Lanka X News* websites in June on grounds of "propagating false and unethical news on Sri Lanka."[148] The journalists were

138 Uditha Kumarasinghe, "Week in Parliament: 19th Amendment a victory for all", *Sunday Observer*, May 3rd, 2015, http://bit.ly/1KjMax7.

139 Namini Wijedasa, "Right to Information Bill to be gazetted soon", *The Sunday Times*, December 6th, 2015, http://www.sundaytimes.lk/151206/sports/right-to-information-bill-to-be-gazetted-soon-174329.html

140 "RTI bill presented in Sri Lankan Parliament", Business Standard News, March 24, 2016, http://www.business-standard.com/article/pti-stories/rti-bill-presented-in-lanka-parliament-116032400454_1.html

141 Lionel Guruge, "The 20th Amendment, Right to Information, and Audit Act," *The Sunday Leader*, May 31, 2015, http://bit.ly/1guvURj; "Strenghtening RTI", DailyFT, March 5th, 2016, http://www.ft.lk/article/529323/Strengthening-RTI

142 Gehan Gunatilleke, "The Struggle for Right to Information in Sri Lanka", *Oxford Human Rights Hub*, April 13, 2016, http://ohrh.law.ox.ac.uk/the-struggle-for-right-to-information-in-sri-lanka-is-it-leaving-victims-behind/

143 "Sri Lanka: Transparency International Sri Lanka supports RTI bill as it stands", *Colombo Page*, April 10th, 2016, http://www.colombopage.com/archive_16A/Apr10_1460269853CH.php.

144 "Three petitions in SC against RTI bill", *The Sunday Times*, April 3rd, 2016, http://www.sundaytimes.lk/160403/news/three-petitions-in-sc-against-rti-bill-188565.html

145 T. Ramakrishnan, "Sri Lanka's RTI Bill: Government to study Supreme Court's suggestions", *The Hindu*, May 7, 2016, http://www.thehindu.com/news/international/sri-lankas-rti-bill-government-to-study-supreme-courts-suggestions/article8569983.ece; Venkatesh Nayak, "The Supreme Court of Sri Lanka suggests changes to the RTI bill to facilitate easy passage through Parliament", CHRI, May 11, 2016, http://www.humanrightsinitiative.org/blog/the-supreme-court-of-sri-lanka-suggests-changes-to-the-rti-bill-to-facilitate-easy-passage-through-parliament.

146 "Sri Lanka RTI Bill Needs Two Thirds Majority – SC; Five Sections Inconsistent with the Constitution", *Sri Lanka Brief*, May 4, 2016, http://srilankabrief.org/2016/05/sri-lanka-rti-bill-needs-two-thirds-majority-sc/

147 P.K. Balachandran, "Lankan Government to Amend RTI Bill as Per Supreme Court's Suggestions", *The New Indian Express*, May 3, 2016, http://www.newindianexpress.com/world/Lankan-Government-To-Amend-RTI-Bill-as-Per-Supreme-Courts-Suggestions/2016/05/03/article3413594.ece

148 "Websites propagating false news sealed—MOD," *Daily Mirror*, June 30, 2012, http://bit.ly/1KTIWG0.

released on bail the day after their arrest, though investigators later said their computers contained further grounds for prosecution, including content that violated the Obscene Publications Act—although the alleged obscenity was unpublished[149]—failure to register the website, ridiculing the president, and evidence of an attempted coup.[150] While the case was finally set aside due to the CID failing to conclude investigations, the journalists filed a fundamental rights petition with the Supreme Court citing illegal arrest, violation of their right to free expression, and their profession.[151] Supreme Court hearings on the petition were ongoing in 2015.[152]

Surveillance, Privacy, and Anonymity

In spite of the new government's commitment to freedom of expression, transparency and right to information, privacy advocates are still cautious about how existing surveillance technology could be utilized and intensified in the future. Civil society groups also fear that website registration could be used to hold registered site owners responsible for content posted by users, or to prevent government critics writing anonymously.[153]

Sri Lanka lacks substantive laws for the protection of individual privacy and data. Extrajudicial surveillance of personal communications is prohibited under the Telecommunications Act No.27 of 1996. However, a telecommunications officer can intercept communications under the direction of a minister, a court, or in connection with the investigation of a criminal offence. There is no provision under the legislation that requires officials to notify users who are targets of surveillance, and under the previous government, many journalists and civil society activists believed their phone and internet communications were monitored, particularly in light of official statements lauding state surveillance.[154] Security surveillance in the north and east still continues.[155]

In 2013, Dialog CEO Dr. Hans Wijesuriya denied the existence of a comprehensive surveillance apparatus in Sri Lanka but agreed that telecommunications companies "have to be compliant with requests from the government."[156] Digital activists in Sri Lanka believe Chinese telecoms ZTE and

149 Farook Thajudeen, "Pornographic material from Sri Lanka Mirror computers—CID," *Daily Mirror*, July 23, 2012, http://bit.ly/1KsHtVf.

150 Binoy Suriyaarachchi, "SL Mirror computers returned," *Ceylon Today*, September 18, 2012, http://www.ceylontoday.lk/13044-print.html.

151 T. Farook Thajudeen, "Sri Lanka Mirror case set aside," *Daily FT*, September 19, 2012, http://www.ft.lk/2012/09/19/sri-lanka-mirror-case-set-aside/.

152 "When the CID raided Sri Lanka Mirror", *Sri Lanka Mirror*, June 30, 2015, http://srilankamirror.com/news/item/4858-when-the-cid-raided-sri-lanka-mirror

153 Centre for Policy Alternatives, "Arbitrary Blocking and Registration of Websites: The Continuing Violation of Freedom of Expression on the Internet," press release, November 9, 2011, http://bit.ly/1guxKkU.

154 "It's ok for government to infiltrate online privacy of Sri Lankan citizens?," *ICT for Peacebuilding* (blog), April 17, 2010, http://bit.ly/1UYLuaC.

155 Ruki Fernando, "Tamils in North & East remember those killed despite intimidation and surveillance," *Groundviews*, May 20, 2015, http://groundviews.org/2015/05/20/tamils-in-north-east-sri-lanka-remember-those-killed-despite-intimidation-and-surveillance/.

156 'Dialog CEO Hans Wijesuriya: "No surveillance program in Sri Lanka, but telecoms have to comply".

Huawei, who collaborated with Rajapaksa's government in the development and maintenance of Sri Lanka's ICT infrastructure, may have inserted backdoor espionage and surveillance capabilities.[157]

During the coverage period of this report, journalists analyzed leaked documents which revealed that the Milan-based fi m Hacking Team was approached by several state security agencies on a number of occasions to acquire the company's digital surveillance technologies.[158] The leaks revealed that in March 2014 the Ministry of Defense was planning on developing an electronic surveillance and tracking system with the help of a local university.[159] While no purchases of the company's equipment were confi med in the published documents, they included a 2013 email exchange between a Hacking Team employee and individual claiming to represent Sri Lankan intelligence agencies describing confidential acquisitions of "interception technologies" he had brokered in the past.[160]

Under the Rajapaksa regime, a Ministry of Defense program to register mobile phone users for the purpose of "curbing negative incidents" was introduced in 2008 and revisited in 2010 after service providers failed to ensure that subscribers registered.[161] Real-name subscriptions are already normal procedure, but the call for registration in 2010 required further information, including photo identification and up- o-date residential details. Unregistered users risked disconnection if they failed to comply, though no cases were reported.

Intimidation and Violence

There were no targeted attacks on online journalists or internet users during the coverage period of this report.

Online reporters, like their counterparts in traditional media, were attacked by forces on both sides during Sri Lanka's civil conflict. Unsol ed cases include the 2005 murder of *TamilNet* co-founder Dharmeratnam Sivaram, who was found dead in a high-security area outside parliament.[162]

The trend of violence against traditional journalists and a culture of impunity as well as intimidation continued during Rajapaksa's presidency despite sustained international pressure. International news reports and rights groups say soldiers acting on the orders of high ranking officials in the p evious

157 ZTE Corporation signed an agreement with Mobitel to develop its 4G LTE network and carried out successful trials in May 2011, while SLT's ADSL infrastructure is supported by Huawei. See, ZTE, "Sri Lanka's Mobitel and ZTE Corporation Carry Out the First Successful 4G(LTE) Trial in South Asia," news release, May 17, 2011, http://wwwen.zte.com.cn/pub/en/press_center/news/201105/t20110517_234745.html; Ranjith Wijewardena, "SLT Tie Up With Huawei to Expand Broadband Internet Coverage," *The Island*, September 29, 2006, http://www.island.lk/2006/09/29/business11.html; Sanjana Hattotuwa, "Are Chinese Telecoms acting as the ears for the Sri Lankan government?," *Groundviews*, February 16, 2012, http://groundviews.org/2012/02/16/are-chinese-telecoms-acting-as-the-ears-for-the-sri-lankan-government/; "The President of Sri Lanka His Excellency Mahinda Rajapaksa holds discussions with Huawei Chairwoman Ms. Sun Yafang, Expressing thanks and acknowledgement on Huawei's contribution to ICT industry and Education locally," *Lanka Business Today*, May 27, 2014, http://pr.huawei.com/en/news/hw-340356-ict.htm#.Vg2CUvlVhBc.

158 "Hacking the hackers: Surveillance in Sri Lanka revealed", *Groundviews*, July 15, 2015, http://groundviews.org/2015/07/15/hacking-the-hackers-surveillance-in-sri-lanka-revealed/

159 "Wikileaks – The Hackingteam Archives", https://wikileaks.org/hackingteam/emails/emailid/238000

160 "Wikileaks – The Hackingteam Archives", https://wikileaks.org/hackingteam/emails/emailid/577225

161 Bandula Sirimanna, "Sri Lanka to tighten mobile phone regulations," *The Sunday Times*, October 31, 2010, http://bit.ly/1UYM0FC.

162 Committee to Protect Journalists, "Journalists Killed, Sri Lanka: Dharmeratnam Sivaram," April 29, 2009, http://bit.ly/1KsU0YC.

government were responsible for the notorious "white van" abductions of critics and activists[163]—named after the vehicle often used to carry them out—a claim the previous administration denies.[164]

In May 2015, President Sirisena reiterated his intention to re-open investigations into all past murders and disappearances of journalists.[165] There are some signs of progress. In February 2016, fi e intelligence personnel were arrested in the case of Prageeth Eknaligoda.[166] The *Lanka-E-News* journalist and cartoonist has been missing since January 24, 2010, after the website backed the political opposition in elections;[167] in the past, officials said he sought asylum o erseas.[168] The suspects are alleged to have connections with the military and intelligence services, and numerous others have been detained during the course of the investigations. In May 2016, the case was ongoing. Other investigations have yet to move forward.[169]

Technical Attacks

Cybercrime is a growing problem in Sri Lanka, with illegal breaches of social media and email accounts becoming more common.[170] Cyberattacks have also targeted critics of Rajapaksa's regime in the past, though no incidents were reported during the coverage period.

The previous government recognized the need to strengthen its defensive capability, yet critics fear technology bought for this purpose could be used to restrict legitimate expression.[171] Following the implementation of the Computer Crimes Act in 2007, the government at the time established the Computer Emergency Readiness Team and Coordination Center (CERT|CC) in order to protect Sri Lanka's digital data. In July 2014, CERT|CC developed a security arm to protect digital banking infrastructure.[172] The CID has also established a Hi-Tech Crime Investigation Unit (HCIU) in order to fight cyber crime a ound the country and not just in the commercial capital, Colombo. The HCIU will be investigating the sexual harassment of women on social media, threats to minors, and cases of financial fraud online [173]

163 "A disappearance every fi e days in post-war Sri Lanka," *Groundviews,* August 30, 2012, http://bit.ly/1YgI6qV.

164 Krishan Francis, "Abduction squads in Sri Lanka target foes of powerful, "*The Washington Times*, August 22, 2012, http://bit.ly/1LAAeXF.

165 "Want to Re-Open Investigations on Attacks on Media: Sri Lankan President Maithripala Sirisena," *NDTV/Press Trust of India*, May 30, 2015, http://bit.ly/1QkO3NM.

166 "Sri Lanka's Rajapaksa family: Crashing fall from grace", BBC News, February 5, 2016, http://www.bbc.com/news/world-asia-35505995

167 T. Farook Thajudeen, "Prageeth Eknaligoda disappearance case still ongoing," *Daily FT*, December 24, 2011, http://bit.ly/1iSm39L;Bob Dietz, "UN Heard Eknelygoda's cry for help; husband still missing," *Committee to Protect Journalists* (Blog), May 21, 2011, http://bit.ly/Gzv9o2.

168 Chris Kamalendran, "Eknaligoda Case: Focus on ex-AG," *The Sunday Times*, December 11, 2011, http://sundaytimes.lk/111211/News/nws_24.html.

169 Scott Griffen,"In Sri Lanka, media settle in for long march to change", International Press Institute, February 1, 2016, http://www.freemedia.at/newssview/article/feature-in-sri-lanka-media-settle-in-for-long-march-to-change.html; Thilaka Sanjaya, "Feet-dragging over Lasantha's grave", *Sunday Observer*, January 17, 2016, http://www.sundayobserver.lk/2016/01/17/sec04.asp.

170 "681 SL cyber security incidents so far in 2011," *The Sunday Times*, October 16, 2011, http://www.sundaytimes.lk/111016/BusinessTimes/bt31.html.

171 Centre for Policy Alternatives, *Freedom of Expression on the Internet*, 42.

172 Data and Information Unit of the Presidential Secretariat of Sri Lanka, "CSIRT system launched in Sri Lanka to prevent cyber attacks on banks," July 2, 2014, http://www.priu.gov.lk/news_update/Current_Affairs/ca201407/20140702csirt_system_launched_sl_prevent_cyber_attacks_banks.htm.

173 Damith Wickremasekera, "CID to fight cyber crime with Hi- ech Crime Investigation Units", *The Sunday Times*, November 1, 2015, http://www.sundaytimes.lk/151101/news/cid-to-figh -cyber-crime-with-hi-tech-crime-investigation-units-169982.html

Freedom House

Sudan

	2015	2016
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	18	16
Limits on Content (0-35)	19	18
Violations of User Rights (0-40)	28	30
TOTAL* (0-100)	**65**	**64**

* 0=most free, 100=least free

Population:	**40.2 million**
Internet Penetration 2015 (ITU):	**27 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- There were no reports of deliberate internet shutdowns in Sudan during the coverage period, marking an improvement from the previous period when a fi e-day internet blackout was reported in the West Darfur region of Sudan (see **Availability and Ease of Access**).
- In February 2016, the authorities raided 130 internet cafes in Khartoum in search of content threatening "public morals" (see **Surveillance, Privacy, and Anonymity**).
- Revisions to the 2004 Press and Printed Press Materials Law were introduced in 2015 with the aim of regulating online media and providing a legal framework to prosecute online journalists (see **Legal Environment**).
- Arrests and prosecutions under the IT Crime Act grew in the past year, reflecting a tactical shift in the government's strategy to limit internet freedom (see **Prosecutions and Detentions for Online Activities**).

Introduction

Internet freedom in Sudan improved marginally in 2015-16 due to the lack of internet shutdowns and content restrictions experienced in previous years, despite a rise in arrests and prosecutions.

The Sudanese government has shifted tactics over the past year, as users increasingly turned to digital platforms to exchange news and opinions in the face of a repressive media environment. There were no blocks on political or social websites reported during the coverage period—in contrast to "immoral" content, which remained systematically blocked—while social media and communications platforms were freely available. WhatsApp has become particularly popular among Sudanese, who have turned to the platform's relative privacy and anonymity to share critical news via the app's group chat function.

Nonetheless, independent online news outlets were subject to frequent technical attacks, which many believe were perpetrated by the Cyber Jihadist Unit, the government's army of trolls. Several users were arrested with the intent of creating a chilling effect online, although no individuals faced trial on legal charges. While several restrictive laws can be applied to penalize online activities, including the 2007 IT Crimes Act, the Sudanese government introduced revisions to the 2004 Press and Printed Press Materials Law in 2015 with the aim of regulating online media and providing a legal framework to prosecute online journalists.

Obstacles to Access

Access to the internet continued to be a challenge for Sudanese citizens in 2015-2016 as a result of economic challenges, increasing costs, and declining quality of services. Mobile phone penetration declined slightly from the previous year, while technical issues with submarine cables disrupted internet access for a number of subscribers.

Availability and Ease of Access

Access to the internet became more challenging for Sudanese citizens during the coverage period amid declining quality and speeds, and increasing costs. Internet penetration stood at 27 percent in 2015, growing incrementally from 25 percent in 2014, while mobile phone penetration declined slightly from 72 percent to 71 percent, according to the International Telecommunications Union (ITU).[1]

The country's staggering economy has created an expensive operating environment for the ICT sector, impacting both telecom companies and their subscribers. In early 2016, Zain, the telecom operator with the largest market share, canceled its daily unlimited internet bundle services and instead increased prices on select data bundles by up to 300 percent.[2] Making matters worse, its newly introduced bundles did not deliver on advertised speeds, forcing subscribers to purchase additional

1 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," and "Mobile-Cellular Telephone Subscriptions, 2000-2015," http://bit.ly/1cblxxY.

2 "A storm of discontent in Sudan following Zain's increase of Internet service prices," [in Arabic] Al-hayat, February 3, 2016, http://bit.ly/1Y30qST; "Sudanese boycott a telecommunications company for increasing Internet tariff by 300%," Alquds, February 3, 2016, bit.ly/21XNVua. Coverage of Zain's CEO press conference, Alyoum Altali, February 21, 2016, bit.ly/1WgoMra.

data more frequently than anticipated[K][P] Mobile providers pointed to high licensing and registration fees and the proliferation of internet-enabled voice and messaging services that have disrupted their traditional revenue flows as justification for price in eases.

Users organized boycott campaigns against the price increases and contested fair usage policies as well as declines in speed quality.[Q] Average connection speeds were registered as 2.1 Mbps by Akamai's 2016 "State of the Internet" fi st quarter report, significantly lo er than the global average of 6.3 Mbps.[R] Internet speeds outside Khartoum are remarkably lower than the country's average, especially during peak hours.[S]

In contrast to rising mobile data rates, the cost of internet access at cybercafés dropped slightly during the coverage period to SDG 2-3 (around USD 0.40) per hour, perhaps due to decreasing visitors. Cybercafés have become less popular in recent years due to increasing access via mobile devices, as well as pervasive surveillance and policing of immoral activities at cybercafés (see Intimidation and Violence). In 2016, many cybercafés were used mainly for printing or during emergencies.

Electricity shortages also limit internet services in Sudan, compounded by recent oil price hikes that have led to outages across the country.[7] Only 35 percent of the population has access to electricity,[8] and the current crisis has reduced the electricity supply by 40 percent.[9]

Furthermore, approximately 1.4 million citizens living in rebel-controlled areas in South Kordofan have extremely limited access to basic services and the internet.[10] Nearly 3.2 million internally displaced persons (IDPs) living in camps as of December 2015 have no access whatsoever.[11] In the rebel-controlled Nuba Mountains region of the country, the Sudan People's Liberation Movement-North (SPLM-N) rebel government issued a directive in August 2015 banning citizens from accessing the internet to prevent information from leaking to the central government, allowing access to only government officials and NGO affili es.[12]

Restrictions on Connectivity

Sudan connects to the global internet through three international gateways controlled by the partly state-owned Sudan Telecom Company (Sudatel), Zain, and Canar TelecomI[N][P] which are in turn connected to four submarine cables: Saudi Arabia-Sudan-1 (SAS-1), Saudi Arabia-Sudan-2 (SAS-2), Eastern Africa Submarine System (EASSy), and FALCON.[N][Q] Partial control over the international

3 Author's interview, May 2016.

4 "Boycott campaign in Sudan targets telecom companies to compel better service," *Sudan Tribune,* July 3, 2015, http://bit.ly/1p7OJ1L

5 Akamai, "Average Connection Speed," map visualization, *State of the Internet, Q1 2016,* accessed March 4, 2016, http://akamai.me/1LiS6KD.

6 " NTC inquires Zain to explain the deterioration of Internet service," *Sudan Tribune*, July 4, 2015, http://bit.ly/1Sr1P5q

7 "Fuel shortage blamed for recent power outages in Sudan," *Sudan Tribune*, March 10, 2015, http://bit.ly/1YgFjN7

8 "Seeking Alterative Energy in Sudan: UNDP and the Ministry Of Water Resources Initiate the Use of Wind Power in Sudan –A 200 Million Dollar Project," UNDP Sudan, Dec 4, 2014**,** http://bit.ly/1UIVmUb

9 "Sudan aspires to increase electricity production by 2020," *Sudan Tribune*, August 2, 2015, http://bit.ly/1UIXBqi

10 See "Mayors in Sudan's South Kordofan demand no-fly zone" Radio Dabanga, February 24, 2014, http://bit.ly/1RkJ8gf, and UNHCR, "Sudan," 2015, http://www.unhcr.org/pages/49e483b76.html

11 OCHA: Sudan: Humanitarian Bulletin | Issue 08 | 15 – 21 February 2016 [EN/AR], http://bit.ly/1EaK287

12 "SPLM-N limits Internet access in Nuba Mountains," *Radio Tamazuj*, August 19, 2015, https://radiotamazuj.org/en/article/splm-n-limits-internet-access-nuba-mountains

13 Doug Madory, "Internet Blackout in Sudan," Dyn Research, September 25, 2013, http://bit.ly/1QN46V3

14 Check interactive, Huawei Marine Networks, "Submarine Cable Map for Sudan," http://bit.ly/1ZRMhKz

gateway has enabled the government to restrict internet connectivity during particular events in the past. For example, internet access was shut down for fi e days in the West Darfur region in August 2014, and nationwide for nearly 24 hours in September 2013 during massive protests across the country.[15]

While the government did not impose largescale restrictions over the past year, Zain's broadband network was intermittently disrupted during a period of 12 hours in January 2016.[16] Zain attributed the disruption to technical glitches. In separate incidences that month, the SEACOM broadband submarine cable near Egypt was temporarily cut, affecting 65 percent of Canar's broadband users, while access for Sudani subscribers was reportedly disrupted for fi e days.[17]

ICT Market

There are four licensed telecommunications operators in Sudan: Zain, MTN, Sudatel, and Canar. All are fully owned by foreign companies with the exception of Sudatel, in which the government owns a 22 percent share.[18] However, the Sudanese government holds significant sway o er Sudatel's board of directors, which includes high-ranking government officials [19]

Two providers, MTN and Sudatel, offer broadband internet, while Canar offers fi ed phone lines and home internet. Emirati-owned Canar was denied a license to provide mobile services in February 2016, demonstrating the lack of competition in the sector.[20] The Bank of Khartoum subsequently purchased Canar from UAE's Etisalat in June 2016, after the bank used its 3.7 percent share in Canar to block Zain's efforts to purchase it. Observers believe the government's move to increase its market share of the telecom industry will have a negative impact on internet freedom for Sudanese users.

Regulatory Bodies

Sudan's telecoms sector is regulated by the National Telecommunications Corporation (NTC), which is housed under the Ministry of Telecommunications and Information Technology. The NTC is tasked with producing telecommunications statistics, monitoring the use of the internet, introducing new technology into the country, and developing the country's telecommunications and IT industry. It is also responsible for deciding what content should be accessible on the internet. Although it is a state body, the NTC receives grants from international organizations such as the Intergovernmental Authority on Development and the World Bank, and its website describes the body as "self-finan ing."

15 See Freedom House, "Sudan," *Freedom on the Net 201*, http://bit.ly/1M2wVig

16 "Zain Sudan Internet cut," *Alwatan*, January 14, 2016

17 "Submarine cable cut causes weakens Internet in Sudan," *Sudan Tribune*, January 27, 2016, http://bit.ly/29MPETk; "SEACOM IS EXPERIENCING A CRITICAL OUTAGE – 16:30 GMT," *SEACOM*, January 21, 2016, http://bit.ly/1nbKeld; "NOT ONE, BUT TWO SA INTERNET CABLES WENT DOWN LAST NIGHT," htxt.Africa, January 22, 2016 http://bit.ly/2a8izQP

18 Rupa Ranganathan and Cecilia Briceno-Garmendia, *Sudan's Infrastructure: A Continental Perspective*, Africa Infrastructure Country Diagnostic, (Washington, D.C.): World Bank, June 2011), http://bit.ly/1OOZoXz

19 Sudan Central Bank, "The Present Board of Directors," http://bit.ly/1jxA7pG

20 "Emeriti owned Canar considering to exit Sudan's market for not denial of mobile phone license," *Sudan Tribune*, February 1, 2016, http://bit.ly/1PPqLlG

Limits on Content

Online news outlets, social media, and communications platforms did not face restrictions during this year. Self-censorship among online journalists and ordinary users was more palpable due to fears of government surveillance and arbitrary legal consequences. Nonetheless, social media users were active in organizing campaigns about important political, social, and economic issues.

Blocking and Filtering

News websites and social media platforms were not blocked in Sudan during the coverage period, though the relatively free environment in which online news outlets operate has faced growing threats in recent years. According to local sources, the Sudanese government is in the process of establishing a new unit devoted to monitoring online outlets that may impose a similar regime of systematic censorship faced by Sudan's print and broadcast media (see Media, Diversity, and Content Manipulation).[21]

The Sudanese government openly acknowledges blocking and fil ering websites that it considers "immoral" and "blasphemous." The NTC manages online fil ering in the country through its Internet Service Control Unit and is somewhat transparent about the content it blocks, reporting that 95 percent of blocked material is related to pornography,[22] though the regulator recently acknowledged that it had not be successful in blocking all pornographic sites in Sudan.[23] The NTC also obligates cybercafé owners to download blocking and fil ering software as a requirement to sustain their licenses.[24]

The NTC's website gives users the opportunity to submit requests to unblock websites "that are deemed to not contain pornography,"[25] but it does not specify whether the appeals extend to political websites. Users attempting to access a blocked site are met with a black page that explicitly states, "This site has been blocked by the National Telecommunications Corporation," and includes links to further information and a contact email address.[26]

In addition to the NTC, National Intelligence and Security Service (NISS) agents reportedly have the technical capability to block websites deemed harmful and threatening to Sudan's national security,[27] while the General Prosecutor also has the right to block any site that threatens national security or violates social mores.[28] The NTC also requires internet café owners to download a blocking and fil ering software to target "immoral" content as a requirement to sustain their licenses.

21 Author's interview, May 2016. See also, "Sudan to set up special body for electronic media monitoring," Sudan Tribune, January12, 2016, http://bit.ly/1pcaxJF

22 National Telecommunications Corporation, "Blocking Or Unblock Websites," last modified Sep ember 21, 2016, http://www.ntc.gov.sd/index.php/en/blocking-websites

23 NTC: pornographic sites are increasing on the Internet and other online platform," *Almeghar*, August 9, 2015, bit.ly/1X8CQDm.

24 "Sudanese intelligence prosecutes Internet content that 'threatens the morals of the nation'," *Alhayat*, February 29, 2016, http://bit.ly/21iftrT

25 NTC, "Blocking Or Unblock Websites."

26 Image of a blocked site: https://docs.google.com/file/d/0B6mgwvplJ6IadER_T3RTZW1jSkk/edit?pli=1

27 "Expert: NISS is capable of blocking websites that are posing a threat to Sudan's national security," *Aljareeda*, November 7, 2014.

28 "Cybercrime is an act of terrorism that threatens the sovereignty of the state," [in Arabic] *Alintibaha*, August 13, 2014, http://bit.ly/1NRfFg5.

Content Removal

The extent to which the government forces websites to delete certain content is unknown, though anecdotal incidents in the past few years suggests that some degree of forced content removal by the state exists, and that such ad hoc requirements lack transparency. No specific incidents ere reported during this report's coverage period.

Media, Diversity, and Content Manipulation

Compared to the highly restrictive space in the traditional media sphere—which is characterized by pre-publication censorship, confiscations f entire press runs of newspapers, and warnings from NISS agents against reporting on certain taboo topics—the internet remains a relatively open space for freedom of expression, with bold voices expressing discontent with the government on various online platforms. Online news outlets such as *Altareeg*,[29] *Altaghyeer*,[30] *Radio Dabnga*,[31] *Hurriyat*, and *Alrakoba* cover controversial topics such as corruption and human rights violations. Facing heavy censorship, many print newspapers have shifted to digital formats, circulating censored or banned material on their websites and social media pages; as a result, Sudanese citizens increasingly rely on online outlets and social media for uncensored information.

WhatsApp has become particularly popular among Sudanese, who have turned to the platform's relative privacy and anonymity to share critical news via the app's group chat function.[32] Blogging is also popular, allowing journalists and writers to publish commentary free from the restrictions leveled on print newspapers and provides ethnic, gender, and religious minorities a platform to express themselves. The more active Sudanese bloggers write in the English language. However, self-censorship has risen in recent years. Many journalists writing for online platforms publish anonymously to avoid prosecution, while ordinary internet users in Sudan have become more inclined to self-censor to avoid government surveillance and arbitrary legal consequences.

In response to Sudan's more vibrant online information landscape, the government employs a concerted and systematic strategy to manipulate online conversations through its so-called Cyber Jihadist Unit. Established in 2011 in the wake of the Arab Spring, the unit falls under the National Intelligence and Security Service (NISS) and works to proactively monitor content posted on blogs, social media websites, and online news forums.[33] The unit also infiltra es online discussions in an effort to ascertain information about cyber-dissidents and is believed to orchestrate technical attacks against independent websites, especially during political events (See Technical Attacks).[34]

In January 2016, the government issued a directive to the Journalists' Association, requiring editors-in-chief of the association to sign a voluntary Charter that obliges editors to match their outlets'

29 *Altareeg* was established in January 2014.

30 *Altaghyeer* [Arabic for change with political connotation] was established in 2013 following the government's crackdown on independent journalists, who were eventually banned from practicing traditional journalism in Sudan.

31 Launched from the Netherlands in November 2008, Radio Dabanga focuses on reporting on Darfur and has a strong online presence and wide audience in conflicts a eas. It website is bilingual and runs in depth reports and features. It is a project of the Radio Darfur Network. Dabnga, "About Us," http://bit.ly/1LkMr5H.

32 Khalid Albaih, "How WhatsApp is fueling a 'sharing revolution' in Sudan," The Guardian, October 15, 2015, https://www.theguardian.com/world/2015/oct/15/sudan-whatsapp-sharing-revolution

33 "Sudan to unleash cyber jihadists," *BBC*, March 23, 2011, bbc.in/1V3FWdi.

34 See Freedom on the Net, Sudan 2015, bit.ly/1QQpZp5.

online articles with printed versions.[35] Considering the government's pre-publication censorship of the print media, observers believe the move is an effort to impose the same restrictions on online outlets.[36]

Digital Activism

Sudanese social media users have become more willing to organize themselves online for common goals, launching several online campaigns to address social, political, and economic concerns in the past year.

In November 2015, users started a campaign in reaction to photos circulated on social media indicating mistreatment of Sudanese citizens in Egypt.[37] Several hashtags called on Sudanese to refrain from traveling to Egypt and boycott EgyptAir and other Egyptian products.[38] While there was no official esponse from the Egyptian government, Egyptian media covered the campaign and Egyptian social media users launched a hashtag to apologize for the mistreatment.[39]

In March 2016, Sudanese social media users called on Khalid al-Wazir, a Blue Nile TV talk show host, to apologize for racially insensitive comments about Ethiopian domestic workers in Sudan.[40] Building on the #اعتذر_اي_خالد_الوزيري hashtag [Arabic for #Say_Sorry Khalid_AlWazie], a Facebook page was created with the same name calling on al-Wazir to apologize. Page administrators also reached out to sponsors of the show, asking them to take a stand against the racist content of the show. The campaign attracted local and regional coverage.[41] Other commentators used the opportunity to address racism, as well as the role of social media and the elite in influencing positi e social change.[42] Within a few days, al-Wazir apologized on his Facebook page, and Blue Nile TV issued a statement promising to conduct an investigation about the allegations of racist comments.[43]

In April 2016, large demonstrations broke out at the University of Khartoum for three days following news circulated on social media about government plans to sell a historical building of the university.[44] Several online campaigns emerged calling for the halt of the sale and for student protests

35 "Signing journalism charter in Sudan," *Ashorooq*, January 26, 2016, bit.ly/1pFgJtI.

36 "Sudanese Journalism charter," *Sada Alahdas*, January 28, 2016, bit.ly/1QPpURh.

37 "Egypt and Sudan: the 'torture incident' beats the drums of war between the Nile Valley Partners," *Sasa Post*, November 23, 2016 http://bit.ly/2aieTZK

38 "Egypt is not my country's sister" Facebook page: http://bit.ly/2aid2Eq
There is a famous Sudanese song that celebrates the historical relations between Sudan and Egypt that is titled Egypt is my country's sister and the hashtag is generated to reject this affinity.

39 "A campaign to contain the anger of our brothers: we are sorry Oh Sudanese," *Elwatan News*, November 22, 2015 http://bit.ly/2aFg4Gs; "Crisis in cyberspace between Egypt and Sudan: the authorities are silent and the citizens are responding," *Dot Msr*, November 21, 2016 http://bit.ly/2aqglIo

40 Khalid Al-Wazir, say sorry Facebook page: http://bit.ly/2az2dyo

41 "Say sorry, Khalid Al-Wazir!," *Alrakoba*, March 26, 2016 http://bit.ly/2aGOkOq; Clip from Al-Arabiya TV uploaded to YouTube http://bit.ly/2apQIaB

42 "Amidst the anger against Alwazir show: an opportunity to call for the better," *Alrakoba,* March 27, 2016, http://bit.ly/2a7QUzl

43 "Blue Nile: administrative action to be taken against a program that offended Ethiopian domestic workers," *Altageer*, March 27, 2016

44 "Demonstrations at the University of Khartoum following reports of the Sudanese government's intention selling its buildings, *Alquds*, April 14, 2016 http://bit.ly/2aFy2YY

against the plan.[45] Dozens of students were briefly ar ested,[46] two students were killed, [47] and at least six students were held for 45 days without charge. Their families protested the police's use of excessive force and arbitrary detention[48] and campaigned online for the release of those held by posting photos and calling for sit-ins.[49] Public pressure fueled by the online activism helped lead to their eventual release.[50]

Violations of User Rights

Revisions to the 2004 Press and Printed Press Materials Law were introduced in 2015 with the aim of regulating online media and providing a legal framework to prosecute online journalists. Arrests and prosecutions under the IT Crime Act grew markedly in the past year, reflecting a tactical shift in the government's strategy to limit internet freedom and creating a chilling effect on freedom of expression online.

Legal Environment

Sudan has restrictive laws that limit press and internet freedom. Most notably, the Informatic Offences (Combating) Act 2007 (known as the IT Crime Act, or electronic crimes law)[51] criminalizes the establishment of websites that criticize the government or publish defamatory material and content that disturbs public morality or public order.[52] Violations involve fines and prison sen ences between two to fi e years.

Broad wording in other laws pertaining to traditional media may be applied to online content, including revisions to the highly restrictive 2004 Press and Printed Press Materials Law in 2009, which extended restrictions on the press in the interests of national security and public order and holds editors-in-chief liable for all content published by their press outlets.[53] The 2010 National Security Act gives the NISS immunity from prosecution and the permission to arrest, detain, and censor journalists under the pretext of national security.[54]

45 "Graduates of the University of Khartoum hold The silent vigils in number of capitals around the world," *Sudan Tribune*, April 22, 2016 http://bit.ly/2aSQudb

46 "Sudanese security arrested dozens of graduates of the University of Khartoum after protests," *Youm7*, April 23, 2016 http://bit.ly/2alAI8A

47 "Sudan student killing sparks wave of protests," *The Guardian*, April 22, 2016 http://bit.ly/2aqk1tu

48 "Killing of Ahlia University's student escalates demonstrations," 3ayin, April 29, 2016 http://bit.ly/2aoWUA8

49 Press Release: The Arabic Network for Human Rights Information (ANHRI): Sudan: protests of families of the University of Khartoum students detainees and civil society. May 26, 2016 http://bit.ly/2aDxDVM "Families of the University of Khartoum students detainees have their Iftar in front of the headquarters of the Sudanese security [National Intelligence and Security Service] since the beginning of Ramadan," *Alquds,* June 11, 2016 http://bit.ly/2acF7v4

50 "Sudanese security released two students and 4 students," *Sky News Arabia*, June 19, 2016 http://bit.ly/2a8iRqz

51 The Informatic Offences (Combating) Act, 2007, http://bit.ly/1NkNx1R.

52 Abdelgadir Mohammed Abdelgadir, *Fences of Silence: Systematic Repression of Freedom of the Press, Opinion and Expression in Sudan*, (International Press Institute, 2012) http://bit.ly/1Pv7nee. According to Section 4, crimes against public order and morality Sudan cyber law, of Sudan's Cybercrime Law (2007), intentional or unintentional producing, preparing, sending, storing, or promoting any content that violates public order or morality, makes the offender liable to imprisonment of 4 to 5 years or a fine or both. The maximum penalty for committing both crimes is 7 years or fine or both. Also, under the same section, c eating, promoting, using, website that calls for, or promote, ideas against public law or morality is punished by 3 years in prison or fine or both. Cyber defamation crimes necessitate 2 years in prison or fine or both. Public o der is not defined clearly in the la . Subsequently, most of the opposition content online falls under this section making online activists liable under this law.

53 Committee to Protect Journalists, "Repressive press law passed in Sudan," June 11, 2009, https://cpj.org/x/2c67.

54 Amnesty International, "Sudanese security service carries out brutal campaign against opponents," July 19, 2010, http://bit.ly/1OP3OOi.

In August 2015, the Minister of Information announced plans to further extend the highly restrictive 2004 Press and Printed Press Materials Law to control online content.[55] Reiterating the new law's intentions in January 2016, the minister warned social media users and online journalists that the law would address the spread of false news that "distorts Sudan's image."[56] While the text of the law remains unpublished, the new law will reportedly establish a specialized council to monitor online media and social media platforms as well as a Summary Press Court to try media and freedom of expression cases.[57] A committee formed by the Ministry of Justice—comprised of representatives from the NISS, Ministry of Interior, Bar Association, and Sudanese Journalist Union—met in May 2016 to finalize the new la ,[58] which is expected to come into effect in 2017.[59]

Prosecutions and Detentions for Online Activities

Arrests for online activities grew markedly in the past year, reflecting a tactical shi t in the government's strategy to limit internet freedom. In an alarming change from previous years, the government kept several individuals in arbitrary detention for lengthy periods of time due to their online activities, denying them the right to a fair trial.

In a growing trend, critical WhatsApp messages frequently implicated users in alleged cybercrimes, which were often leaked to the authorities by the members of group chats. In November 2016, for example, Seraj al-Naeem, the founder of the online news outlet *Awtar al-Aseel*, was arrested and charged with libel under the IT Crime Act for sending a WhatsApp message that accused a doctor of medical malpractice. Al-Naeem was detained for hours and released on bail, but not before he was asked to surrender his smartphone to the police as evidence.[60] Al-Naeem was subsequently charged for inquiring about the legality of surrendering his phone.[61] He was acquitted of all charges in May 2016.[62]

In January 2016, the administrator of a WhatsApp group for journalists was charged with libel under the IT Crime Act for a message that criticized the Minister of Health. He was detained and questioned for several hours along with the individual who sent the original message; both were subsequently released on bail, and as of October 2016, still awaiting trial.[63]

Facebook posts also led to several arrests. In January 2016, a humanitarian activist in the town of

55 "Sudanese Minister of Information: New press law will include strict sanctions to control violations in online media," *Alwafd,* August 18, 2015, bit.ly/1U7NDzm.

56 "The Sudanese government vows to deprive journalists of their last self-expression venue," *Alarab*, January 14, 2016, bit.ly/1RNliMv.

57 "Sudanese government: Summary press courts to reduce the 'exceptional measures'," *Global Media Service (Sudan)*, November 2, 2015, bit.ly/1P73KW5. "'A new press court to suppress freedom of expression," *Alarab*, August 20, 2016, bit.ly/1QR080a.

58 "A committee that includes NISS considers modifying the press and publications law in Sudan," *Altareeq*, May 15, 2016 http://bit.ly/29N1dK1

59 "[The government to take measurements against what it perceives as lack of discipline on the part of the media], *AlSaiha*, June 17, 2016 http://bit.ly/29SZbpg

60 "A case against Seraj Alnaeem is before court for writing about the death of Dr. Ghada," *Awtar Alaseel,* February 29, 2016, bit.ly/1g3AhR6.

61 "Investigation Office brings Seraj Alnaeem befo e Criminal Court for sending a text message to the Director General of Police," *Alnilin*, November 30, 2015, bit.ly/24ZUz5z.

62 "Acquittal of Seraj Alnaeem of the charge of publishing an article about the death of the (Ghada Ahmad Badawi) as a result of medical error," *Alnilin*, May 29, 2016, http://bit.ly/29ZNWfq

63 "In an unprecedented incident, Cybercrime Prosecutor interrogates a WhatsApp manager," *Almshaheer*, January 4, 2016, bit.ly/1nHUAcA. "Two Sudanese journalists face defamation accounts for messages exchanged on 'WhatsApp'," *Sudan Tribune*, January 3, 2016, bit.ly/1RJhsAA. "Only happening in Sudan: a comment «WhatsApp» leads a person to court," Al-quds Al-Arabi, January 9, 2016 http://bit.ly/29HI7zb; https://twitter.com/iyad_elbaghdadi/status/684033732559241216

Tandali, located in South Kordofan State, was arrested for a Facebook post criticizing the town's mayor.[64] No further information was available about this case as of October 2016. In February 2016, Ibrahim Baggal, a digital journalist and online activist, was arrested for criticizing the governor of North Darfur in a Facebook post and charged under the IT Crime Act.[65] Baggal spent 55 days in detention before his release on bail,[66] but was detained again days later and held for another week, for seemingly arbitrary reasons.[67] The public prosecutor later dropped some of the charges leveled against Baggal, namely undermining the constitutional order, waging war against the state, and contempt for authority; however, Baggal still faces charges of spreading false information, disclosing military information, and breaching public safety.[68]

The authorities increasingly went after bloggers and journalists who have turned to online outlets to avoid heavy-handed censorship in the print and broadcast sectors. At least one online journalist was arrested. In July 2015, Waleed al-Hussein, the creator of the critical online news outlet *al-Rakoba*, was arrested by the authorities in Saudi Arabia, where al-Hussein was residing. He was arrested without charges and eventually released in February 2016; three months of his detention were spent in solidarity confinement [69] Family members believe he was arrested at the request of the Sudanese government, which had targeted al-Hussein for his work in the past and was seeking to have him extradited back to Sudan,[70] though the government denied the accusations.[71]

In May 2016, the Cyber Crime Investigations Unit interrogated journalist Sarah Taj Elsir for an article she wrote for *al-Jarida* newspaper that was republished by the online outlet *al-Rakoba*.[72] She was charged under article 17 of the IT Crime Act for allegedly spreading false news, though she was not responsible for the online distribution of her article.[73] Elsir was also questioned about her relation to an individual who had commented on the online version of her article. She later filed a Case emoval Request to have the charges dropped.[74]

Users who violated "public morals" also faced arrests. In 2015, an individual was arrested at a cybercafe for viewing a secular website in Khartoum; he was held for two days and beaten before being released without charges.[75]

Surveillance, Privacy, and Anonymity

Unchecked surveillance of ICTs is a grave concern among citizens in Sudan, where the government is

64 "Security Apparatus of Al- Bashir regime arrests activist Mohammed Jaili in Tandali," Sudan Voices, January 25, 2016, http://bit.ly/1UCFJhc

65 "Health of a journalist arrested by authorities in Khartoum transferred to Elfashir deteriorates," *Sudan Tribune*, February 2016, bit.ly/1M1hQ0M.

66 "El Fasher: Baggal released after 55 days of detention," *Radio Dabang*, April 8, 2016 http://bit.ly/2a8FcVh

67 "Baggal re-arrested and transferred to Shalla under the guidance of the governor," *Radio Dabang,* April 12, 2016, http://bit.ly/29MKXCJ

68 "Release of Baggal" *Radio Dabanga*, April 15, 2016, http://bit.ly/29N9626

69 Author interview, May 2016.

70 Amnesty International, "Sudanese Activist Arrested, Risks Deportation," urgent action, September 9, 2015, http://bit.ly/1LH10lk

71 "Khartoum denies involvement in Sudanese blogger arrest by Saudi police," *Sudan Tribune*, September 7, 2015, http://bit.ly/1LV7nju

72 Link to the article on Alrakoba: http://bit.ly/1Ufl0LJ

73 "Sudan | Cyber Crime Investigations Unit Interrogates a Female Journalist of Al-Jaridah," Arabic Network for Human Rights Information, May 4, 2016, http://bit.ly/1YyJqWt

74 "For the second time, Cyber Crime Investigations Unit Interrogates Sarah Taj Elsir, journalist with Al-Jarida newspaper because of the material published by Alrakoba," *Alrakoba*, May 10, 2016, http://bit.ly/1Xwf87E

75 Author's interview.

known to actively monitor internet communications on social media platforms and target online activists and journalists during politically sensitive periods. The NISS regularly intercepts private email messages, enabled by sophisticated surveillance technologies.[76]

Internal emails leaked by hackers in July 2015 confi med that the NISS had purchased Hacking Team's Remote Control System (RCS) spyware in 2012,[77] which has the ability to steal files and ass- words, and to intercept Skype calls and chats.[78] While other leaked emails revealed that the company had discontinued business with Sudan in November 2014,[79] Citizen Lab research found that Sudan also possesses high-tech surveillance equipment from the U.S.-based Blue Coat Systems, a technology company that manufactures monitoring and fil ering devices. The surveillance system was initially traced to three networks inside Sudan, including on the networks of the private telecom provider Canar.[80]

Article 9 of the NTC's General Regulations 2012, based on the 2001 Communications Act, obligates mobile companies to keep a complete record of their customers' data, thus requiring SIM card registration, which was enacted in 2008.[81] The government reportedly plans to link SIM cards to users' national identification numbe s in the future,[82] while the Ministry of Information stated in March 2016 that it is considering new requirements to register all mobile devices with real names.[83]

Cybercafés lack privacy and are also subject to intrusive government surveillance. In February 2016, the NISS and Ministry of Interior special cybercrime units raided 130 internet cafes in Khartoum in search of content threatening "public morals."[84]

Intimidation and Violence

Online journalists and activists often face extralegal intimidation, harassment, and violence for their online activities. Female activists in particular were subject to multilayered attacks on social media. In 2015, an anonymously run Facebook page titled "Sudanese Women against Hijab"[85] trolled female activists by attributing fabricated statements against religion and the Hijab (headscarf) to several women known for their activism and posting their photos alongside the statements. The page elicited heresy accusations and death threats against the female activists, who sought to have the Facebook page removed.[86]

76 See, "Sudan," Freedom on the Net 2015, Freedom House.

77 PDF of a receipt that shows the National Intelligence and Security Services of Sudan purchased Hacking Team's services: http://bit.ly/1Pv9A9p.

78 Hacking Team, "Customer Policy," accessed February 13, 2014, http://bit.ly/1GnkbjG.

79 Cora Currier and Morgan Maqruis-Boire, "A Detailed look At Hacking Team's Emails About Its Repressive Clients," *The Intercept*, July 7, 2015, http://bit.ly/1jxGv0h.

80 Ellen Nakashima, "Report: Web monitoring devices made by US fi m Blue Coat detected in Iran, Sudan," *Washington Post*, July 8, 2013, http://wapo.st/1Pv95fA.

81 SIM card registration compromises mobile phone users' privacy and anonymity, as it requires an official identification c d and home address information. "NTC announces the end of grace period to register sim cards," [in Arabic] *Sudani Net*, June 1, 2014, http://bit.ly/1W2A0n3.

82 "Sudan: Telecoms companies block non-registered SIM cards," *African Manager,* June 1, 2014, http://bit.ly/1NRlJ8x.

83 "A proposal for a new cybercrime law that stipulates prison sentences unto to 3 years," *AlJaridah*, March 20, 2016

84 "Sudanese intelligence prosecutes Internet content that 'threatens the morals of the nation'," *Alhayat*, February 29, 2016, http://bit.ly/21iftrT

85 See Link to the page: http://bit.ly/1W7r1jm

86 Petition: Save the lives of Sudanese women and men, take down "Sudanese Women Against Hijab" Page! http://chn.ge/1omvbp9

Technical Attacks

Independent news sites are frequently subject to technical attacks, which many believe are perpetrated by the government's Cyber Jihadist Unit. Attacks usually intensify during political events and unrest, while some prominent news sites ward off daily DDoS attempts.[87]

The online outlet *al-Rakoba*, whose Sudanese founder was arrested in Saudi Arabia in July 2015 (see Prosecutions and Detentions for Online Activities), suffered regular DDoS attacks that intensified during the national dialogue events in early 2016, which sought solutions for lasting peace amid the country's various conflicts [88] Publicized attacks during the coverage period include a DDoS attack on the online newspaper *al-Tareeq*, which took the site offline for half a day on August 12, 2015 [89]

87 Author's interview with internal sources who requested to stay anonymous with this info to avoid making their vulnerabilities known.

88 Author's interview, May 2016. http://www.usip.org/olivebranch/2016/02/11/sudan-s-national-dialogue-poses-test-government-s-commitment

89 "From Altareeg to its supporters against the recent hacking attack," *Altareeg*, August 16, 2015, bit.ly/1M6BEdE. Journalists for Human Rights (JHR). (2015). Altareeq online newspaper hacked. [Press release].

Freedom House

Syria

	2015	2016
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	24	24
Limits on Content (0-35)	26	26
Violations of User Rights (0-40)	37	37
TOTAL* (0-100)	**87**	**87**

* 0=most free, 100=least free

Population:	**18.5 million**
Internet Penetration 2015 (ITU):	**30 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- The so-called Islamic State (IS) issued strict regulations on the provision of internet access at cybercafes, requiring business to obtain licenses for setting up operations in Raqqa and Deir al-Zor (see **Availability and Ease of Access**).
- The internet was reportedly restored to parts of Aleppo, which had been shut off from access for seven months due to damage to telecommunications infrastructure. Authorities continue to shut down internet access in preparation for military offensives (See **Restrictions on Connectivity**).
- At least 17 netizens and citizen journalists remain imprisoned by the regime on charges related to their digital activism. It was confi med in September 2015 that cartoonist Akram Raslan died while in state custody, likely as a result of torture (see **Prosecutions and Detentions for Online Activities**).
- Several activists and bloggers were murdered by IS militants both in IS-controlled territory and neighboring Turkey, including two members of Raqqa is Being Slaughtered Silently and a female blogger who wrote about daily life in Raqqa (see **Intimidation and Violence**).
- Russia stepped up cyberattacks against Syrian human rights organizations and opposition groups in a bid to disrupt reporting on human rights violations and obtain intelligence (see **Technical Attacks**).

Introduction

Syria remained one of the most repressive and dangerous environments for users in 2015-16, marked by the fi st execution of a female blogger by extremists and the arbitrary detention of tech activists by the regime.

Syrian cyberspace remains fraught with conflict, ften mirroring the brutality of the war on the ground and its complex geopolitics. Citizen journalists were killed during air raids, regime opponents were tortured in state prisons, and the so-called Islamic State (IS) murdered individuals for chronicling the hardships of life under the religious extremists. Pro-regime hackers in the Syrian Electronic Army conducted spear-phishing other cyberattacks, joined by Russian hackers who have increasingly targeted human rights organizations and opposition groups.

Syria's telecommunications infrastructure is highly decentralized. In areas controlled by the regime, the state-owned service provider employs sophisticated technologies to fil er political, social, and religious websites. Meanwhile, individuals in rebel-controlled areas often rely on Turkish mobile internet beamed in from across the border, or in many cases, expensive satellite connections. Authorities regularly shut down internet access to prevent the dissemination of information, particularly before and during military operations. Shelling and sabotage have led to heavy damage to infrastructure, affecting internet and power connections in several provinces.

The internet has played a significant ole in documenting popular protests against the Syrian regime and its heavy-handed response against civilians. Authorities prevented foreign media from accessing the country, prompting many ordinary Syrians to take up mobile phones and small cameras to cover the deteriorating situation and post videos of the conflict on social media. These citizen jou nalists have become vital in the quest to document flagrant human rights abuses by all arties to the conflict.

Obstacles to Access

The war has devastated telecommunications infrastructure and disconnected around two-thirds of the country from Syrian internet service providers (ISPs). As a result, internet access has become highly decentralized with some relying on microwave links from Turkish cities or pooled satellite connections serving cybercafes. Internet access is regularly shutdown in areas controlled by the regime and disparate rebel groups alike.

Availability and Ease of Access

Syria's telecommunications infrastructure is one of the least developed in the Middle East, with broadband connections among the most difficult and expensi e to acquire.[1] This worsened after 2011, as inflation and electricity outages inc eased dramatically following public protests and the government's corresponding crackdown. Damage to the communications infrastructure is particularly bad in cities where the government is no longer in control, due to shelling by both the Syrian

1 Kyle Wansink, *Syria - Telecoms, Mobile, Broadband and Forecasts*, BuddeComm, accessed March 8, 2012, http://bit.ly/1OdycSD.

armed forces and opposition fighters. This has led to a decentralized telecommunications infrastructure, whereby each and every part of the country has a different internet gateway.

According to estimates by the International Telecommunication Union, some 30 percent of Syrians had access to the internet at the end of 2015, up from 21 percent in 2010.[2] The estimated number of fixed broadband subscribers also increased, but remained low at just over 3 subscriptions per 100 inhabitants. The number of mobile phone subscriptions decreased slightly over the past year, with 62 subscriptions per 100 inhabitants.

The price, speed, and availability of internet access vary depending on the region of the country. According to a pricelist published by the Syrian Computer Society Network, the monthly cost for a 1 Mbps ADSL connection was SYP 1950 (approximately US$6) as of March 2016,[3] in a country where monthly gross domestic product per capita was US$274[4] in 2012 and has since dropped.[5] While the Syrian lira (SYP) has lost a large amount of its value, prices have not changed dramatically during the conflict.

Around two-thirds of the country is disconnected from Syrian ISP networks, instead relying on a WiMax or WiFi microwave links from Turkish cities[6] or satellite connections (VSAT).[7] The former is particularly prominent in Kurdish areas along the Turkish border, such as Qamishli, where Wi-Fi connections are around US$50 per month. Prices are reportedly lower in the city than last year, with cybercafes reportedly available in every neighborhood.[8]

In areas controlled by the so-called Islamic State (IS), such as Deir al-Zor and Raqqa, internet access is subject to many regulations and often depend on military developments on the ground. For example, IS authorities reportedly banned the internet from the village of al-Boukamal in the province of Deir al-Zor in September 2015 in preparation for a military operation against regime forces in a nearby village.[9] Due to the prohibitive cost of VSAT connections, businesses in IS-controlled areas have established cybercafes where users split the cost of satellite infrastructure and purchase separate Wi-Fi connectivity. Based on Skype interviews with Syrians living under IS-controlled areas, the cost of Internet access inside the Internet cafes is 100 SYP (US$ 0.50) for 1 hour connection, while for smartphone users, 15 MB of data transactions costs 100 SYP.

In mid-2015, IS released a statement requiring these cybercafes to "remove Wi-Fi boosters in internet cafes as well as private wireless adapters, even for soldiers of the Islamic State."[10] The move is an attempt to limit private internet access in Raqqa and Deir al-Zor to public locations[11] that can be policed by the extremists in order to restrict reporting by activists as well as GPS-tracking of mili-

2 International Telecommunication Union, "Statistics," 2015, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

3 Syrian Computer Society Network, "ADSL Services and price" [in Arabic], accessed March 3, 2016, http://bit.ly/250BUqt.

4 World Bank Databank, "GDP per capita (current US$)," 2008-12, accessed March 12, 2014, http://bit.ly/1eRbn2E.

5 Democratic Arabic Center, "Reports: Syrian conflict losses f $ 80 billion and 11 percent of the population were killed or injured," [Arabic] February 11, 2016, http://democraticac.de/?p=27360.

6 "Northern Syria, Internet cafes are everywhere in the North, Chatting, Smoking and Porn," [in Arabic], *Hunasaotak*, http://bit.ly/1Q4ieIU.

7 "Internet through satellite and Turkish providers as an alternative of Al-Assad network in the countryside of Idlib," [in Arabic] *Orient News*, August 10, 2014, http://bit.ly/1PEllt8.

8 Interview with the Amjad Othman, journalist from Qamishli city via Skype.

9 Zainah Alsamman, "ISIS Bans the Internet in al-Boukamal, Deir Ezzor," SecDev Foundation, September 25, 2015, https://secdev-foundation.org/isis-bans-the-internet-in-al-boukamal-deir-ezzor/.

10 Erika Solomon, "Isis to cut private internet access in parts of Syria," *Financial Times*, July 20, 2015, http://on.ft.com/1M4z2ff.

11 ISIS is allowing the Internet but under surveillance, (Arabic), Alrai media, May 22nd , 2016 http://www.alraimedia.com/ar/article/others/2015/05/22/591978/nr/iraq

tants using the services.[12] Licenses are only provided to "loyal" businesses and require cafe owners to restrict WiFi availability to the physical space of the cybercafé, to log all customers using their IDs, and to separate men from women.[13] IS has allowed only four cybercafes in Deir al-Zor city (one each in the neighborhoods of Hamidiyeh, al-Ommal, Ghassan Aboud, and al-Sheikh Yassin) and all are under heavy surveillance by authorities.[14] Recent airstrikes targeting IS militants have also damaged telecommunications infrastructure in IS-held areas.[15]

Restrictions on Connectivity

The Syrian government has engaged in extensive and repeated internet shutdowns since 2011. Damage to telecommunications infrastructure disconnected the war-torn city of Aleppo from March to November 2015.[16] In a change from pre-March, internet connections to Aleppo were being routed through Syrian networks, rather than Turkish networks. Researchers speculated the move reflec ed recent gains made by the Syrian government army over rebel forces in the areas surrounding Aleppo, once Syria's most populous city. Researchers noted the city was reconnected using a "high capacity microwave link to the coastal city of Latakia, Syria."[17]

In areas controlled by the Syrian government, the Syrian Telecommunications Establishment (STE) serves as both an internet service provider (ISP) and the telecommunications regulator, providing the government with tight control over internet infrastructure.[18] In addition, private fi ed-line and mobile ISPs are required to sign a memorandum of understanding to connect to the international internet via gateways controlled by the Syrian Information Organization (SIO).[19]

ICT Market

As of 2012, some 14 ISPs operated in Syria. Independent VSAT connections are prohibited, although in reality they are heavily employed due to the damage that government ICT infrastructure has sustained as a result of the conflict [20] ISPs and cybercafes must obtain approval from the STE and pass security vetting by the Ministry of Interior and other security services.[21] Moreover, cybercafe owners are required to monitor visitors and record their activities. There are two main mobile phone providers in Syria: Syriatel—owned by Rami Makhlouf, a cousin of President Bashar al-Assad—and MTN Syria, a subsidiary of the South African company.

12 "ISIL is shutting down Internet Cafes around Deir ez-Zor Airport," [in Arabic] *Al-Arabiya*, December 8, 2014, http://ara.tv/mhf43.

13 "The Islamic state to prevent Internet in Abu Kamal," (Arabic), The Syrian Observatory for Human Rights, September 19, 2015, http://www.syriahr.com/?p=136555.

14 Skype Call with Samer Al-Deri.

15 Firas Alhakar "Hello.. Al-Raqa is offline" *Al-Akbar*, July 24, 2015, https://al-akhbar.com/node/238429.

16 Doug Madory, "Internet Returns to Aleppo, Syria," Dyn Research, November 11, 2015, http://research.dyn.com/2015/11/internet-returns-to-aleppo-syria/.

17 Doug Madory, "War-torn Syrian city gets new fiber lin ," Dyn Research, October 12, 2016, http://research.dyn.com/2016/10/war-torn-syrian-city-gets-new-fibe -link/.

18 Syrian Telecom, "Intelligent Network Project," http://www.in-ste.gov.sy/inindex_en.html.

19 Jaber Baker, "Internet in Syria: experimental goods and a field f a new control," White and Black Magazine, posted on Marmarita website, August 10, 2008, http://www.dai3tna.com/nuke/modules.php?name=News&file=a ticle&sid=6019. (no longer available)

20 "Online Syria, Offline yrians," *One Social Network with a Rebellious Message,* The Initiative or an Open Arab Internet, accessed March 8, 2012, http://bit.ly/1NSCAHQ.

21 Ayham Saleh, "Internet, Media and Future in Syria" [in Arabic], The Syrian Center for Media and Free Expression, November 14, 2006, http://bit.ly/1hfdwWl.

Regulatory Bodies

Syria's ICT market and internet policy is regulated by the SIO and the state-owned STE, which owns all fi ed-line infrastructures. The STE is a government body established in 1975 as part of the Ministry of Telecommunications and Technology.[22] Domain name registration is handled by the Syrian Computer Society, which was once headed by Bashar al-Assad prior to his appointment as president in 2000.[23]

Limits on Content

The Syrian government engages in extensive filtering of websites related to politics, minorities, human rights, and foreign affairs. Self-censorship is highly prevalent, particularly in areas under government control. Despite these limitations, activists make use of communication apps to save lives in rebel-controlled areas and citizen journalists continue to make use of video-uploading sites and social networks to spread information about human rights abuses and the atrocities of war.

Blocking and Filtering

The blocking of websites related to government opposition, human rights groups, the Muslim Brotherhood, and activism on behalf of the Kurdish minority is very common.[24] A range of websites related to regional politics are also inaccessible, including the prominent London-based news outlets *Al-Quds al-Arabi* and *Asharq al-Awsat*, as well as several Lebanese online newspapers and other websites campaigning to end Syrian influence in Le anon. Access to the entire Israeli top-level domain ".il" is also restricted. However, the websites of most international news sources and human rights groups have remained accessible.

Censorship is implemented by the STE and private ISPs with the use of various commercially available software programs. Independent reports in recent years pointed to the use of ThunderCache software, which is capable of "monitoring and controlling a user's dynamic web-based activities as well as conducting deep packet inspection."[25] In 2011, evidence emerged that the Syrian authorities were also using technology provided by the Italian company Area SpA to improve their censorship and surveillance abilities. The contract with Area SpA included software and hardware manufactured by companies such as Blue Coat Systems, NetApp, and Sophos. Blue Coat had reportedly sold 14 devices to an intermediary in Dubai which then sent them to Area SpA, ostensibly with Blue Coat believing that the equipment would be given to the Iraqi government; however, logs obtained by the hacktivist group Telecomix in August 2011 revealed evidence of their use in Syria instead.[26] In October of that year, Blue Coat acknowledged that 13 of the 14 devices had been redirected to the Syrian government, an inadvertent violation of a U.S. trade embargo, and that the company was

22 Ministry of Communication and Technology, "Overview," [in Arabic], http://www.moct.gov.sy/moct/?q=ar/node/21.

23 Sean Gallagher, "Network Solutions seizes over 700 domains registered to Syrians," Ars Technica, May 8, 2013, http://arstechnica.com/tech-policy/2013/05/network-solutions-seized-over-700-domains-registered-to-syrians/.

24 Reporters Without Borders, *Internet Enemies,* March 2011, http://bit.ly/eLXGvi.

25 Reporters Without Borders, "Syria," *Enemies of the Internet: Countries under surveillance*, March 12, 2010, http://bit.ly/1OCZ0cS.
Platinum, Inc., "ThunderCache Overview," accessed August 14, 2012, http://www.platinum.sy/index.php?m=91.

26 Andy Greenberg, "Meet Telecomix, The Hackers Bent on Exposing Those Who Censor and Surveil The Internet," *Forbes*, December 26, 2011, http://onforb.es/1Bu1tQx.

cooperating with the relevant investigations.[27] Analysis of the exposed Blue Coat logs revealed that censorship and surveillance were particularly focused on social-networking and video-sharing websites.[28] The *Wall Street Journal* identified effo ts to block or monitor tens of thousands of opposition websites or online forums covering the uprising. Out of a sample of 2,500 attempts to visit Facebook, the logs revealed that three-fi ths were blocked and two-fi ths were permitted but recorded.[29]

The Syrian government also engages in fil ering SMS messages. Beginning in February 2011, such censorship was periodically reported around dates of planned protests. In February 2012, Bloomberg reported in a series of interviews and leaked documents that a special government unit known as Branch 225 had ordered Syriatel and MTN Syria to block text messages containing key words like "revolution" or "demonstration." The providers reportedly implemented the directives with the help of technology purchased from two separate Irish fi ms several years earlier for the alleged purpose of restricting spam.[30]

The government continues to block circumvention tools, internet security software, and applications that enable anonymous communications. By enabling deep packet inspection (DPI) fil ering on the Syrian network, authorities were able to block secure communications tools such as OpenVPN, Later 2 Tunneling Protocol (L2TP), and Internet Protocol Security (IPsec) in August 2011.[31] Websites used to mobilize people to protest or resist the regime, including pages linked to the network of Local Coordination Committees (LCCs)—groups that have formed since the revolution to organize the opposition—continue to be blocked.[32] Websites that document human rights violations, such as the Violations Documentation Center, remain blocked,[33] as does the Mondaseh website, an online initiative to gather information and raise public awareness.[34] Authorities have repeatedly blocked the website and key search terms of *SouriaLi,* an internet radio station started by a group of pluralistic young Syrians.[35]

Facebook remains accessible in Syria after the government lifted a four-year block on the social-networking site in February 2011. The video-sharing website YouTube was also unblocked. Some activists suspected that the regime unblocked the sites to track citizens' online activities and identities. As of 2016, both were within the top-three most visited websites in the country.[36] Other social media platforms like Twitter are freely available, although they are not as popular and do not figu e within the top 25 most visited sites in the country.

The Voice-over-Internet-Protocol (VoIP) service Skype often has suffered from disruptions, either due to low speeds or intermittent blocking by the authorities. In February 2012, the government also began restricting access to certain applications for mobile phone devices that activists had been using

27 Blue Coat, "Update on Blue Coat Devices in Syria," news release, December 15, 2011, http://bit.ly/1FzFd8X.

28 "Blue Coat device logs indicate the levels of censorship in Syria," *Arturo Filasto*, accessed August 14, 2012, http://bit.ly/1LZDZJ3.

29 Jennifer Valentino-Devries, Paul Sonne, and Nour Malas, "U.S. Firm Acknowledges Syria Uses Its Gear to Block Web," *Wall Street Journal*, October 29, 2011, http://on.wsj.com/t6YI3W.

30 Ben Elgin and Vernon Silver, "Syria Disrupts Text Messages of Protesters With Dublin-Made Equipment," *BloombergBusiness*, February 14, 2012, http://bloom.bg/1i0TOEU.

31 Dlshad Othman, "Bypassing censorship by using obfsproxy and openVPN, SSH Tunnel," *Dlshad,* June 22, 2013, http://bit.ly/1KH3KjZ.

32 Local Coordination Committees, "Home,": http://www.lccsyria.org/en/.

33 "Leaked list of all blocked websites in Syria," Arab Crunch, May 19, 2013, http://bit.ly/1KGFPBm.

34 "Home," *the-syrian,* http://english.the-syrian.com/.

35 Syria Untold, "Syrian Creativity: Radio SouriaLi Broadcasts over the Internet," *Global Voices*, June 7, 2013, http://bit.ly/1EQI2ZS.

36 Alexa, "Top Sites in SY," accessed October 25, 2016, http://www.alexa.com/topsites/countries/SY.

to circumvent other blocks. Anti-virus software and updates to operating systems remain blocked due to U.S. sanctions, to the dismay of many U.S.-based activists.[37]

Decisions surrounding online censorship lack transparency and ISPs do not publicize the details of how blocking is implemented or which websites are banned, though government officials ha e publicly admitted engaging in internet censorship. When a user seeks to access a blocked website, an error message appears implying a technical problem rather than deliberate government restriction. Decisions on which websites or keywords should be censored are made by parts of the security apparatus, including Branch 225, or by the executive branch.

Content Removal

According to digital security organization SecDev, dozens of opposition pages, media centers, and independent NGOs have been closed by Facebook.[38] These include numerous pages of local coordination committees (LCCs) and the London-based Syrian Network for Human Rights. Activists believe that Facebook users sympathetic to President Assad may be reporting the pages en masse as violating user guidelines, thereby provoking Facebook into action. Razan Zaitouneh of the Violations Documentation Center shared a letter urging Facebook to keep the sites open, stating that "Facebook pages are the only outlet that allows Syrians and media activists to convey the events and atrocities to the world." Representatives from Facebook have cited the difficulties in disce ning between objective reporting and propaganda, particularly since many armed extremists have taken to using the site.

Media, Diversity, and Content Manipulation

In an environment of extreme violence and arbitrary "red lines," self-censorship is widespread. Sensitive topics include criticizing President Assad, his late father, the military, or the ruling Baath party. Publicizing problems faced by religious and ethnic minorities or corruption allegations related to the ruling family, such as those of Assad's cousin Rami Makhlouf, are also off limits. Most Syrian users are careful not only to avoid such sensitive topics when writing online, but also to avoid visiting blocked websites.[39] However, the period of May 2012 to April 2013 witnessed a large number of local Syrian users expressing opposition to Assad, his father, Makhlouf, the Baath party, and certain ethnic or sectarian groups.[40] In 2014, users living in areas under control of IS or other extremist groups have stepped up their self-censorship in order to avoid criticizing the militants or Islam in general.

Pro-regime forces have employed a range of tactics to manipulate online content and discredit news reports or those posting them, though it is often difficult o directly link those who are carrying out these activities with the government. Most notable has been the emergence of the Syrian Electronic Army (SEA), a progovernment hacktivist group that targets the websites of opposition forces, human rights websites, and even Western media outlets (see "Technical Attacks"). For news websites and other online forums based in the country, it is common for writers to receive phone calls from gov-

37 Mike Rispoli, "Access joins open letter to tech industry addressing overcompliance with U.S. sanctions," Access, June 28, 2012, http://bit.ly/1i0XdDM.

38 Michael Pizzi, "The Syrian Opposition Is Disappearing From Facebook," *The Atlantic*, February 4, 2014, http://theatln.tc/1aojZAO.

39 Email communication from a Syrian blogger. Name was hidden.

40 Interview with a Syrian activist, November 2012, Damascus, November 2012.

ernment officials ffering "directions" on how to cover particular events.[41] The Syrian government also pursues a policy of supporting and promoting websites that publish progovernment materials in an attempt to popularize the state's version of events. These sites typically cite the reporting of the official sta e news agency SANA, with the same exact wording often evident across multiple websites. Since early 2011, this approach has also been used to promote the government's perspective about the uprising and subsequent military campaign.[42] Interestingly, in 2012, the progovernment website Aksalser changed its stance to support the opposition and was subsequently blocked by the government.[43]

U.S. sanctions have resulted in the blocking of paid online services, making it difficult for yrians to purchase a domain or host their websites in the U.S. Restrictions on importing funds into Syria have had a significant im act on the ability to publish content. For instance, the Syrian magazine *Syrian Oxygen* was unable to obtain SSL certifica es for their website from U.S. providers, apparently because the domain syrianoxygen.com has the word Syria in it.

Digital Activism

Online tools have proven crucial for Syrians inside and outside the country seeking to document human rights abuses, campaign for the release of imprisoned activists, and disseminate news from the front lines of the conflict. Communication apps ha e become particularly important in saving lives during the conflict. A WhatsApp g oup called "The Monitors" was created by individuals based in regime-controlled areas to warn individuals living in rebel-controlled areas of impending Syrian and Russian air raids.[44] The U.S.-based Syrian American Medical Society has used WhatsApp for telemedicine, in one instance guiding a veterinarian who delivered twin babies by caesarean section in the besieged town of Madaya.[45]

Syrians are very active on Facebook, using it as a platform to share news, discuss events, release statements, and coordinate both online and offline activities [46] A Facebook petition for the release of Youssef Abdelke, initiated by a group of Syrian intellectuals and artists, was signed by over 2,500 users.[47] Abdelke, an illustrator and painter who has often expressed political dissent through his art, was arrested in July 2013 after he signed a declaration, posted online, which called for a democratic transition and the stepping down of President Assad.[48] He was released one month later.[49]

In addition, one observer has called the conflict in yria the fi st "YouTube War" due to the extraor-

41 Guy Taylor, "After the Damascus Spring: Syrians search for freedom online," *Reason,* February 2007, http://theatln.tc/1aojZAO.

42 Guy Taylor, "After the Damascus Spring: Syrians search for freedom online," *Reason,* February 2007, http://theatln.tc/1aojZAO.

43 The Syrian "Aksalser website with the revolution," [in Arabic] *the-syrian*, August 28, 2012, http://the-syrian.com/archives/86170.

44 Maya Gebeily, "Secret Syria network warns of air raids over WhatsApp," *The Times of Israel*, January 21, 2016, http://www.timesofisrael.com/sec et-syria-network-warns-of-air-raids-over-whatsapp/.

45 Avi Asher-Schapiro, "The Virtual Surgeons of Syria," *The Atlantic*, August 24, 2016, http://www.theatlantic.com/international/archive/2016/08/syria-madaya-doctors-whatsapp-facebook-surgery-assad/496958/.

46 Judith Dublin, "Syrian Fight Fire with Facebook," *Vocativ*, September 23, 2013, http://voc.tv/1UJqcIP.

47 Clara Olshansky, "The Web Petitions to Free Syrian Artist Youssef Abdelke," *Artfcity*, August 1, 2013, http://bit.ly/1VQezSS.

48 "Déclaration pour Syrie democratique" [Declaration for a Democratic Syria], *Babelmed*, accessed March 14, 2014, http://bit.ly/1izKKHU.

49 Khalil Sweileh and Omar al-Sheikh,"Syria: Youssef Abdelke Free, Resolved to Stay in Damascus," *Al-Akhbar,* August 23, 2013, http://bit.ly/1XQaLmi.

dinarily high coverage of human rights violations, military battles, and post-conflict de astation that is contained in videos posted to the site.[50] Indeed, as the Syrian government shifted to the use of heavy arms and missiles against opposition figh ers, the role of citizen journalists has shifted from live event coverage to documenting the bloody aftermath of an attack. Although many obstacles stand in the way of media coverage, citizen journalists have designed techniques to ensure media coverage of remote and conflict a eas. "Local Media Offices" ensu e that local journalists cover limited geographic areas, and then use a social network as a platform to collect, verify, and publish news stories. Hundreds of thousands of videos have been posted to YouTube by citizen journalists, rebel groups, and civil society groups, mostly documenting attacks. A Syrian group categorizing YouTube videos and sharing them via the platform OnSyria had posted almost 200,000 videos in 2013.[51]

Violations of User Rights

Syria remains one of the most dangerous places to use the internet in the world. Citizen journalists, bloggers, and activists are detained and often tortured by both government forces and, increasingly, fighters linked to extremist groups like the so-called Islamic State (IS). Several netizens were killed during the coverage period, including a female blogger who wrote of daily life in the IS stronghold of Raqqa.

Legal Environment

Laws such as the penal code, the 1963 State of Emergency Law, and the 2001 Press Law are used to control traditional media and arrest journalists or internet users based on vaguely worded terms such as threatening "national unity" or "publishing false news that may weaken national sentiment."[52] Defamation offenses are punishable by up to one year in prison if comments target the president and up to six months in prison for libel against other government officials, including judges, the military, or civil servants.[53] In addition, Syria's cybercrime law allows prison sentences of up to three years and fines f up to SYP 250,000 (US$ 1,500) for anyone who incites or promotes crime through computer networks.[54] The judiciary lacks independence and its decisions are often arbitrary. Some civilians have been tried before military courts.

Prosecutions and Detentions for Online Activities

Since antigovernment protests broke out in February 2011, the authorities have detained hundreds of internet users, including several well-known bloggers and citizen journalists. While it is very difficult o obtain information on recent arrests, 17 netizens remain in prison according to Reporters Without Borders.[55] Many of those targeted are not known for their political activism, so the reason for their arrest is often unclear. This arbitrariness has raised fears that users could be arrested at any

50 Christophe Koettl, "The YouTube War: Citizen Videos Revolutionize Human Rights Monitoring in Syria," *Mediashift* (blog), *PBS,* February 18, 2014, http://bit.ly/1Nkfnw9.

51 The platform, http://onsyria.org/, is now offline and the elated Facebook page has not been updated since 2013: Onsyria, Facebook Page, http://on.fb.me/1GnVymR.

52 Syrian Penal Code, art. 285, 286, 287.

53 Syrian Penal Code, art. 378.

54 Global Resource and Information Directory, "Legislation," in "Syria," http://www.fosigrid.org/middle-east/syria.

55 Reporters Without Borders, "Netizens Imprisoned," 2016, https://rsf.org/en/barometer?year=2016&type_id=237#list-barometre.

time for even the simplest online activities—posting on a blog, tweeting, commenting on Facebook, sharing a photo, or uploading a video—if it is perceived to threaten the regime's control. Veteran blogger Ahmad Abu al-Khair was taken into custody in February 2011 while traveling from Damascus to Banias and was later released, though he remains in hiding.[56] More recently, in an effort to pressure al-Khair to turn himself in, security forces have twice detained his brother, once for a period of 60 days.[57] Bassel Khartabil, an open source activist and recipient of the 2013 Index on Censorship Digital Freedom Award, remains in prison after he was taken by authorities without explanation in March 2012.[58]

Human rights activists who work online are also targeted by the government and the rebels. Four members of the Violations Documentation Center (VDC) were kidnapped by an unknown group from a rebel-controlled area in December 2013.[59] Authorities raided the offices of the Syrian Center for Media and Freedom of Expression (SCM) in February 2012, arresting 14 employees.[60] One SCM member and civil rights blogger, Razan Ghazzawi,[61] was detained for 22 days.[62] Three others remain in prison and face up to 15 years for "publicizing terrorist acts" due to their role in documenting human rights violations by the Syrian regime.[63] The organization's founder and director, Mazen Darwish, was reportedly released in August 2015 after three years in pretrial detention and recently moved to Germany.[64]

Surveillance, Privacy, and Anonymity

Surveillance is rampant on Syrian internet service providers, which are tightly aligned with security forces. Meanwhile, in IS-controlled territory, there are reports that militants have conducted unannounced raids at cybercafes in which they force users to leave their machines, going through their open web browsing sessions and social media accounts to ensure users are not viewing or writing impermissible content.[65]

The Law for the Regulation of Network Communication against Cyber Crime, passed in February 2012, requires websites to clearly publish the names and details of the owners and administrators.[66] The owner of a website or online platform is also required "to save a copy of their content and traffic data to allow verification of the identity of persons who contribute content on the network" for a period of time to be determined by the government.[67] Failure to comply may cause the website to

56 Anas Qtiesh, "Syrian Blogger Ahmad Abu al-Khair Arrested This Morning," *Global Voice Advocacy*, February 20, 2011, http://bit.ly/1vxJk5g.

57 Email communication with activist who wished to remain anonymous, April 2012, Syria.

58 "Renewed calls for Bassel Khartabil's release on 4th anniversary of detention," Reporters Without Borders, March 17, 2016, https://rsf.org/en/news/renewed-calls-bassel-khartabils-release-4th-anniversary-detention.

59 Hania Mourtada, "'She Was My Mandela' – Famous Syrian Activist Gets Abducted," *Time*, December 11, 2013, http://ti.me/1KcXrTc.

60 Maha Assabalani, "My colleagues are in prison for fighting for free expression," UNCUT - Index on Censorship, May 11, 2012, http://bit.ly/1EYHMX9.

61 Jared Malsin, "Portrait of an Activist: Razan Ghazzawi, the Syrian Blogger Turned Exile," *Time*, April 2, 2013, http://ti.me/1Q46vKi.

62 An interview with Syrian blogger, February 2013, Skype.

63 Sara Yasin,"Syrian free speech advocates face terror charges," Index on Censorship, May 17, 2013, http://bit.ly/1VQg2IL.

64 Prominent Syrian activist Mazen Darwish freed" SKeyes, August 10, 2015, http://bit.ly/1GgvGK5.

65 Interview with Abu Ibrahim Raqqawi of Raqqa Is Being Slaughtered Silently, Skype.

66 "Law of the rulers to communicate on the network and the fight against cyber crime" art. 5-12. Informal English translation: https://telecomix.ceops.eu/material/testimonials/2012-02-08-Assad-new-law-on-Internet-regulation.html.

67 "Law of the rulers to communicate on the network and the fight against cyber crime" art. 2.

be blocked and is punishable by a fine of SYP 100,000 to 500,000 (US$1,700 to $8,600). If the violation is found to have been deliberate, the website owner or administrator may face punishment of three months to two years imprisonment as well as a fine of SYP 200,000 to 1 million (US$1,500 to $7,500).[68] In early 2014, however, the authorities were not vigorously enforcing these regulations.

In early November 2011, Bloomberg reported that the Syrian government had contracted Area SpA in 2009 to equip them with an upgraded system that would enable interception, scanning, and cataloging of all email, internet, and mobile phone communication flowing in and out of the country. According to the report, throughout 2011, employees of Area SpA had visited Syria and began setting up the system to monitor user communications in near real-time, alongside graphics mapping users' contacts.[69] The exposé sparked protests in Italy and, a few weeks after the revelations, Area SpA announced that it would not be completing the project.[70] No update is available on the project's status or whether any of the equipment is now operational.

One indication that the Syrian authorities were potentially seeking an alternative to the incomplete Italian-made surveillance system were reports of sophisticated phishing and malware attacks targeting online activists that emerged in February 2012.[71] The U.S.-based Electronic Frontier Foundation (EFF) reported that malware called "Darkcomet RAT" (Remote Access Tool) and "Xtreme RAT" had been found on activists' computers and were capable of capturing webcam activity, logging keystrokes, stealing passwords, and more. Both applications sent the data back to the same IP address in Syria and were circulated via email and instant messaging programs.[72] Later, EFF reported the appearance of a fake YouTube channel carrying Syrian opposition videos that requested users' login information and prompted them to download an update to Adobe Flash, which was in fact a malware program that enabled data to be stolen from their computer. Upon its discovery, the fake site was taken down.[73] Due to the prevailing need for circumvention and encryption tools among activists and other opposition members, Syrian authorities have developed fake Skype encryption tools and a fake VPN application, both containing harmful Trojans.[74]

A report from Kaspersky Labs, published in August 2014, revealed that some 10,000 victims' computers had been infected with RATs in Syria, as well as in other Middle Eastern countries and the United States. [75] The attackers sent messages via Skype, Facebook, and YouTube to dupe victims into downloading surveillance malware. One file was disguised as a spreadsheet listing names of activists and "wanted" individuals.

Anonymous communication is possible online but increasingly restricted. Registration is required to purchase a cell phone, though over the past years, activists have begun using the SIM cards of friends and colleagues killed in clashes with security forces in order to shield their identities. Cell phones from neighboring countries like Turkey and Lebanon have been widely used since 2012, no-

68 "Law of the rulers to communicate on the network and the fight against cyber crime" art. 8.

69 Ben Elgin and Vernon Silver, "Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear," *Bloomberg Business*, November 3, 2011, http://bloom.bg/1VQij6R.

70 Vernon Silver, "Italian Firm Said Exits Syrian Monitoring Project, Repubblica Says," *Bloomberg Business*, November 28, 2011, http://bloom.bg/1igDnoL.

71 Ben Brumfield, "Computer spyware is newest weapon in Syrian conflict" CNN, February 17, 2012, http://cnn.it/1LZPQXn.

72 Eva Galperin and Morgan Marquis-Boire, "How to Find and Protect Yourself Against the Pro-Syrian-Government Malware on Your Computer," Electronic Frontier Foundation, March 5, 2012, http://bit.ly/xsbmXy.

73 Eva Galperin and Morgan Marquis-Boire, "Fake YouTube Site Targets Syrian Activists With Malware," Electronic Frontier Foundation, March 15, 2012, http://bit.ly/1XQhHzX.

74 "Syrian Malware" Up-to-date website collecting the malware http://syrianmalware.com/.

75 Kaspersky Lab Global Research and Analysis Team, *Syrian Malware, the evolving threat*, August 2014, http://bit.ly/1pCJ0gK.

tably by Free Syrian Army fighters. However, civilians in Syria are now also using these foreign cell phones due to the lack of cell service in the country. Meanwhile, activists and bloggers released from custody report being pressured by security agents to provide the passwords of their Facebook, Gmail, Skype, and other online accounts.[76]

Intimidation and Violence

Once in custody, citizen journalists, bloggers, and other detainees reportedly suffered severe torture at the hands of government authorities. Although the precise number is unknown, it is estimated that dozens of individuals have been tortured to death for filming protests or abuses and then uploading them to YouTube.[77] In September 2015, it was confirmed that *al-Fida* newspaper's cartoonist Akram Raslan had died in state custody in 2013 due to sharing antigovernment cartoons on Arabic news sites and social media.[78] He had been arrested in October 2012 and it is believed he was tortured to death.[79]

According to Reporters Without Borders, seven "netizens" were killed during the coverage period, mostly for work as citizen journalists. Separately, in a video recording published by IS on June 26, 2016, five journalists—many of them whose work was primarily online—were brutally murdered. In at least two cases, IS militants had rigged the individuals' computers or cameras with explosives.[80] Citizen journalists have also been targeted by IS militants while in Turkey. Ibrahim Adul Kader of the human rights organization Raqqa is Being Slaughtered Silently (RBSS) was killed by IS militants in the city of Urfa, Turkey along with his friend Fares Hammadi in October 2015.[81] Naji Jaraf, editor-in-chief- of the opposition Hentah Magazine and an activist with RBSS, was shot and killed in the Turkish city of Gaziantep in December 2015.[82] Hundreds of activists have gone into hiding or fled the country, fearing that arrest may not only mean prison, but also death under torture.[83] Blogger Assad Hanna left Syria following online threats stemming from his criticism of the regime, but was badly injured by knife-wielding assailants at his apartment in Turkey in April 2015.[84]

In a move some observers called unprecedented, IS executed a female journalist in September 2015. Ruqia Hassan, also known as Nissan Ibrahim, was blogging about daily life in the city of Raqqa.[85] She was accused of being a spy for the Free Syrian Army. Shortly before her death, she reportedly com-

76 Interviews with released bloggers, names were hidden.

77 Interview A.A, Human Rights Lawyer, December 12, 2011, Damascus, Skype.

78 "Well-known Syrian cartoonist died in detention after being tortured," *Reporters Without Borders*, September 22, 2015, https://rsf.org/en/news/well-known-syrian-cartoonist-died-detention-after-being-tortured.

79 Ibrahim Naffee, "Cartoonist Raslan arrested in Syria," *Arab News*, October 16, 2012, http://www.arabnews.com/cartoonist-raslan-arrested-syria.

80 Enab Baladi Online, "ISIS Executes Five Journalists in Deir-ez-Zor," The Syrian Observer, June 27, 2016, http://syrianobserver.com/EN/News/31250/ISIS_Executes_Five_Journalists_Deir_Zor.

81 Lizzie Dearden, "Isis beheads 'Raqqa is Being Slaughtered Silently' activist and friend in Turkey," *Independent*, October 30, 2015, http://ind.pn/1Wm9dAh.

82 AP, "Reporters Without Borders urges Turkey to protect exiled Syrian journalists," US News and World Report, December 29, 2015, http://www.usnews.com/news/world/articles/2015-12-29/journalism-group-calls-on-turkey-to-protect-syrian-reporters.

83 Interviews with two photographers who have taken refuge in Turkey, December 2011.

84 Amira al Hussaini, "Syrian Blogger Stabbed in His Istanbul Home After Receiving Threats Online," *Global Voices Advocacy*, April 21, 2015, http://bit.ly/1jS03fb.

85 Aisha Gani and Kareem Shaheen, "Journalist Ruqia Hassan murdered by Isis after writing on life in Raqqa," *The Guardian*, January 5, 2016, http://bit.ly/1O8Gqbh.

plained of death threats stemming from IS. International journalists, including those whose work is mainly featured online, have also been killed by Syrian militant groups in previous years.[86]

Technical Attacks

Numerous reports from the past year have detailed the spillover of the country's conflict o the online sphere. According to the cybersecurity group FireEye, Russia's intelligence agency, the FSB, has stepped up technical attacks against Syrian human rights organizations and opposition groups in a major campaign to glean intelligence and disrupt reporting on Russian human rights violations.[87] In December 2014, the University of Toronto's Citizen Lab released a report entitled, "Malware Attack Targeting Syrian ISIS Critics," focusing on groups such as Raqqa is Being Slaughtered Silently (RSS), which documents human rights abuses committed by IS. Citizen Lab believes the malware was developed by IS or pro-IS hackers in order to discover more information about the nonviolent group.[88]

The Syrian Electronic Army (SEA) continues to target Syrian opposition websites and Facebook accounts, as well as Western or other news websites perceived as hostile to the regime. In March 2016, the FBI added three SEA members to its "Cyber Most Wanted" list.[89] The SEA made headlines after hacking major Western media outlets and organizations, including the websites of the *New York Times*,[90] the U.S. Marines,[91] Facebook,[92] and many others. Most of the attacks occurred on the DNS level, which involved redirecting requests for the domain name to another server. The Twitter account of Barack Obama, run by staff from Organizing for Action (OFA), was briefly hac ed by the SEA, resulting in the account posting shortened links to SEA sites.[93] The hackers had gained access to the Gmail account of an OFA staffer. On March 17, 2013, the SEA hacked the website and Twitter feed of Human Rights Watch, redirecting visitors to the SEA homepage.[94] These tactics continued with the high-profile hacking f *Forbes* in February 2014[95] and the *Washington Post* in May 2015.[96]

Though the hacktivist group's precise relationship to the regime is unclear, evidence exists of gov-

86 See Committee to Protect Journalists, "James Foley," *Journalists Killed/Syria*, 2014, https://cpj.org/killed/2014/james-foley.php, Committee to Protect Journalists, "Steven Sotloff," *Journalists Killed/Syria*, 2014, https://cpj.org/killed/2014/steven-sotloff.php, and Committee to Protect Journalists, "Kenji Goto," *Journalists Killed/Syria*, 2015, https://cpj.org/killed/2015/kenji-goto.php; I-fan Lin, "Hate Is Not What Humans Should Do: Slain Journalist Kenji Goto's Words Live On Online," *Global Voices*, February 7, 2015, http://bit.ly/1MyBlt1.

87 Sam Jones, "Russia steps up Syria cyber assault," *Financial Times*, February 19, 2016, https://www.ft.com/content/1e97a43e-d726-11e5-829b-8564e7528e54.

88 John Scott-Railton and Seth Hardy, *Malware Attack Targeting Syrian ISIS Critics*, CitizenLab, December 18, 2014, http://bit.ly/1JbRwMW.

89 James Temperton, "FBI adds Syrian Electronic Army hackers to most wanted list," *Wired*, March 23, 2016, http://www.wired.co.uk/article/syrian-electronic-army-fbi-most-wanted.

90 Christine Haughney and Nicole Perlroth, "Times Site Is Disrupted in Attack by Hackers," *New York Times*, August 27, 2013, http://nyti.ms/17krXEO.

91 Julian E. Barnes, "Syrian Electronic Army Hacks Marines Website," *The Wall Street Journal*, September 2, 2013, http://on.wsj.com/1KGVnFf.

92 Adario Strange, "Syrian Electronic Army Hacks Facebook's Domain Record," *Mashable*, February 5, 2014, http://on.mash.to/1EQuHPY.

93 Gregory Ferenstein, "The Syrian Electronic Army Hacked Obama's Twitter Links And Campaign Emails," *Tech Crunch*, October 28, 2013, http://tcrn.ch/1Xi62bV.

94 Max Fisher, "Syria's pro-Assad hackers infiltra e Human Rights Watch Web site and Twitter feed," *Washington Post*, March 17, 2013. http://wapo.st/1eU9nKI.

95 Andy Greenberg, "How the Syrian Electronic Army Hacked Us: A Detailed Timeline," *Forbes*, February 20, 2014, http://onforb.es/MEWYiq.

96 Brian Fung, "The Syrian Electronic Army just hacked the Washington Post (again)," *Washington Post*, May 14, 2015, http://wapo.st/1jS0eY7.

ernment links or at least tacit support. These include the SEA registering its domain in May 2011 on servers maintained by the Assad-linked Syrian Computer Society;[97] a June 2011 speech in which the president explicitly praised the SEA and its members;[98] and positive coverage of the group's actions in state-run media.[99]

97 The Syrian Electronic Army, http://sea.sy/index/en.

98 Haroon Siddique and Paul Owen, "Syria: Army retakes Damascus suburbs-Monday 30 January," *The Guardian*, January 30, 2012, http://bit.ly/1LZSDQA; Voltaire Network, "Speech by President Bashar al-Assad at Damascus University on the situation in Syria," June 20, 2011, http://bit.ly/1FzOUEp.

99 "The Syrian Electronic Army Fights Rumors and Gives the True Picture of the Incident," [in Arabic], *Wehda*, May 17, 2011, http://bit.ly/1OfOsCp.

Freedom House

Thailand

	2015	2016
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	9	10
Limits on Content (0-35)	22	23
Violations of User Rights (0-40)	32	33
TOTAL* (0-100)	**63**	**66**

* 0=most free, 100=least free

Population:	**68 million**
Internet Penetration 2015 (ITU):	**39 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- Social media users were put on trial for administering Facebook pages, "liking" posts, and even receiving an antiroyal comment in a Facebook Messenger exchange; decades-long prison sentences were handed down for online activity (see **Prosecutions and Detentions for Online Activities**).
- Proposed revisions to the Computer-related Crimes Act would permit censorship of any "inappropriate" content or platform and could undermine encryption (see **Legal Environment**).
- Plans for a single national internet gateway enabling censorship were ostensibly dropped following opposition, though observers remained wary (see **Restrictions on Connectivity**).
- Penalties in the April 2016 Referendum Act and official th eats hampered online discussion of a military-drafted constitution before a national referendum (see **Legal Environment**).

Introduction

Internet freedom declined in 2016 as the military leadership continued its efforts to codify censorship and surveillance powers through legislation.

General Prayuth Chan-ocha, former commander of the Royal Thai Army, continues to head the junta calling itself the National Council for Peace and Order (NCPO). The period since he seized power in the May 2014 coup has been characterized by increasingly extreme prosecutions of internet users for defamation and criticism of the monarchy. The longest sentence in the history of *lese majeste* cases, 60 years in prison reduced to 30 after a guilty plea, was passed during the coverage period of this report.

Successive governments have blocked tens of thousands of websites in Thailand, but censorship has become more severe and less transparent since 2014. In April, a Referendum Act imposed 10-year prison terms for influencing oters in an August referendum on a draft constitution, chilling online discussion of the document, which was ultimately approved. Problematic revisions to the Computer-related Crimes Act, the penal code, and other laws are also under consideration. Wide-ranging "digital economy" laws are still pending, despite criticism from academics and internet freedom activists about their implications for privacy and freedom of speech.

Since the coup, journalists, academics, and activists have been subject to overt surveillance, and military officials ha e interrogated hundreds of people, requiring them to give up their Facebook passwords as a condition of release. Documents leaked during the coverage period documented army and government agencies attempting to procure surveillance equipment as recently as December 2014, which General Prayut Chan-ocha denies. The military leadership was otherwise open about its efforts to step up control of the telecommunications infrastructure, interfering in a spectrum auction through executive order, and developing plans for a single national internet gateway which observers likened to China's Great Firewall.

Obstacles to Access

Internet penetration has increased steadily in recent years, in part thanks to affordable government-run access programs, though usage remains concentrated in Bangkok and other urban centers, and speed and quality of service can vary. After the May 2014 coup, officials declared their intention to establish a single gateway to the international internet, potentially enabling them to control or even shut down access nationwide. Plans to strip the regulatory National Broadcasting and Telecommunication Commission of its remaining independence continue to progress.

Availability and Ease of Access

Internet penetration was at 39 percent in 2015, up from 35 percent in 2014.[1] Most Thai internet and smartphone users reside in the Bangkok greater metropolitan and southern regions, which boast a higher average household income. The lowest penetration is in the northeast, in part due to lack of

1 International International Telecommunication Union, "Percentage of Individuals Using the internet, 2000-2015," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

service.[2] Connections functioned at average speeds of 20 Mbps, according to one 2015 report,[3] most reliably in the greater Bangkok area. This represented a significant inc ease over the 2014 average of 12 Mbps.

Mobile penetration fell from 144 to 126 percent in the same period, in part because of a campaign to disconnect unregistered SIM cards (see Surveillance, Privacy, and Anonymity). The number of active mobile numbers declined by over 10 million in 2015 after providers cleared inactive numbers. A February 2015 Cabinet resolution required registration of all pre-paid mobile users and free Wi-Fi users by July 31, 2015.[4]

The price of mobile data in Thailand has consistently declined since 2008, from THB 1.3 to 0.07 per kilobyte in 2015.[5] Thailand ranks fourth in Southeast Asia, behind Brunei, Singapore, and Cambodia, in terms of affordability, calculated by comparing price to the minimum wage.[6]

The NCPO continued the ICT Free Wi-Fi program initiated under the previous government. Although many users have complained of connectivity issues, such programs help 18 percent of Thai users to access the internet free of charge, while another 16 percent paid less than THB 200 ($6.73) a month, according to official 2015 fig es.[7]

In January 2016, the National Broadcasting and Telecommunications Commission (NBTC), Thailand's telecom regulator, and the Ministry of Information and Communication Technology (MICT) announced their collaboration to provide broadband internet access at a reasonable cost to all 70,000 villages nationwide by the end of 2016. The links will be made via both wireless and fi ed-line broadband access points.[8]

Restrictions on Connectivity

There were no reports of the state blocking or throttling internet and mobile connections for political or security reasons during the coverage period of this report, but the government was developing ways to do so in future by extending state control of the infrastructure.

Within a week of the May 2014 coup, the Deputy Minister of MICT announced plans to establish a "national digital internet gateway" through two state-owned companies, Communication Authority of Thailand (CAT) Telecom and TOT Telecom, and six other ISPs, with the explicit intention of enabling

2 Telecommunications Data and Research Center, "Report on the Survey of Thai People's Telecom Behavior 2012-2013," (in Thai) The National Broadcasting and Telecommunication Commission, http://www.nbtc.go.th/wps/PA_WCMLocalRendering/jsp/html/NTC/download/NBTC-SurveyReport2556.pdf.

3 "Thailand Internet 8th Fastest in Asia," *Bangkok Post,* May 21, 2015, http://www.bangkokpost.com/tech/local-news/568859/thailand-internet-8th-fastest-in-asia. Akamai reported average connection speed was 10.8 Mbps and average peak connection speeds of 69.6 Mbps in 2016. http://akamai.me/2ewzRnD.

4 NBTC, "Telecommunications industry : 2015 Q3 summary overview" (The National Broadcasting and Telecommunications Commission, September 2015), http://bit.ly/2fvJnfp.

5 NBTC, "Internet Market Report: Price/Kbps," http://www.nbtc.go.th/TTID/internet_market/price_kbps/.

6 "The cost of mobile data in Southeast Asia (INFOGRAPHIC)," *TechInAsia,* January 20, 2016, https://www.techinasia.com/cost-mobile-data-southeast-asia-infographic.

7 National Statistical Office, The 2015 Household Survey on the Use of Information and Communication Technology," http://service.nso.go.th/nso/nsopublish/themes/files/icthh_ eport_58.pdf.

8 "Broadband to reach 70,000 villages in 2016, *The Nation,* January 15, 2016, http://www.nationmultimedia.com/business/Broadband-to-reach-70000-villages-in-2016-30276930.html.

the MICT to interrupt access directly.[9] Access to the international internet gateway was previously limited to CAT until it opened to competitors in 2006.[10] In a June 30, 2015 resolution, the junta-appointed Cabinet ordered the MICT to proceed with "implementation of a single gateway to be used as a device to control inappropriate websites and flow f news and information from overseas through the internet system." This resolution, and others that reaffi med it, were not publicized until an internet user found directives describing the policy on government websites in September 2015.[11]

The resolution came under immediate attack from users and experts alike. Many saw it as a Chinese-style "Great Firewall," enabling censorship and personal data collection while undermining speed and security.[12] An online petition opposing the plan attracted over 150,000 signatures in less than two weeks.[13] Many users staged a "virtual sit-in," deliberately crashing government websites by reloading them continuously in their browsers at the same time to simulate a denial of service attack, and briefly disabled websites run by the Office of the Prime Minister, the Defence Ministry, MICT, and CAT Telecom.[14] After two weeks of intense public opposition, Deputy Prime Minister Somkid Jatusripitak said the plan had been halted.[15]

Many observers remain wary. In June 2015, the MICT had announced plans to set up a "national broadband company" to consolidate and spearhead the expansion of broadband access, primarily through CAT Telecom,[16] a project which some fear demonstrates that government control over the infrastructure is being expanded anyway.[17] In 2015, *TelecomAsia*, a telecom news website, received leaked documents which suggested that the single gateway project had been a military priority since 2006.[18]

Thailand's international bandwidth usage amounted to 2,510 Gbps in February 2016, and domestic bandwidth amounted to 3,510 Gbps,[19] 179 percent and 172 percent higher than same month in the previous year respectively.

ICT Market

Although 20 ISPs have licenses to operate in Thailand, high-speed internet is concentrated in a handful of large providers, and the trend points toward more concentration. According to

9 Thai Netizen Network, "Looking back at LINE: Thai government's attempts at surveillance," *Thai Netizen Network*, January 7, 2015, http://thainetizen.org/2015/01/thailand-chat-app-surveillance-timeline/.

10 World Bank, "Telecommunications Sector," *Thailand Infrastructure Annual Report 2008*, World Bank, accessed May 1, 2012, http://bit.ly/2fhMYgD

11 "Not only proposal: cabinet resolution presses for Single Gateway to control websites," *Blognone,* September 22, 2015, https://www.blognone.com/node/72775 (in Thai).

12 "To be or not to be: The great fi ewall of Thailand," *Al Jazeera America,* October 7, 2015, http://bit.ly/26nKj87

13 "Go against Thai govt to use a Single internet Gateway," *Change.org,* http://bit.ly/1PDXGHc.

14 "'Great Firewall of Thailand' under website attack as online users strike back," *The Sydney Morning Herald,* October 1, 2015, http://www.smh.com.au/world/great-fi ewall-of-thailand-under-website-attack-as-online-users-strike-back-20151001-gjyurx.html.

15 "Thailand scraps unpopular internet 'Great Firewall' plan," *Reuters,* October 15, 2015, http://www.reuters.com/article/us-thailand-internet-idUSKCN0S916I20151015.

16 "ICT accelerates plans to set up National Broadband Company," (in Thai), *Bangkok Biznews,* June 4, 2015, http://www.bangkokbiznews.com/news/detail/650144.

17 Don Sambandaraksa, "Thai deregulation experiment has failed," *TelecomAsia,* January 21, 2016, http://www.telecomasia.net/blog/content/thai-deregulation-experiment-has-failed.

18 "International hackers strike," *Bangkok Post,* October 22, 2015, http://www.bangkokpost.com/tech/local-news/739884/anonymous-steps-up-single-gateway-protest.

19 Internet Information Research Network Technology Lab, Internet Bandwidth, National Electronics and Computer Technology Center, http://internet.nectec.or.th/webstats/bandwidth.iir?Sec=bandwidth

statistics published in 2014, True Internet—a subsidiary of the communications conglomerate True Corporation, which also controls Thailand's third-largest mobile phone operator True Move—remained the market leader with nearly 40 percent market share, followed by TOT with 31 percent, and 3BB with 29 percent. Other providers serve a fraction of remaining users.[20] In July 2015, the National Telecommunication Commission (NTC), a branch of the NBTC which focuses on telecommunications, deemed that True Internet has "significant dominance" f the fi ed-line internet market. The NTC demanded that True submit details of its customers and services in order to determine the appropriate course of action, but had taken no further measures in mid-2016.[21]

The three main mobile phone service providers are the Singaporean-owned Advanced Info Service, the Norwegian-controlled DTAC, and True Move. The fi st two still operate some spectrum under concessions from state-owned TOT and CAT Telecom, an allocation system that hinders free-market competition.

Regulatory Bodies

The 11-member National Broadcasting and Telecommunication Commission (NBTC), an independent regulator viewed as broadly fair,[22] still managed the industry as of May 2016, but its authority was significantly e oded.

In December 2014 and January 2015, the Thai Cabinet approved a series of draft laws that would establish a Digital Ministry for Economy and Society and a Commission for Digital Economy and Society (CDES). The drafts included proposed amendments to the NBTC law which would transform it from an independent regulator to a government agency under CDES jurisdiction. The CDES would be empowered to penalize noncompliant government or private entities, and take over the allocation of spectrum for state and public interest uses, while the NBTC will only allocate spectrum for commercial use.[23] Many analysts believe this would retard Thailand's spectrum allocation and delay the planned release of spectrum being utilized commercially by military-owned media.

In January 2015, the Cabinet approved changing the ICT Ministry's name to Digital Ministry for Economy and Society—though the original name remains in common use—and restructuring it in accordance with the subcommittees outlined in the draft digital promotion law: hard infrastructure, soft infrastructure, service infrastructure, digital society, knowledge resources, and digital economy promotion.[24] The draft laws would also transfer assets belonging to the Broadcasting and Telecommunications Research and Development Fund (BTRDF) under the existing NBTC law to a new "Fund for Developing Digital for Economy and Society" (FDDES). While the BTRDF is considered to operate in the public interest, the FDDES would be used to finance digital economy opera ors, a potential conflict f interest.[25] Furthermore, the draft laws also stipulate that representatives from

20 NBTC, "Thailand Telecommunication Indicators Yearbook: 2013-2014" (Bangkok, Thailand: NBTC, 2014), http://bit.ly/2fBfVSQ

21 "NTC chided TRUE internet over 'too high market share' at 38.69" (in Thai), *Thairath Online,* July 1, 2015, http://www.thairath.co.th/content/508593.

22 Komsan Tortermvasana, "NBTC Approves Spectrum, Broadcasting Master Plans," *Bangkok Post*, March 22, 2012, http://www.bangkokpost.com/business/telecom/285448/nbtc-approves-spectrum-broadcasting-master-plan.

23 Thai Netizen Network, "weekly feedback after Cabinet approved 10 draft digital economy-cybersecurity laws," *Thai Netizen Network*, January 11, 2015, http://thainetizen.org/2015/01/digital-economy-cyber-security-bills-comments/.

24 Than News, "Deputy ICT Minister prepares for digital ministry," January 23, 2015, http://bit.ly/2fhS2S9

25 Thai Netizen Network, "Drafter insist: 'security' in draft cybersecurity bill is information security, not military security," *Thai Netizen Network*, February 3, 2015, http://thainetizen.org/2015/02/seminar-nbtc-surangkana-somkiat/.

state-owned TOT and CAT Telecom—which, as telecommunications providers, operate under license from the NBTC—would be appointed to the CDES. This would effectively give the regulated powers over the regulator, undermining the principle of free and fair competition.[26]

Civil society and private sector actors called the laws obstructive, and criticized the focus on creating new agencies with broad powers. After much public outcry (see "Digital Activism"), the government established the Preparation Committee for Digital Economy and Society chaired by junta leader General Prayuth Chan-ocha in lieu of the CDES.[27] At its first meeting in February 2016, the Committee approved the 20-year Digital for Economy and Society Development Plan.[28] New versions of the digital economy laws were still being drafted in mid-2016.

In April 2016, the Thai Cabinet approved a new frequency act that, if it becomes law, will formally strip the NBTC of independence, placing it under the jurisdiction of the Commission for Digital Economy and Society (CDES) chaired by the Prime Minister. The new National Broadcasting and Telecommunications Act calls for a single seven-member NBTC board (reduced from two five-member boards for broadcasting and telecommunications, plus one chairman). A committee consisting of high-ranking members of the judiciary and bureaucrats will select candidates for the board which the new Digital Economy Ministry will forward to the senate for approval; the Prime Minister will have the final say.[29] On May 31, 2016, the proposed law was pending review in the junta-appointed National Legislative Council.

The NBTC's failing authority was already evident. After issuing an order in July 2014 to delay a pending 4G spectrum auction for one year,[30] the NCPO finally allowed the 900MHz auction to go ahead in December 2015. The newcomer Jas Mobile Broadband (JAS), a subsidiary of Jasmine International, won the first licence block by quoting THB 75.6 billion, while True Move H Universal Communication (TUC) of True Corporation won the second block at THB 76.3 billion. The final price per capita MHz was described as one of the highest in the world.[31] After JAS defaulted on its instalment payment for the license in January 2016, junta leader General Prayuth Chan-ocha invoked Clause 44 of the interim constitution, commonly known as the "absolute power" clause, since it is final and cannot be appealed under any court. He ordered the NBTC to hold a new auction for the same spectrum on May 27, 2016, with a reserve price of THB 75.6 billion to match the JAS winning bid. The order also stated that the current spectrum holder, Advanced Info Services Plc. (AIS), could continue to serve its customers until June 30, or until the NBTC grants license to the new winner, whichever comes first.[32] AIS, the only bidder, readily won the auction at the reserve price.[33]

26 Thai Netizen Network, "Want real digital economy+cybersecurity? National Legislative Council must disapprove the whole set of draft digital economy laws," *Thai Netizen Network*, February 20, 2015, http://thainetizen.org/2015/02/seminar-cyberspace-law-security-privacy/.

27 Regulation of the Office of the Prime Minister: Preparation Committee for Digital Economy and Society, http://www.ratchakitcha.soc.go.th/DATA/PDF/2558/E/053/1.PDF

28 "ICT proposed four-stage, twenty-year digital economy plan: free Wifi, hi-speed internet, data center development," (in Thai), Manager Online, 8 February 2016, http://www.manager.co.th/Politics/ViewNews.aspx?NewsID=9590000013960

29 Don Sambandaraksa, "Thai telecom regulator weakened in new frequency act," *TelecomAsia,* April 25, 2016, http://www.telecomasia.net/content/thai-telecoms-regulator-weakened-new-frequency-act

30 Komsan Tortermvasana, "Regulator Confirms Delay in 4G Auctions," *Bangkok Post*, February 25, 2015, http://www.bangkokpost.com/business/telecom/483189/regulator-confirms-delay-in-4g-auctions.

31 "Who are real winners of 900MHz auction?" *Nation Multimedia,* December 21, 2015, http://www.nationmultimedia.com/business/Who-are-real-winners-of-900MHz-auction-30275326.html.

32 "It's official: new 4G auction due on May 27" *Bangkok Post,* April 12, 2016, http://www.bangkokpost.com/business/news/931165/its-official-new-4g-auction-due-on-may-2 .

33 Bangkok Post, "AIS wins 4G re-auction at B75.65bn," May 27, 2016, http://www.bangkokpost.com/news/general/991181/ais-wins-4g-re-auction-at-b75-65bn.

Limits on Content

Since the May 2014 coup, both the NCPO and the junta-appointed government have issued orders that prohibit online content perceived to criticize the Thai monarchy, the NCPO, or the government. Amendments to the Computer-related Crimes Act (CCA) under consideration during the coverage period would cement that practice. Self-censorship by journalists and social media users continued amid fresh warnings not to debate a draft constitution in advance of a national referendum. Despite more pervasive censorship and pressure from the authorities, online platforms allowed dissidents and activists to organize in opposition to the CCA amendments and other repressive developments, with some success.

Blocking and Filtering

During the reporting period, online censorship by the NCPO and MICT continued under NCPO orders issued after May 2014 coup. NCPO Announcement no. 17/2014 ordered ISPs to monitor and prevent dissemination of any information that distorts facts, could provoke disorder, or affects national security.[34] In January 2015, the NBTC, in its role as regulator, requested that every ISP monitor and censor online content that may cause conflict or disrupt peace and o der.[35] These orders empowered public officials at any le el, as well as ISP employees, to block websites directly using their own judgment. As a result, there are no longer official censo ship statistics.

Prior to the 2014 coup, the process to block websites was more rigorous, though it still lacked transparency. Article 20 of the 2007 Computer-related Crimes Act (CCA) authorizes MICT officials to request court orders to block content that is deemed a threat to natural security, or contravenes public morals or public order.[36] The government also censored content under special laws, such as the State of Emergency Act and Internal Security Act, which it invoked in 2010. The Thai government has been blocking some social and political content since 2007, though some controls on pornography, gaming, and other topics were announced earlier.[37]

In April 2016, a revised draft of the amended CCA was submitted to the National Legislative Assembly. Clause 20(4) would allow the government, under a newly established "computer information screening committee," to remove any online content or platform, including social media platforms such as Facebook and Line, if they are deemed "inappropriate," even without violating any law.[38] In addition, the amended Clauses 15 and 20 said the ICT Ministry would mandate decryption protocols to allow the government to access, block, or delete encrypted content.[39] There was strong opposition to the draft, which remained under review at the end of the coverage period (see Digital Activism).

Content that was most censored after the coup falls into two main categories: criticism of the Thai

34 iLaw, "Before-after coup: self-censorship, online media censorship, community radio shutdowns, and other incidents," *iLaw*, January 6, 2015, http://freedom.ilaw.or.th/blog/Other2014.

35 Thai Netizen Network, "Looking back at LINE: Thai government's attempt at surveillance," *Thai Netizen Network*, January 7, 2015, http://thainetizen.org/2015/01/thailand-chat-app-surveillance-timeline/.

36 Journalists sometimes refer to it as the "Computer Crime Act."

37 Karnjana Karnjanatawe, "Govt Forces ISPs to Block `Inappropriate' Web Sites," *Bangkok Post*, July 9, 2003, accessible at NARCHIVE Newsgroup Archive, http://bit.ly/19eoIgS.

38 "New computer crime law to give govt more control over content," *The Nation,* April 28, 2016, http://www.nationmultimedia.com/politics/New-computer-crime-law-to-give-govt-more-control-o-30284860.html.

39 "ICT Ministry to amend law to read encrypted websites," *Prachatai,* May 26, 2016, http://www.prachatai.com/english/node/6196

monarchy, and criticism of the NCPO or junta-appointed government. Blocked websites include foreign news websites such as Reuters and the UK-based *Daily Mail* newspaper; websites of human rights groups such as Human Rights Watch; academic websites such as Midnight University; personal websites of political bloggers and activists; and many Facebook and YouTube pages that contain anti-coup material.[40] None of the affected content was unblocked during the reporting period. Facebook was blocked entirely by MICT for about half an hour six days after the coup.[41]

The military government has also been ramping up its technical censorship capacity. One of the biggest developments in the past two years was the plan to route all internet traffic th ough a single internet gateway, dubbed by critics the "Great Firewall of Thailand" (see Restrictions on Connectivity). Although the government appeared to back down after intense public opposition, observers fear that the government may still be trying to consolidate gateway traffic th ough state-owned CAT Telecom to facilitate censorship and surveillance.

Content Removal

As with blocking, takedown requests were expedited and decentralized after the coup. The new process is highly unsystematic and uncoordinated. Arrests and intimidation frequently result in content removal (see Media, Diversity, and Content Manipulation, Prosecutions and Detentions for Online Activities, and Intimidation and Violence).

The CCA allows the prosecution of content providers or intermediaries—such as webmasters, administrators, and managers—accused of posting or allowing the dissemination of content considered harmful to national security or public order.[42] This potential liability encourages compliance with content removal requests. A draft law governing materials that incite dangerous behavior would also hold access providers liable for failing to remove such material from their systems if they know it exists (see Legal Environment). Announcement no. 12/2014 ordered social media users and operators to limit content that incites violence or provokes protests or opposition to NCPO rule.[43]

Companies also restrict access to some content. In early 2016, Facebook restricted access within Thailand to "GuKult," a satirical page that sometimes makes fun of the monarchy, replacing it with a message that read, "You're unable to view this content because local laws restrict our ability to show it."[44]

Facebook's "report" feature, which allows users to flag con ent which violates the site's terms, is separately used as a tool to temporarily suppress content. In 2015 and 2016, Facebook users and page administrators periodically complained that their content had been removed during harassment campaigns waged by other users, indicating that their opponents had reported it for contravening community guidelines, requiring them to appeal to the platform to have it reinstated.

40 Individual social media pages remained accessible through encrypted HTTPS connections. iLaw, "Online media censorship report after 22 May 2014 coup," *iLaw*, May 22, 2014, http://freedom.ilaw.or.th/blog/OnlineMedia2014.

41 "Thai ministry sparks alarm with brief block of Facebook," *Reuters,* May 28, 2014, http://reut.rs/2eWUbzM

42 The act states that "any service provider intentionally supporting or consenting to an offense…within a computer system under their control shall be subject to the same penalty as that imposed upon a person committing an offense." See, "An unofficial translation f the Computer Crime Act," *Pratachai,* July 24, 2007, http://www.prachatai.com/english/node/117.

43 iLaw, "Before-after coup: self-censorship, online media censorship, community radio shutdowns, and other incidents," *iLaw*, January 6, 2015, http://freedom.ilaw.or.th/blog/Other2014.

44 Asian Correspondent, "Facebook blocks page that mocks Thai monarchy," May 5, 2016, http://bit.ly/29957IO

Media, Diversity, and Content Manipulation

NCPO content regulations have increased self-censorship and undermined the diversity of information available on the internet in Thailand.

NCPO Announcement no. 18/2014 banned news reporting that disrupts national security, peace, and order.[45] Journalists, editors, and media personalities who report stories that are critical of the government or NCPO are routinely summoned for "attitude adjustment" with the military, which can last up to seven days without charge under NCPO Announcement no. 3/2015. As a result, mainstream media outlets and reporters by and large choose to self-censor. In February 2016, the ministry of foreign affairs issued new guidelines for foreign journalists working in Thailand for longer than three months, introducing discretionary powers to deny visas for disrupting public order or the security of the kingdom," in language similar to NCPO orders regulating Thai media.[46]

The minority who still attempted to convey criticism of the NCPO continued to face harassment during the coverage period. Notable cases include Pravit Rojanaphruk, then-senior reporter at *The Nation* (he later moved to *Khao Sod English*), who was blindfolded and taken to an undisclosed location for three days of interrogation in September 2015. He was told that his offense was "tweeting and posting comments questioning the legitimacy of the NCPO and its leader."[47] After the coup in 2014, Pravit was also summoned for seven days. Separately, in October 2015, Sakda Saw-lew, the political cartoonist known as Sia who draws for Thailand's largest daily newspaper, *Thai Rath*, was "invited" to report to army headquarters to discuss his critical cartoons, which are frequently shared online.[48] This was also the second time he had been summoned.

Ordinary internet users were warned not to discuss a constitution drafted by the military in advance of a national referendum to approve its adoption, threatening the diversity of opinions online. In March 2016, General Teerachai Nakvanich, army chief and secretary-general of the NCPO, ordered an "immediate crackdown" on any action the government believes will lead people to "misunderstand" or be "confused" about the government's work before the referendum, which was scheduled for August.[49] A law passed in April 2016 governing the referendum process carries harsh prison terms for "influencing" oters, undermining freedom of expression (see Legal Environment). However, social media platforms like Facebook and Twitter still offered a vital platform for Thai people to express their opinions and criticize the government (see Digital Activism).

There was no public documentation of paid actors manipulating political content on the internet during the coverage period, though there were organized efforts to restrict political engagement online. Officials ffered financial incenti es to citizens to monitor one another online (see Surveillance, Privacy, and Anonymity), and many organized informally to harass the junta's opponents (see Intimidation and Violence).

A number of outspoken activists and academics have fled Thailand since the coup, but emain active

45 iLaw, "Before-after coup: self-censorship, online media censorship, community radio shutdowns, and other incidents," *iLaw*, January 6, 2015, http://freedom.ilaw.or.th/blog/Other2014.

46 Committee to Protect Journalists, "Thailand tightens visa requirements for foreign reporters," February 19, 2016, https://cpj.org/2016/02/thailand-tightens-visa-requirements-for-foreign-re.php.

47 Pravit Rojanaphruk, "How Thailand's Military Junta Tried to 'Adjust My Attitude' in Detention," *The Diplomat,* September 23, 2015, http://thediplomat.com/2015/09/how-thailands-military-junta-tried-to-adjust-my-attitude-in-detention/.

48 "Thai Rath cartoonist Sia reports to NCPO," *Bangkok Post,* October 4, 2015, http://www.bangkokpost.com/print/717232/.

49 "Army boss orders crackdown on 'confusing' dissent," *Bangkok Post,* March 28, 2016, http://www.bangkokpost.com/news/politics/913064/army-boss-orders-crackdown-on-confusing-dissent.

on social media. For example, Somsak Jiamteerasakul and Pavin Chachavalpongpun, two prominent academics, relocated abroad and continue to publish commentaries and political analysis via Facebook. Being physically outside the country allows them to be more outspoken.

Digital Activism

Social media platforms such as Facebook and Twitter, chat applications such as Line, and online petition sites such as Change.org have become indispensable as more Thais access the internet. Since the coup, many bloggers, activists, and human rights lawyers have formed coalitions such as Thai Lawyers for Human Rights (TLHR) to monitor the situation and document human rights violations by the junta. Anonymously operated Facebook pages allow individuals to share their opinions and organize political activities, including *Stop Fake Thailand,* which has over half a million followers.

Two recent online campaigns are notable for their success in rallying users to defend internet freedom. The Foundation for Internet and Civic Culture (Thai Netizen Network) gathered over 20,000 signatures opposing the junta's draft digital economy laws in February 2015, leading the government to announce that the drafts would be improved.[50] Separately, a Change.org campaign set up in September 2015 to oppose the "single gateway" plan attracted over 150,000 signatures in less than two weeks, prompting the deputy prime minister to announce that the plan had been scrapped, though observers remained sceptical (see Restrictions on Connectivity).

A third campaign was ongoing in mid-2016. A user-mounted campaign to oppose amendments to the Computer-related Crimes Act (see Blocking and Filtering) had gathered over 34,000 signatures as of June 30.[51]

Violations of User Rights

Internet users, bloggers, citizen journalists, and independent media practitioners continued to face persecution in 2015 and 2016. In addition to problematic draft digital laws that remain pending, legislation to suppress materials that incite dangerous behavior, as well as amendments to the CCA and the penal code could further erode internet freedom. The longest prison sentences for criticizing the monarchy were documented during the reporting period, and dozens of people were detained or interrogated for legitimate online speech.

Legal Environment

Clause 45 of the Constitution of the Kingdom of Thailand 2007 guaranteed broad freedom of speech, but was replaced with a 2014 interim constitution after the May coup d'etat. Although it maintains the same safeguards, Thailand remains subject to various NCPO orders which prohibit individuals and the media from any public political activity.

50 Bangkok Post, "21,000 Oppose New Cyber Laws," February 3, 2015, 00, http://www.bangkokpost.com/news/general/465262; Thai Netizen Network, "4 civil society organizations asked Constitution drafters, NLA, NRC to review 'digital security' laws," *Thai Netizen Network*, February 3, 2015, http://thainetizen.org/2015/02/civil-society-groups-submit-letters-legislators-cybersecurity-concerns/.

51 "Change.org: stop Single Gateway, stop privacy intrusion law," https://www.change.org/p/ค้นซ-หยุด-single-gateway-หยุดกฎหมายล้วงข้อมูลส่วนบุคคล (in Thai).

Internet users are frequently charged under Clause 14 of the 2007 Computer-related Crimes Act (CCA), pertaining to content that affects national security, and Clause 112 of the criminal code pertaining to *lese majeste*, or criticism of the monarchy. Defamation is a criminal offense under the penal code, and Clause 14(1) of the CCA criminalizes "bringing false computer information into the system," which has been used to punish alleged libel (see Prosecutions and Detentions for Online Activities).

Many NCPO decrees and orders criminalize speech, and NCPO announcements 37/2014, 38/2014, and 50/2014 also expanded military court jurisdiction over civilians, including violations of Clause 116 of the penal code, the equivalent of sedition, which punishes actions that "aim to change the government, create unrest amongst people, or cause people to transgress the law" with a maximum seven years' imprisonment. Clause 116 has been used to charge politicians, human rights defenders, students, and individuals who peacefully express critical opinions of the junta government. At least 47 people were arrested under the clause between the coup and the end of this coverage period, and several were subsequently charged and sentenced.[52]

The military court has no appellate or higher division, and has handed down more severe punishments than civilian judges. In *lese majeste* cases judged between 2010 and 2015, regular courts handed down average jail terms of 4.4 years out of a possible 3-15 years. Sentences issued by martial courts are much higher. In August 2015, separate military courts in Bangkok and Chiang Mai found two internet users guilty of *lese majeste* over Facebook posts, and handed down jail terms of 60 and 58 years respectively before guilty pleas reduced the final erdicts. These marked the highest imprisonments ever recorded in Thailand for *lese majeste* offences (see Prosecutions and Detentions for Online Activities).[53]

Military control was further entrenched during the coverage period. On March 29, 2016, General Prayuth Chan-ocha issued NCPO Announcement no. 13/2016, allowing military office s and anyone appointed by the junta leader to arrest anyone who commits one of 27 categories of crimes, including those considered to involve threats to "public peace." They can also carry out search, seizure, and any other act instructed by the NCPO, with impunity.[54] Local and international human rights organizations feared the order will be used to silence dissent.[55]

In April, the Referendum Act was introduced to govern a national referendum on a draft constitution scheduled for August. Clause 62 punishes anyone "deceiving, forcing, or influencing a oter" with up to 10 years' imprisonment or fines up o THB 200,000.[56] Critics said this broad wording effectively criminalized free speech and campaigning.[57] In June, after the coverage period of this report, the Constitutional Court upheld the law,[58] and the referendum approved the military-drafted constitution in August.[59]

52 iLaw, "Politically charged cases since May 2014 coup" (in Thai), http://freedom.ilaw.or.th/politically-charged.

53 iLaw, "Politically charged cases since May 2014 coup."

54 Thai Lawyers for Human Rights, "A legal opinion by the Thai Lawyers for Human Rights (TLHR) concerning the Order of the Head of the National Council for Peace and Order (NCPO) no.13/2016," April 6, 2016, https://tlhr2014.wordpress.com/2016/04/08/legal_opinion-order_of_head_of_ncpo_no13-2016/.

55 FIDH, "Human rights groups condemn NCPO Order 13/2016 and urge for it to be revoked immediately," https://www.fidh.org/en/region/asia/thailand/human-rights-groups-condemn-ncpo-order-13-2016-and-urge-for-it-to-be.

56 "Bill warns of jail for referendum 'crimes'," *The Nation,* April 7, 2016, http://bit.ly/2eWXNlb

57 South China Morning Post, "New Thai law carries 10-year jail sentence for campaigning in build-up to referendum on new constitution," April 23, 2016, http://bit.ly/2fhUzvR

58 "Referendum law not unconstitutional, court rules," *The Nation,* June 29, 2016, http://bit.ly/2fGlWxT

59 BBC News, "Thai referendum: Military-written constitution approved," August 7, 2016, http://bbc.in/2aReRZU

The digital economy package of 10 draft laws was still under consideration during the coverage period (see Regulatory Bodies).[60] The draft Commission for Digital Economy and Society (CDES) law stipulates that CDES would have authority over every other ministry and government agency, including the power to initiate disciplinary action against any government official or citizen that does not comply with their orders.[61] The draft cybersecurity law would also grant authorities lawful interception powers without a warrant, based on a perceived threat which is not properly defined.

A revised criminal procedural law also pending before the National Legislative Council separately grants surveillance powers to authorized police officials. The dra t stipulates a wide range of offenses for which surveillance is lawful; in addition to violations of national security and organized crime, it includes very broad categories like "complex" crimes.[62]

Under a separate draft law for the prevention and suppression of materials that incite dangerous behavior, officials ould require a warrant to access any private information that is deemed to provoke dangerous behavior such as sexually deviant acts, child molestation, or terrorism. Creating and distributing such information would be punishable by one to seven years in prison and fines up to THB 700,000. Access providers (as defined by the CA) that know such information exists in the computer system under their control but fail to remove it also face a maximum 5-year jail term and THB 500,000 fine[63]

A revised draft of the amended Computer-related Crimes Act was also submitted to the National Legislative Assembly in April 2016, sparking opposition (see Blocking and Filtering). At the end of the coverage period, all of these draft laws were under review pending submission to the National Legislative Assembly.

Besides the problematic content of these laws, critics called the lawmaking process—which lacked participation from relevant stakeholders or public hearings—rushed and secretive. The Electronic Transactions Development Agency director, who heads the legal drafting team, said the top-down drafting process resulted from the urgency of the policy for the interim government.[64]

Prosecutions and Detentions for Online Activities

Prosecutions and detentions of internet users increased in frequency and became more extreme during the reporting period, as military or police office s interpreted even symbolic acts of dissent as national security threats violating the CCA and various NCPO announcements.

Four cases stand out as examples that suppressed freedom of speech in Thailand's online space:

60 Thai Netizen Network, "Thailand's Digital Economy-Cyber Security Bills [English Translation]," *Thai Netizen Network*, January 15, 2015, http://thainetizen.org/2015/01/digital-economy-cyber-security-bills-en/.

61 Thai Netizen Network, "Sittichai Pokai-udom: don't worry, we based cybersecurity law on Homeland Security Act; government entity is guilty if it does not obey order of digital committee," *Thai Netizen Network*, February 6, 2015, http://thainetizen.org/2015/02/sitthichai-digital-economy-homeland-security/.

62 iLaw, "Draft criminal procedural law amendment: add wiretap authority, anyone exercising Miranda right is to be speculated guilty," *iLaw.or.th*, January 17, 2015, http://ilaw.or.th/node/3400.

63 Thai Netizen Network, "ICT Laws under NLA: wiretap powers in 4 laws not just 'cybersecurity'; media academic insists "spectrum belongs to all of us"," *Thai Netizen Network*, January 25, 2015, http://thainetizen.org/2015/01/seminar-ict-laws-nbtc-nida; iLaw, "draft prevention and suppression of materials that incite dangerous behavior law: child protection, or rights violation?," *iLaw.or.th*, February 10, 2015, http://ilaw.or.th/node/3485.

64 Thai Netizen Network, "Drafter insist: 'security' in draft cybersecurity bill is information security, not military security," *Thai Netizen Network*, February 3, 2015, http://thainetizen.org/2015/02/seminar-nbtc-surangkana-somkiat/.

- Eight internet users were arrested in April 2016 and charged under Clause 116 of the penal code and Clause 14 of the CCA. They collectively ran "We Love Gen Prayut," a satirical Facebook page with over 70,000 followers famous for popularizing memes and doctored photos of General Prayut Chan-ocha accompanied by satirical quotes. They were denied bail by the military court; the case was pending trial in mid-2016.[65]

- Thanakorn, a 27-year-old factory worker, was arrested on December 8, 2015 for sharing infographics on Facebook linking General Prayut Chan-ocha and other NCPO members to a scandal involving Rajabhakti Park. Media reports have accused high-level army officers of accepting kickbacks during construction of the park, newly built on army-owned land in Prachuab Kiri Khan province to honor past Thai kings.[66] Thanakorn was held at an undisclosed location for seven days, raising fears over his disappearance,[67] then charged with violating the CCA and Clause 116 of the penal code. He was additionally accused of committing *lese majeste* for "liking" a Facebook page deemed to contain *lese majeste* content, and for posting a sarcastic comment under an image of the royal dog.[68] He was released on THB 500,000 bail in March 2016, after 86 days in custody. His case is pending trial in the military court, and marks Thailand's first prosecution for "liking" content on Facebook.[69] Separately, Jaem (pseudonym) was arrested in November 2015 for violating the CCA and Clause 116 of the penal code, for alleging on Facebook that several high-ranking members of the NCPO are implicated in the Rajabhakti Park corruption scandal. She was released from custody on THB 100,000 bail. In mid-2016, a military prosecutor was still considering whether to bring the case to trial.[70]

- Theerawan Charoensuk, 57, was arrested in Chiang Mai on March 29, 2016 under Clause 116 of the penal code. Theerawan had shared a photo of herself on Facebook, holding a red water bowl and a Thai New Year poster from former Prime Ministers Thaksin and Yingluck Shinawatra. The photo was also printed in the daily *Thai Rath*. Theerawan said she found the poster and bowl in a temple where she was participating in a religious ceremony. She was released on THB 100,000 bail pending military trial in mid-2016.[71]

- Patnaree Chankij, the mother of a prominent student activist, was charged with *lese majeste* for "failing to criticize or take action against *lese majeste* comments" made by a friend of her son in a private exchange on Facebook Messenger. The military court granted THB 500,000 bail, and her case was pending trial in mid-2016.[72]

65 "'Facebook 8' remain in jail," *Bangkok Post,* April 29, 2016, http://www.bangkokpost.com/news/politics/953229/no-bail-for-facebook-8.

66 Saksith Saiyasombut, "Rajabhakti Park: The corruption case the Thai junta doesn't want you to talk about," *Asian Correspondent,* December 17, 2015, https://asiancorrespondent.com/2015/12/rajabhakti-park-controversy/.

67 "Thailand: Junta Critic Feared 'Disappeared'," *Human Rights Watch,* December 11, 2015, https://www.hrw.org/news/2015/12/11/thailand-junta-critic-feared-disappeared.

68 "Thai man faces jail for insulting king's dog with 'sarcastic' internet post," *The Guardian,* December 15, 2015, http://www.theguardian.com/world/2015/dec/15/thai-man-faces-jail-insulting-kings-dog-sarcastic-internet-post.

69 iLaw, "Thanakorn: Clicking "Like" on Facebook Page and made sarcastic remark on the royal dog," http://freedom.ilaw.or.th/case/702.

70 "Cham: Facebook post about Rajabhakti Park," (in Thai) *iLaw,* 2015, http://freedom.ilaw.or.th/case/707.

71 "Clause 116 charge: woman photographed with red bowl; released on 100,000 Baht bail from military court," *Thai Lawyers for Human Rights,* March 29, 2016, https://tlhr2014.wordpress.com/2016/03/29/redbowl_sedition/.

72 "Human Rights Watch condemns arrest of Ja New's mother," *The Nation,* May 7, 2016, http://www.nationmultimedia.com/breakingnews/Human-Rights-Watch-condemns-arrest-of-Ja-News-moth-30285482.html.

Internet users were also sentenced during the coverage period:

- On August 7, 2015, military courts in Bangkok and Chiang Mai sentenced a man and a woman to 30 and 28 years in prison respectively, in separate cases involving Facebook posts deemed critical of the monarchy. The sentences were reduced from 60 and 56 years after the defendants pleaded guilty. The court sentenced Pongsak (pseudonym) to 10 years in prison for each of 6 Facebook posts,[73] while Sasivimol (pseudonym) was convicted to 8 years in prison for 7 posts.[74] The Office f the United Nations High Commissioner for Human Rights called them the highest sentences imposed for *lese majeste* since they began documenting them in 2006.[75] Police also arrested Chayo (pseudonym), an individual in Pongsak's Facebook Messenger contacts, on the same charge based on private statements and photos deemed *lese majeste*.[76] In December 2015, the military court in Srakaew province sentenced him to 18 years in prison, reduced to 9 years after he entered a guilty plea.

- In July 2015, a Bangkok military court sentenced each of the eight alleged members of an online "antimonarchy network" to fi e years in prison. Two other people who were deemed sympathizers got three-year sentences.[77] In early 2015, the Department of Special Investigations, which is tasked with identifying and tracking down anonymous online authors of content deemed *lese majeste*, announced that it had broken up the so-called "Banpot Network", which they accused of distributing hundreds of podcasts with information and political commentary critical of the royal family over the past three years, including its alleged founder, Hassadin "Banpot" Uraipraiwan.

- Thanes (pseudonym) has been in custody since July 2014 for allegedly sending a link to *lese majeste* content to a foreigner by email in 2010. In June 2015, a criminal court sentenced him to 5 years in prison, reduced to 3 years and 4 months for offering useful testimony.[78]

- Piya (pseudonym) was accused of publishing *lese majeste* content on a Facebook account in December 2014, though he denied operating the account. In January 2016, a criminal court sentenced him to 9 years in prison, reduced to 6 years for offering useful testimony.[79]

Besides *lese majeste* and political speech, libel is a longstanding problem in Thailand. Clause 14(1) of the CCA criminalizes "bringing false computer information into the system." Suing people under this clause concurrently with the charge of libel has become the norm. Attorney generals and judges have shown no understanding of the differences between the two laws, nor the fact that "false computer information" means technical crimes such as hacking, not the veracity of online speech. The vast majority of plaintiffs in these cases are government officials or la ge corporations.

During the reporting period, at least one court demonstrated an improved understanding of the Computer-related Crimes Act, acquitting a *Phuketwan* editor and journalist sued by the Royal Thai

73 "Pongsak: Posted *lese majeste* messages on Facebook." *iLaw*, 2015. http://freedom.ilaw.or.th/case/650.

74 "Sasivimol: Posted *lese majeste* messages on Facebook." *iLaw*, 2015. http://freedom.ilaw.or.th/en/case/681.

75 ICJ and Thai Lawyers for Human Rights, "Submission to the Universal Periodic Review (UPR) of Thailand," September 2015, http://www.icj.org/icj-and-thai-lawyers-for-human-rights-submission-to-the-universal-periodic-review-upr-of-thailand/.

76 iLaw, "Freedom of Expression Bulletin January 2015," (in Thai) *iLaw*, February 4, 2015, http://freedom.ilaw.or.th/blog/FOEBulletinJan2015.

77 "Banpot Network," (in Thai) *iLaw,* 2015, http://freedom.ilaw.or.th/th/case/670.

78 Tanet (in Thai), iLaw (Criminal Court 2014).

79 Piya (in Thai), iLaw (Criminal Court 2014). http://freedom.ilaw.or.th/en/case/645

Navy for re-publishing a Pulitzer prize-winning Reuters article accusing Navy officials f profiting from a refugee smuggling ring. Editor Alan Morison and reporter Chutima Sidasathian were charged with criminal defamation and an offence under the CCA. On September 1, 2015, the court acquitted both accused on all counts, ruling that the CCA was not intended to be used in defamation cases. The website shut down in 2015 because of the uncertainty during the trial,[80] and in May 2016 had not been restored.

Another case also saw a more positive outcome, though still based on a misinterpretation of the false information clause. Maitree, a citizen journalist of Lahu ethnic descent, was sued by the military for violating Clause 14(1) of the CCA. On January 1, 2015, he videotaped an incident in his village in which a villager was slapped by a soldier, then shared the footage on his personal Facebook account. The military alleged that he violated Clause 14 because the content of the video clip was "false information" that damaged the reputations of the soldiers involved. On March 9, 2016, a criminal court in Chiang Mai acquitted Maitree, saying he posted the video clip because he believed it was true; his action would be an offense under Clause 14(1) only if "he was aware that the information he posted were false."[81]

However, these two court verdicts remain a minority in the overall trend of courts handing out guilty verdicts under the CCA for supposedly libelous online content. For example, Natural Fruit, a canned fruit company, sued migrant labor rights activist Andy Hall over dissemination of research reports that allege violations of labor rights in the company's plants. The company sued him in three separate cases, one of which uses the computer-related crimes law because the report was disseminated online. The cases were being tried in a criminal court during the reporting period;[82] in September 2016, Hall was sentenced to a suspended three-year prison term and a THB 150,000 fine [83]

As in past years, a number of computer crimes charges filed against jou nalists or public persons for alleged libel were dropped or dismissed, suggesting they lacked merit, but were filed o intimidate the defendant. In August 2015, a criminal court in Mae Sot indicted Suraphan Rujichaiwat, a community-based human rights defender from Loei Province, on charges of criminal defamation and violating Clause 14(1) of the CCA. Suraphan was sued by Tungkhum, a mining company in dispute with the community about its environmental impact. The plaintiff dropped the charge in March 2016.[84] In December 2015, the same company sued Wanpen Khunna, a 15-year-old student in Loei province who had helped document the mine's impact on villages for ThaiPBS, Thailand's public broadcaster.[85] In mid-2016, the case was pending trial.

Surveillance, Privacy, and Anonymity

A number of NCPO decrees and orders specifically manda e surveillance of online media. NCPO

80 Lindsay Murdoch, "Crusading Phuketwan website shut down as journalists face Thai court," *Sydney Morning Herald,* July 12, 2015, http://www.smh.com.au/world/crusading-phuketwan-website-shut-down-as-journalists-face-thai-court-20150712-giacup.html

81 "Maitree: disseminating clip that defamed the soldier," *iLaw,* 2015, http://freedom.ilaw.or.th/th/case/669.

82 Andy Hall: Computer Crimes Case, iLaw (Criminal Court 2014). http://freedom.ilaw.or.th/en/case/469

83 http://www.bbc.com/news/world-asia-37415590

84 iLaw, "March 2016 report," http://freedom.ilaw.or.th/report/march2016.

85 "Mining fi m seeking to sue schoolgirl, 15," *The Nation,* December 15, 2015, http://www.nationmultimedia.com/national/Mining-fi m-seeking-to-sue-schoolgirl-15-30274935.html.

order no. 26/2014 mandated surveillance and monitoring of social media by military agencies.[86] Pending draft laws also include provisions that will grant police and other agencies overbroad surveillance powers (see Legal Environment).

Thai government officials f equently announce that they are monitoring private communication on chat applications such as LINE,[87] and actively seeking cooperation from social media platforms such as Facebook. In 2015, Facebook reported that it received three user requests from the junta government, but produced no data in response.[88] In May 2016, following the arrests of eight Facebook page administrators (see Violation of Users Rights), Facebook reiterated that it had not shared users' private communications with the junta.[89]

Internet users and journalists have reported that the Department of Special Investigations is pursuing an aggressive surveillance policy, joining private chat groups on the social messaging service LINE, creating Facebook accounts in order identify the authors of "illegal" messages, and even "baiting" some people to criticize the monarchy or the junta in order to arrest them.[90] In several cases where individuals were summoned or arrested, the authorities confisca ed smartphones to peruse personal information and photos, or check for potential links to other people.

In June 2014, Somyot Poompanmuang, Deputy Commissioner of the Royal Thai Police, publicly invited Thai people to "serve as eyes and ears" of the state by submitting images of anti-coup symbols displayed in public and online to police. He offered a monetary reward of THB 500 for photos that result in an arrest. He also urged the public to inform the police via the *Jah Hook* ("Owl Sergeant") Facebook page.[91] The Cyber Scout program, which began in 2011 under the ICT and education ministries, trains students to monitor and report online behavior they deem a danger to national security. In 2015, there were over 120,000 cyber scouts nationwide, spanning 88 schools. The curriculum stresses recruiting new members and training cyber scout leaders.[92]

During the reporting period, several revelations shed more light on the inner workings of Thailand's technical surveillance apparatus. In July 2015, leaked internal documents belonging to Milan-based Hacking Team revealed that a number of government agencies in Thailand bought spyware from them between 2012 and 2014. Those agencies included the Royal Thai Police, the National Security Council, the Royal Thai Army, and the Department of Corrections under the Ministry of Justice. Correspondence between National Security Council and Hacking Team revealed that the Thai intelligence wanted the ability to eavesdrop on popular messaging programs, especially Line, Skype, and WhatsApp.[93] Police spokesman Pol. Lt. General Prawut Thawornsiri said reports of the 2012 deal with Hacking Team were "groundless" because "surveillance on citizens was illegal and

86 iLaw, "Before-after coup: self-censorship, online media censorship, community radio shutdowns, and other incidents," *iLaw*, January 6, 2015, http://freedom.ilaw.or.th/blog/Other2014.

87 iLaw, "Before-after coup.".

88 Facebook, "Government Requests Report: Thailand 2015," https://govtrequests.facebook.com/country/Thailand/.

89 Asian Correspondent, "Thailand: Facebook denies sharing user information with military," May 11, 2016, https://asiancorrespondent.com/2016/05/thailand-facebook-sharing-info-military/.

90 Reporters without Borders, *Media Hounded by Junta Since 2014 Coup.* November 2015, https://rsf.org/en/news/thai-juntas-persecution-media.

91 Thai Netizen Network, "Looking back at LINE: Thai government's attempts at surveillance."

92 MICT, "ICT Ministry continues expanding Cyber Scout network to help online society," *MICT*, May 26, 2015, http://bit.ly/1Mczefe; MICT, "ICT Ministry joined forces with 88 schools, expanding Cyber Scout network to help take care of clean online society," *MICT*, March 6, 2015, http://bit.ly/2fLQ26u.

93 Don Sambandaraksa, "Even HackingTeam gets fed up with corruption in Thailand," *TelecomAsia,* September 17, 2015, http://www.telecomasia.net/blog/content/even-hackingteam-gets-fed-corruption-thailand.

ran counter to national police agency policy."[94] General Prayut Chan-ocha, who was head of the Royal Thai Army at the time the procurement was approved, also denied the reports. According to emails documented in the leak, the Royal Thai Army was in the process of buying spyware worth EUR 360,000 as of December 2014.[95] The company's Remote Control System software would give the junta the ability to intercept communications, remotely activate a mobile phone's microphone and camera, and access all of the phone's content including contacts and messages without the user's knowledge.[96]

From August 2015 onwards, users of pre-paid mobile phone cards and free Wi-Fi nationwide in Thailand must be registered pursuant to a February 2015 Cabinet resolution. Every user must supply their full name and ID or passport number, or lose service. Partly as a result of this blow to online anonymity, the number of mobile numbers in Thailand declined during the reporting period (see Availability and Ease of Access).[97]

Intimidation and Violence

In addition to charging internet users, the NCPO uses extrajudicial measures to intimidate its opponents. In one prominent 2016 case, Sarawut Bamrungkittikhun, administrator of the Facebook page *Peod Praden* ("Open Issue"), which is critical of the junta government, was abducted from his residence in Surat Thani province, his laptop and mobile confisca ed, transported to Bangkok and held in an undisclosed military barracks for seven days.[98] Sarawut subsequently terminated his Facebook page.

After the May 2014 coup, the NCPO summoned hundreds of people for questioning in order to suppress potential dissent, often through public announcements in the media. Summons to "attitude adjustment" at military barracks continued in 2015 and 2016, but were made via phone calls or by post. The NCPO also diversified their intimidation methods, making epeated home visits unannounced, threatening family members, or issuing mandatory "invitations" for coffee or meals. During interrogations, individuals reported being required to sign written agreements promising not to voice political opinions or criticize the NCPO. A number of people were ordered to reveal their Facebook passwords.[99]

In 2015, at least 234 people were summoned or visited by the military.[100] Watana Muangsook, a politician with the Pheu Thai party of former Prime Ministers Thaksin and Yingluck Shinawatra, was summoned multiple times without charge after expressing disagreements with the junta on Facebook, including over the draft constitution.[101]

94 "Police deny plans to spy on people's e-mails, mobiles," *Nation,* July 21, 2015, http://bit.ly/2eWVePX

95 "Prayut denies army procurement of spyware-counters "Wikileaks," insists never hires hackers for surveillance" (in Thai), *Manager Online,* July 21, 2015, http://www.manager.co.th/Politics/ViewNews.aspx?NewsID=9580000082541.

96 Reporters without Borders, *Media Hounded by Junta Since 2014 Coup.* November 2015, https://rsf.org/en/news/thai-juntas-persecution-media.

97 Khaosod English, "Cabinet Approves Mandatory SIM Card Registration," *Khaosod English*, accessed February 28, 2015, http://www.khaosodenglish.com/detail.php?newsid=1424412737.

98 Thai Lawyers for Human Rights, "Public Statement: Sarawut Bamrungkittikhun released from military custody," March 16, 2016, https://tlhr2014.wordpress.com/2016/03/16/public-statement-sarawut-bamrungkittikhun-released-from-military-custody/

99 iLaw, "Summary of freedom of speech 2014 part 1/5: individual summons and retention under martial law," *iLaw*, January 6, 2015, http://freedom.ilaw.or.th/blog/Arrest2014.

100 iLaw, "Review of the situations in 2015: Justice Made to Order, Freedom Still Out of Stock," December 23, 2015, http://freedom.ilaw.or.th/en/2015%20report.

101 https://www.amnesty.org/en/documents/asa33/3866/2016/en/; http://www.prachatai.com/english/node/6064

Alleged violations of national security or *lese majeste* laws prompted persecution from fellow internet users as well as the state. Ultra-royalist groups increasingly organize online to track down people they deem to have insulted the monarchy, often filing criminal cha ges against them. "Rubbish Collection Organization," a group of ultra-royalists led by Maj. Gen. Rientong Nan-nah, wages witch-hunt campaigns on Facebook; its targets are often ostracized socially and lose their jobs. The organization asks Thais based abroad to help track down "fugitives," and post their addresses online to facilitate further harassment, and has threatened to sue Facebook for allowing *lese majeste* content.[102]

Technical Attacks

There have been sporadic reports of hacking attacks on online news outlets in Thailand in the past. None were documented during the coverage period of this report, though hackers did target government sites. In October 2015, the international hacking collective Anonymous hacked websites of several Thai government agencies, including the Royal Thai Police and CAT Telecom, to express their opposition to the junta's single gateway plan.[103]

102 "Ultra-royalist steps up lèse majesté campaign against Facebook and YouTube," *Prachatai,* October 13, 2015, http://www.prachatai.org/english/node/5539.

103 "Anonymous claims hack of police servers, releases case data," *Bangkok Post,* April 12, 2015, http://www.bangkokpost.com/print/785129/; "International hackers attack CAT Telecom," *Bangkok Post,* October 23, 2015, http://www.bangkokpost.com/learning/learning-news/741072/international-hackers-attack-cat-telecom.

Freedom House

Tunisia

	2015	2016
Internet Freedom Status	Partly Free	Partly Free
Obstacles to Access (0-25)	10	10
Limits on Content (0-35)	8	8
Violations of User Rights (0-40)	20	20
TOTAL* (0-100)	**38**	**38**

* 0=most free, 100=least free

Population:	**11.1 million**
Internet Penetration 2015 (ITU):	**49 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Partly Free**

Key Developments: June 2015 – May 2016

- A new mobile provider launched operations inside the country in late 2015. Lycamobile, a mobile virtual network operator, will be operating on the infrastructure of Tunisie Télécom (see **ICT Market**).
- A new counterterrorism law passed in August 2015 outlined a maximum of fi e years in prison for those found to have "publicly and clearly praised" a terrorist crime, its perpetrator, and groups connected with terrorism (see **Legal Environment**).
- The new counterterrorism law requires security and intelligence services to obtain judicial approval prior to engaging in surveillance and communication interception in terrorism-related cases (see **Surveillance, Privacy, and Anonymity**).
- A number of journalists and ordinary users were arrested on terrorism charges for nonviolent speech posted online. Noureddine Mbarki, editor of the news site *Ekher Khabar Online*, was arrested for publishing a photograph showing a terrorist attack in Sousse, while mathematics teacher Abdelfatteh Said spent seven months in prison for alleging on Facebook that the attack was a conspiracy carried out by security forces (see **Prosecutions and Detentions for Online Activities**).
- News site *Inkyfada* was forced offline by a cyberattack that came a few days a ter it reported on the "Panama Papers" leaks detailing international tax havens (see **Technical Attacks**).

Introduction

Internet freedom in Tunisia in 2015-16 was marked by the passage of a new counterterrorism law that had mixed repercussions for free speech and privacy online.

The law contains some positive provisions, such as providing journalists with immunity from prosecution for refusing to reveal sources when reporting on terrorism. Although the press code contains similar protections against imprisonment, journalists have been targeted under the penal code in the past. Journalist Noureddine Mbarki was charged with "complicity in terrorism" for refusing to reveal to the authorities the source of a photo he obtained depicting a terrorism suspect leaving a car right before killing tourists in a beach resort on June 26.

As the government continues to grapple with increased terrorist attacks, authorities have resisted calls to reinstitute blocking and fil ering. Instead, officials ha e declared their intention to work together with social media companies to combat violent extremism. Digital rights activists have expressed fears over surveillance now that the Technical Telecommunications Agency (ATT) is up and running, lacking a clear mandate and oversight mechanisms. However, certain provisions within the antiterrorism law provide an important check on authorities when conducting surveillance during the course of terrorism cases.

The online landscape changed dramatically with the ouster of autocratic president Zine El Abidine Ben Ali on January 14, 2011. His repressive censorship apparatus largely dissipated and internet users have started to enjoy an unprecedented level of open access. Despite these slow reforms to Tunisia's legal environment, internet freedom remains threatened by a number of laws dating from the Ben Ali era, including the Telecommunications Code and the Internet Regulations. The judiciary continues to restrict free speech through the prosecution of users over content posted online, mainly regarding defamation, religion, and insults to state bodies. A high school student was charged with defamation over Facebook posts critical of the police. Several other Tunisians were detained or suffered legal harassment on vague charges.

Obstacles to Access

Growth in mobile internet subscriptions has underpinned an increase in internet penetration in Tunisia over the past year. A new operator, Lycamobile Tunisia, entered the market in late 2015 offering low-cost calls and data plans. However, the telecommunications market remains dominated by three major players, with state-controlled Tunisie Télécom continuing its monopolistic control over the internet backbone.

Availability and Ease of Access

According to the International Telecommunication Union (ITU), internet penetration stood at 48.5 percent at the end of 2015, up from 36.8 percent fi e years earlier.[1] As of March 2016, there were more than 7 million mobile data plans, compared to some 517,440 fi ed broadband subscriptions. Of these data plans, more than 1 million are purchased for use on 3G-equipped mobile phone

1 "Percentage of individuals using the Internet, fi ed (wired) Internet subscriptions, fi ed (wired)-broadband subscriptions," International Telecommunication Union (ITU), 2009 & 2014, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

devices, while 1.1 million are for internet connections through 3G USB keys.[2] USB keys used for 3G internet cost at least TND 40 (approximately US$20.5), while the service costs TND 25 (US$13) per month for 10GB of data.

The number of computers per 100 inhabitants rose from approximately 12 in 2009 to 22 as of 2015,[3] while the number of internet subscriptions (fi ed and 3G USB keys) is estimated to have exceeded 1.7 million over the same year.[4] The popularity of mobile phones is also on the rise, with over 14.7 million mobile phone subscriptions and a penetration rate of 130.7 percent as of March 2016.[5]

A number of Tunisians access the internet at privately owned cybercafes known as "publinets," where one hour of connection costs at least 1 TND (US$0.51). Before 2011, wireless access in cafes and restaurants was not permitted by law, which allowed only licensed ISPs to offer access. Nonetheless, since the revolution it has become common for cafes and restaurants in major cities to offer free internet access without any registration requirements, attracting mainly young social network users. The ICT ministry issued new regulations on the provision of internet access by cybercafes on July 29, 2013.[6] These regulations do not require users to register or to hand over identification documents, nor do they require owners to monitor their customers' activities. The ICTs ministry has registered a slight decrease in the number of cybercafes across the country, due mainly to a growth in the number of users accessing the internet through 3G data plans.[7] As of March 2016 there were 261 cybercafes, compared to 271 one year earlier.

Fixed-line internet subscribers must fi st buy a landline package from Tunisie Télécom (TT), which manages the country's 180 Gbps bandwidth capacity, before choosing one of 11 ISPs. The TT landline package costs 45 TND (US$23) for a three-month subscription period. ISP prices range from TND 10 (US$5) a month for a connection speed of 1 Mbps to TND 50 (US$25) for a connection speed of 20 Mbps. Although there are no legal limits on the data capacity that ISPs can supply, the bandwidth remains very low and connectivity is highly dependent on physical proximity to the existing infrastructure.

Restrictions on Connectivity

The Tunisian government does not impose any restrictions on ICT connectivity. However, Tunisie Télécom remains the sole manager of the country's 10,000KM fibe -optic internet backbone. Tunisie Télécom also acts as a reseller to domestic ISPs, granting it an oversized role in the country's internet governance. However, some positive signs have emerged of late. In September 2014, private

2 Instance National des Télécommunications, "Suivi des principaux indicateurs du marché de l'Internet en Tunisie" [Monitoring of main indicators regarding the Internet market in Tunisia], March 2016, accessed February 23, 2016, http://www.intt.tn/upload/files/TB3_Data%20-%20Ma s%202016.pdf.

3 Ministère des Technologies de la Communication," وزارة تكنولوجيا الإتصال و الإقتصاد الرقمي: مؤشرات و معطيات إحصائية معطيات شهر سبتمبر,"[Ministry of Communication Technologies and Digital Economy: statistical indicators and data: access and infrastructure], March 2015 , accessed on June 24, 2015: http://www.mincom.tn/index.php?id=315&L=1 .

4 Ministère des Technologies de la Communication," وزارة تكنولوجيا الإتصال و الإقتصاد الرقمي: مؤشرات و معطيات إحصائية معطيات شهر سبتمبر,"[Ministry of Communication Technologies and Digital Economy: statistical indicators and data], March 2015, accessed on June 24, 2015, http://www.mincom.tn/index.php?id=305&L=1.

5 Instance National des Télécommunications (INT), "Suivi des principaux indicateurs du marché de la téléphonie mobile en Tunisie" [Monitoring of main indicators regarding the mobile phone market in Tunisia], March 2016, accessed May 30, 2016, http://www.intt.tn/upload/files/TB2_Mobile%20-%20Ma s%202016.pdf.

6 Decision of July 29, 2013 on the conditions for the exploitation of public internet centers: http://bit.ly/1PkBfqq.

7 Instance National des Télécommunications, "Suivi des principaux indicateurs du marché de l'Internet en Tunisie" [Monitoring of main indicators regarding the Internet market in Tunisia], March 2016, accessed February 23, 2016, http://www.intt.tn/upload/files/TB3_Data%20-%20Ma s%202016.pdf.

operators Ooredoo Tunisie and Orange Tunisie inaugurated their own international submarine cable, thus easing the monopoly of Tunisie Télécom on Tunisia's international submarine communications cables.[8] The 175km long cable which links Tunisia to Italy is the fi st privately owned cable to enter into service in Tunisia. 4G is expected to be officially launched this summe , and the three main operators are required to cover at least 20 percent of the territory in one year,[9] including two marginalized interior regions.[10]

ICT Market

The main providers of internet service are Tunisie Télécom, Ooredoo Tunisie, and Orange Tunisie. The state controls a 65 percent stake in Tunisie Télécom, while the remainder is owned by Emirates International Telecommunications (EIT). In June 2013, EIT announced a plan to sell its shares in Tunisie Télécom, citing employees' strikes over higher salaries as a reason for the move—however no action has yet been taken.[11] Ooredoo Tunisie is a subsidiary of the multinational company Ooredoo, which is partially owned by the state of Qatar. Finally, Orange Tunisie has been controlled by the state since 2011, when a 51 percent stake was seized from Marwan Ben Mabrouk, son-in-law of fallen dictator Ben Ali. The remaining 49 percent stake is owned by the multinational group Orange.

A new operator, Lycamobile Tunisia, entered the ICT market in late 2015. Lycamobile is an international mobile virtual network operator (MVNO) which provides low cost rates for domestic and international calls and data services.[12] The operator was allocated a fi e-year renewable license and will be exploiting the infrastructure of Tunisie Télécom. According to media reports, three other companies applied for licenses to operate mobile virtual networks.[13]

Regulatory Bodies

The Ministry of Communication Technologies and Digital Economy (ICT ministry) is the main government body responsible for the ICT sector. The National Instance of Telecommunication (INT) is the regulator for all telecom and internet-related activities and has the responsibility of resolving technical issues and disputes between actors.

The INT's governance body is made up of mainly government officials nomina ed by the ICT Minister, which activists argue leads to a lack of regulatory independence. Nevertheless, the INT has initiated some positive changes in internet policy, namely through the introduction of a more liberal domain name chart and an invitation to independent arbitrators from civil society to help develop a new Alternative Domain Name Dispute Resolution Process.

Internet policy is decided by the INT and executed by the Tunisian Internet Agency (ATI), a state

8 "Didon cable linking Italy and Tunisia enters service," *Telecom Paper*, September 22, 2014, http://bit.ly/1L9DFV2.

9 "Tunisie: Le gouvernement tunisien espére le lancement de la 4G cet été". *Huffpost Tunisie.* March 1, 2016. http://www.huffpostmaghreb.com/2016/03/02/tunisie-4g_n_9367760.html.

10 " Drugeon, Antony. "La 4G arrive en Tunisie: à quels changements s'attendre?" *Huffpost Tunisie.* March 10, 2016. http://www.huffpostmaghreb.com/2016/03/10/4g-tunisie-changements_n_9425008.html.

11 Roger Field, "Emirates International Telecommunications Sells Its 35% Stake in Tunisie Telecom," *Arabian Industry,* June 23, 2013, http://bit.ly/1IOKHgk.

12 Lycamobile to Launch in Tunisia as its Global Network Reaches 20 Countries. *PR Newswire.* October 1, 2015. http://www.prnewswire.com/news-releases/lycamobile-to-launch-in-tunisia-as-its-global-network-reaches-20-countries-530220811.html.

13 "L'opérateur "Lycamobile" s'installe bientôt en Tunisie "[Operator Lycamobile soon in Tunisia]. *Tekiano.com*. October 1 2015. http://www.tekiano.com/2015/10/01/loperateur-lycamobile-sinstalle-bientot-en-tunisie/.

body governed by a board of trustees comprised of representatives from the main shareholder, Tunisie Télécom. The company controls 37 percent of ATI shares and the state owns a further 18 percent, while the remaining 45 percent is divided among private banks. The head of the ATI is appointed by the ICT ministry. The INT and ATI manage the ".tn" country domain. Under Ben Ali, the ATI was a government organ for surveillance and censorship. The ATI now manages the internet exchange point (IXP) between national ISPs that buy connectivity from Tunisie Télécom, as well as the allocation of internet protocol (IP) addresses.

Passed in December 2014, government decree n°2014-4773 regulates the granting of business licenses to ISPs.[14] Under the new decree, ISPs are subject to prior authorization from the ICT ministry, after consulting with the ministry of interior and the INT. Article 8 established a new advisory board tasked with examining licensing requests and advising on matters related to infractions and sanctions. The board is presided over by the ICT minister or his representative and is composed of representatives from the ministries of defense, interior, ICT, and commerce; the INT; and the Union for Industry and Commerce (UTICA). Businesses wishing to apply for a license need to have a standing capital of at least TND 1 million (approximately US$520,000). Licensing applications must be answered by the ministry within one month.

Limits on Content

Tunisian users continue to enjoy an open internet. However, in the absence of legal reforms, laws regarding censorship and intermediary liability from the Ben Ali era continue to pose a threat to free expression online. As the authorities continue to grapple with mounting terrorist attacks, more attention has turned to the fight against online extremism.

Blocking and Filtering

Censorship remains sparse in Tunisia, with no instances of politically motivated blocking over the past year. Popular social media tools such as Facebook, YouTube, Twitter, and international blog-hosting services are freely available.

Despite calls by several politicians and media commentators to censor web pages affilia ed with terrorism, there were no indications the authorities took concrete action. In June 2015, Telecommunications Minister Noomane Fehri has stated he "will not adopt a policy of blocking websites whatever their danger to us because we believe this solution is technologically useless."[15] As of mid-2016, there was no evidence that authorities were fil ering terrorist related content, but legal actions against users posting such content are very common.

Content Removal

While authorities admit fil ering "won't solve the problem" of users accessing extremist content, the telecommunications ministry has revealed it is coordinating with social media companies to suspend

14 Presidency of the Government, أمر عدد 4773 لسنة 2014 مؤرخ في 26 ديسمبر 2014 يتعلق بضبط شروط وإجراءات إسناد تراخيص نشاط مزود خدمات الأنترنات. [Decree n°4773 of 26 December 2014 fixing the conditions and p ocedures for allocating authorizations for ISP activities], December 26, 2014, http://bit.ly/1UrOYlW.

15 "Tunisia will not censor internet," *Middle East Monitor*, June 2, 2015, http://bit.ly/1K7i0jJ.

pages that incite violence or extremism.[16] It seems, however, that this coordination is mostly limited to requesting user data rather than removing content. According to Facebook's Transparency report, Tunisia made one request for user data affecting 48 accounts and not a single request for content takedown over the first half of 2015.[17] Google noted it received one request in the second half of 2015 and took action to remove the post, which was classified as defamatory.[18] No removal requests were sent to Twitter.

Under laws inherited from the dictatorship era, ISPs are liable for third-party content. According to Article 9 of the 1997 Internet Regulations, ISPs are required to continuously monitor content to prevent the dissemination of information "contrary to public order and good morals." There is no evidence that laws such as these have been used to take down political or social content from June 2015 to date.

Media, Diversity, and Content Manipulation

Tunisia's online media landscape is vibrant and open. Since the revolution, numerous online sources of information have been launched alongside new newspapers, radio stations, and television channels, enriching the information landscape through the addition of viewpoints from a diverse range of social actors. Nonetheless, Tunisia's post-revolutionary vibrancy has not eliminated all self-censorship. Some users might still avoid crossing certain red lines on topics such as religion, the military, and security institutions over fears of legal prosecution. Still, users are more open to discussing these sensitive issues on the web compared to traditional media platforms.

Digital Activism

Tunisian youth and civil society organizations have continued to use digital media for initiatives relating to political and social issues. In July 2015, users launched a campaign demanding better internet speeds and lower prices, prompting the regulator to release a statement urging operators to improve their quality of service and listen to their subscribers.[19]

Since the revolution, pro-LGBT rights groups have been taking advantage of the opening up of the internet to raise awareness and to campaign for the decriminalization of homosexuality.[20] In September 2015, following the sentencing of a young man to prison for homosexuality, LGBTI groups stepped up campaigning both online and offline against article 230 of the penal code, which punishes homosexuality with three years in jail.[21]

16 "Tunis 24/7 Mokhtar Khalfaoui/ Noomane El Fehri," YouTube video, 1:31:35, published by Elhiwar Ettounsi, March 26, 2015, https://youtu.be/8iVo_m-wULE.

17 "Tunisia," *Government Requests Report*, Facebook, January 2015-June 2015: https://govtrequests.facebook.com/country/Tunisia/2015-H1/.

18 "Tunisia," *Transparency Report*, Google, accessed October 31, 2016, https://www.google.com/transparencyreport/removals/government/TN/?hl=en.

19 Tunisia: a new campaign for a better internet. Medium. July 18, 2015. https://medium.com/@yosrjouini/tunisia-a-new-campaign-for-a-better-internet-84fced38e038#.5scve3xzo.

20 "LGBT : Le coup de pouce du Net" [LGBT: a boost from the Internet], *Inkyfada*. May 17, 2015, https://inkyfada.com/2015/05/lgbt-le-coup-de-pouce-du-net-tunisie/.

21 "We Must Fight Homophobia in Tunisia," *The Huffington Post,* February 10, 2016, http://www.huffington post.com/magdalena-mughrabi/we-must-figh -homophobia-_b_8235478.html.

Violations of User Rights

While Tunisia has taken significant steps to promote internet access and reverse online censorship, the country's legal framework remains a significant threat to internet freedom. Despite the adoption of a new constitution hailed as "democratic,"[22] the absence of legal reforms continues to hold Tunisia back. Most problematically, the judiciary continues to employ laws from the Ben Ali-era to prosecute users over online expression. Criminal defamation remains one of the biggest obstacles to independent reporting, while several users have been charged with defamation.

Legal Environment

The 2014 constitution, the first to be passed since the 2011 revolution, enshrines the right to free expression and freedom of the press, and bans "prior censorship." Specific articles guarantee the right to privacy and personal data protection, as well as the right to access information and communication networks.[23] However, the text contains vague language tasking the state with "protecting sanctities" and banning "takfir" (apostasy accusations). Such language could act as a constitutional restriction on internet freedom, where religious issues are currently debated more openly than in the mainstream media or on the streets.

Despite improvements to the constitution, the repressive laws of the Ben Ali regime remain the greatest threat to internet freedom. Article 86 of the Telecommunications Code states that anyone found guilty of "using public communication networks to insult or disturb others" could spend up to two years in prison and may be liable to pay a fine. Articles 128 and 245 of the penal code also punish slander with two to five years' imprisonment. Article 121(3) calls for a maximum punishment of five years in jail for those convicted of publishing content "liable to cause harm to public order or public morals". In addition, Tunisia's code of military justice criminalizes any criticism of the military institution and its commanders.[24]

Decree 115/2011 on the Press, Printing and Publishing provides protections to journalists against imprisonment. However, Tunisia's press code does not provide bloggers and citizen journalists with the same protections afforded to traditional journalists. Article 7 defines a "professional journalist" as a person holding a BA degree who "seeks the collection and dissemination of news, views and ideas and transmits them to the public on a primary and regular basis," and "works in an institution or institutions of daily or periodical news agencies, or audiovisual media and electronic media under the condition that it is the main source of income." In addition, authorities continue to use the penal code and the antiterrorism law to prosecute journalists.[25]

In August 2015, the parliament adopted a new counterterrorism law to replace a 2003 law used by the Ben Ali regime to crack down on critics and opponents.[26] The law outlines a maximum of five

22 National Democratic Institute, "Tunisia finally passes democratic constitution," news release, January 27, 2014, http://bit.ly/1ilUSnj.

23 Constitution of The Tunisian Republic, trans. Jasmine Foundation, January 26, 2014, http://bit.ly/LErybu.

24 Maher Chaabane and Lilia Weslaty, "Tunisie : Yassine Ayari ne doit pas être jugé par le tribunal militaire selon Rahmouni," [According to Rahmouni, Yassine Ayari should not be prosecuted by the military court] *Webdo,* December 25, 2014, http://bit.ly/1JTUtTC.

25 Safa Ben Said," In Tunisia, press freedom erodes amid security fears," Committee to Protect Journalists, October 27, 2015, https://www.cpj.org/reports/2015/10/in-tunisia-press-freedom-erodes-amid-security-fear.php.

26 Counter-terrorism law of 7 August 2015: http://www.legislation.tn/sites/default/files/news/ta2015261.pd

years in prison for those found to have "publicly and clearly praised" a terrorist crime, its perpetrator, and groups connected with terrorism.[27] Chapter fi e outlines surveillance and communication interception practices in terrorism-related cases. To monitor and intercept suspected terrorists' communications, security and intelligence services need to obtain judicial approval in advance for a period of four months, renewable only once (also for four months). Article 64 punishes unauthorized surveillance by a year in jail and 1000 TND (US$ 450). Under the new law, the authorities cannot prosecute journalists for not revealing terror related information they obtain during the course of their professional work.

The ICT minister announced his intention to introduce a draft cybercrime law for parliamentary review in August 2015. After parts of the law were leaked in 2014, reports showed the bill included problematic provisions extending criminal defamation to digital media.[28]

Prosecutions and Detentions for Online Activities

Several users were arrested or prosecuted against international norms of free speech over the past year:

- On July 8, 2015, authorities charged Noureddine Mbarki, editor of the news site *Ekher Khabar Online*, with complicity in terrorism under the 2003 anti-terrorism law for publishing a photograph showing Sousse beach attack gunman Seifeddine Rezgui leaving a car before he started shooting tourists on June 26.[29] The photograph was removed by the site less than an hour after its publication on June 5, at the request of the police. A day later, Mbarki was summoned for investigation and was interrogated for four hours by office s who pressed him to reveal the source of the photo. After refusing to disclose the photo's source, Mbarki was released, and was later charged with complicity in terrorism.

- On July 16, 2015, mathematics teacher Abdelfatteh Said was arrested and charged with complicity in terrorism for alleging on Facebook that the Sousse attack was a conspiracy carried out by security forces.[30] He was further charged with "accusing, without proof, a public agent of violating the law" under Article 128 of the penal code for sharing and commenting on a photo-shopped picture of Prime Minister Habib Essid originally posted by another user. The photo showed Essid holding a shovel along with the caption "Don't tell me that they weren't ready for the Sousse attack…" Though the terror and defamation charges were later dropped, Said was still sentenced to one year in jail for "knowingly broadcasting false news", under Article 306 of the Tunisian Penal Code. On February 5, after spending seven months in prison he was released after a court of appeal dismissed his case.[31]

27 "Tunisia: Counter-terror law endangers rights," Human Rights Watch, July 31, 2015. https://www.hrw.org/news/2015/07/31/tunisia-counterterror-law-endangers-rights

28 Safa Ben Said," In Tunisia, press freedom erodes amid security fears," Committee to Protect Journalists, October 27, 2015, https://www.cpj.org/reports/2015/10/in-tunisia-press-freedom-erodes-amid-security-fear.php.

29 "Tunisia charges editor with complicity in terrorist attack". Committee to Protect Journalists. July 23, 2015, https://cpj.org/2015/07/tunisia-charges-editor-with-complicity-in-terroris.php.

30 "Human Rights Protections Weaken as Tunisia Fights Terror". *Global Voices.* August 17, 2015, https://globalvoices.org/2015/08/17/human-rights-protections-weaken-as-tunisia-fights- error/#.

31 "Tunisia: Abdelfattah Said released," Amnesty USA, February 19, 2016, https://www.amnesty.org/en/documents/mde30/3467/2016/en/.

- Police union activist Walid Zarrouk continued to face legal trouble over his Facebook publications. On October 21, he was sentenced to three months in jail after he was convicted of defaming the Tunis deputy public prosecutor.[32] He was released on 15 December.[33] Last year, a primary court sentenced Zarrouk in absentia to one year in jail for "insulting others through public communication networks" over a 2013 Facebook post.[34] In the post, he accused the then-general prosecutor of the Tunis Tribunal, Tarek Chkioua, and Minister of Justice Noureddine Bhiri of "politicizing prosecutions".[35]

- In December 2015, 17-year old high school student Afraa Ben Azaa was charged with insulting police office s in her Facebook posts under article 125 of the Penal Code. Ben Azza was arrested on December 16 while she was protesting against the planned destruction of a historic monument in El Kef, northwestern Tunisia.[36] She spent a day in police custody. On January 29, a children's judge dismissed her case.[37]

- On February 23, a court sentenced in absentia Slim Riahi, founder and leader of the Free Patriotic Union, a liberal political party currently serving in the coalition government, to six months in jail for defamation. Riahi was sentenced following a complaint filed by aher Ben Hassine, a politician and owner of an opposition TV station at the time of Ben Ali, over a 2014 Facebook post. In the post, Riahi accused Ben Hassine of being an informant to the Ben Ali regime.[38]

- Following its publication of the "Panama Papers" leaks surrounding the global offshore accounts, the online media outlet *Inkyfada* faced threats of legal prosecutions for writing about local politicians mentioned in the leaks. Politician Mohsen Marzouk, who is the former secretary general of the governing Nidaa Tounes party, threatened to sue *Inkyfada* for defamation after revealing that he sent emails to the Panamanian law fi m Mossack Fonseca inquiring how to launch an offshore business.[39] Marzouk later abandoned his plans to sue the site.[40] Rached Ghannouchi, leader of the Islamist Ennahda party, a member in the governing coalition, also threatened legal action against *Inkyfada* for mentioning him "without justification" in a eport about the company owning Tunisian News Network (TNN), a privately owned news channel with close ties to Ennahdha. In the report, *Inkyfada* did not imply Ghannouchi's name appears in the Panama Papers, but only mentioned his links

32 "NGO Founder Sentenced to Prison". ecoi.net. October 26, 2015. https://www.ecoi.net/file_upl ad/1226_1446100787_mde3027432015english.pdf.

33 "Walid Zarrouk sort de prison," [Walid Zarrouk released from prison] *Kapitalis*, December 15, 2015, http://www.businessnews.com.tn/walid-zarrouk-sort-de-prison,520,61028,3.

34 "Un an de prison pour Walid Zarrouk pour atteinte à un procureur de la république" [One year in prison against Walid Zarrouk for insulting state prosecutor] *Kapitalis* , May 7, 2015, http://bit.ly/1LPv7FH.

35 Human Rights Watch, "Tunisia: Spate of Prosecutions for Free Speech," September 13, 2013, http://bit.ly/1EFlucV.

36 "Tunisie: une adolescente de 17 ans risque la prison pour des statuts Facebook". [Tunisia: A 17 year old teen risks prison over Facebook posts]. *Le Monde.* December 31, 2015. http://www.lemonde.fr/afrique/article/2015/12/31/tunisie-une-adolescente-de-17-ans-risque-la-prison-pour-des-statuts-facebook_4840473_3212.html.

37 "Kef: Non lieu pour la jeune militante Afraa Ben Azza". [Kef Case against young activist Afraa Ben Azaa dismissed]. *Tuniscope.* January 29, 2016, http://www.tuniscope.com/article/87581/actualites/tunisie/afraa-nonlieu-201712.

38 "تونس: الحكم بالسجن غيابيا على رئيس حزب" ["Tunisia: a party leader sentenced to jail in absentia"], *Alaraby,* February 24, 2016, http://bit.ly/2eUfBOe.

39 Antony Drugeon, "Le journal électronique Inkyfada poursuivi pour diffamation par Mohsen Marzouk: Les enjeux de la plainte". *Huffpost Tunisie.* April 8, 2016, http://www.huffpostmaghreb.com/2016/04/07/inkyfada-diffamation-marzouk_n_9631980.html?ir=Maghreb&ncid=fcbklnkfrhpmg00000006.

40 Drugeon, Antony. "Mohsen Marzouk renonce à porter plainte contre Inkyfada". *Huffpost Tunisie.* April 28, 2016. http://www.huffpostmaghreb.com/2016/04/28/marzouk-plainte-inkyfada_n_9794160.html?utm_hp_ref=tunisie.

to TNN.[41] To this date, however, *Inkyfada* was not the subject of any legal investigations or prosecutions.

- On December 5, police arrested six young male students on "sodomy" charges.[42] The six were sentenced to three years in jail under article 230 of the Penal Code which bans homosexual acts. One of the students was sentenced to another six-month jail term under article 226 for "indecent behavior" over pornographic videos the police found on his computer. On January 7, a court ordered their release for "procedural irregularity" after police raided an apartment of one of the accused with a written warrant.[43]Nearly two months later, a court of appeal confi med the "sodomy" conviction but reduced the students' sentences to one month in jail each.[44]

Authorities have also arrested several individuals for advocating extremism. Early in June 2015, the interior ministry announced the arrest of three individuals running a Twitter account in support of Okba Ibn Nafaa Brigade, a terrorist group active on the border with Algeria.[45] A month later, eight users were arrested for inciting to terrorism on social media sites.[46] There were no reports that these arrests contravened international norms on free speech.

Spotlight on Marginalized Communities

Freedom on the Net 2016 asked researchers from India, Indonesia, Kenya, Kyrgyzstan, Jordan, Mexico, Nigeria, and Tunisia to examine threats marginalized groups face online in their countries. Based on their expertize, each researcher highlighted one community suffering discrimination, whether as a result of their religion, gender, sexuality, or disability, that prevents them using the internet freely.

In Tunisia, Karim Abdelkarim and Dhouha Ben Youssef examined online expression and religious freedom.[1] The study found:

- The internet is a critical space for religious minority communities, who rely on social media to help organize private gatherings that are safe from persecution. Tunisians report converting to Christianity as a result of participating in online forums, and practice their religion through religious broadcasts and online resources like the El Massih Fi Tunis ("Christians in Tunisia") website.
- Yet individuals who publish minority religious views online often face a severe backlash from other internet users who identify with the Muslim majority. The intensity of harassment and threats often causes minorities to engage in self-censorship.
- At least two atheists have received prison sentences in recent years for their online posts. The government's aggressive response to perceived threats to the majority Sunni Muslim tradition, including surveillance and arrests for online expression, compounds the problem of self-censorship among minority groups.

1 Ben Abdallah AbdelKarim and Dhouha Ben Youssef, "Building Religious Tolerance Online in Tunisia," research paper, September 2016, on file with Freedom House.

41 "Associé à son tour aux "Panama papers", R. Ghannouchi annonce porter plainte contre Inkyfada". *Huffpost Tunisie.* April 18, 2016, http://www.huffpostmaghreb.com/2016/04/18/panama-ghannouchi-inkyfada_n_9718048.html.

42 "Tunisia: 3-year sentence for homosexuality," Human Rights Watch, December 16, 2015, https://www.hrw.org/news/2015/12/16/tunisia-3-year-sentence-homosexuality.

43 Tunisie: "Condamnés et bannis de la ville de Kairouan pour homosexualité, les six jeunes sont en liberté (provisoire)," *Huffpost Maghreb*, January 7, 2016, http://huff.to/2eSnwuY

44 "Tunisie : peine réduite en appel pour les six jeunes condamnés pour homosexualité". [Tunisia: on appeal, sentence against six youth for homsexuality, reduced]. *Jeune Afrique,* March 4, 2016, http://www.jeuneafrique.com/307413/societe/tunisie-peine-reduite-en-appel-pour-les-six-jeunes-accuses-dhomosexualite/.

45 "تونس تقبض على مترو طيران باسم كتيبة عقبة بن نافع إلى الجهاد" [Tunisia arrests individuals involved in running the twitter account of Ifriqiya for Media], *Alaraby.* June 4, 2015, http://bit.ly/2fnoOmG.

46 تونس تعتقل ثمانية أشخاص استخدموا مواقع التواصل الاجتماعي لدعم الإرهاب" [Tunisia arrests eight individuals who used social media sites to support terrorism], *CNN.* July 20, 2015, http://arabic.cnn.com/world/2015/07/20/tunisia-social-network-terrorism.

Surveillance, Privacy, and Anonymity

Surveillance remains a strong concern in Tunisia due to the country's history of abuse under the Ben Ali regime. While there have not been any reports of extralegal government surveillance in the post-Ben Ali period, the deep-packet inspection (DPI) technology once employed to monitor the internet and intercept communications is still in place, sparking worries that the technology can be reactivated if desired.

The creation of a new government surveillance agency in November 2013 raised concerns among human rights and privacy groups, particularly given the lack of transparency surrounding its duties. The Technical Telecommunications Agency (ATT) was established by decree n°2013-4506 under the former administration of Ali Laarayedh. The decree tasks the ATT with "providing technical support to judicial investigations into information and communication crimes," but neither defines nor specifies these crime [47] Netizens immediately criticized the decision for its lack of parliamentary scrutiny, as well as a failure to provide the body with a clear and limited mandate, with independence from government interference, and with mechanisms to guarantee user rights.[48] According to Article 5 of the decree, the ATT's activities are not open to public scrutiny.

The ICT minister is charged with appointing the ATT's general director and department directors. An oversight committee was established "to ensure the proper functioning of the national systems for controlling telecommunications traffic in the frame ork of the protection of personal data and civil liberties." The committee mainly consists of government representatives appointed from the ministries of ICT, human rights and transitional justice, interior, national defense, and justice.

Despite this early criticism, the ATT started operating in "full capacity" in the summer of 2014[49] after the appointment of Jamel Zenkri, who previously served at the ATI and the INT, as general-director.[50] Responsibilities for conducting internet surveillance for the purposes of law enforcement have thus been transferred to the ATT from the ATI, which often assisted the judiciary in investigating cybercrime cases despite the absence of a law requiring it to do so.

Fears over the ATT have been boosted by the fact that Tunisia' legislators have been slow to initiate any legal reforms that would protect citizens from mass surveillance.[51] Draft amendments by Tunisia's Data Protection Authority (INPDP) to amend the country's 2004 privacy law have not been discussed by the constituent assembly or by the new parliament elected in October 2014.

Laws that limit encryption also remain a concern in the post-Ben Ali era. In particular, Articles 9 and 87 of the 2001 Telecommunication Code ban the use of encryption and provide a sanction of up to fi e years in prison for the unauthorized use of such techniques. While there have been no reports of

47 Reporters Without Borders, "Authorities urged to rescind decree creating communications surveillance agency," December 3, 2013, http://en.rsf.org/tunisia-authorities-urged-to-rescind-02-12-2013,45531.html.

48 Afef Abrougui, "Will Tunisia's ATT Ring in a New Era of Mass Surveillance," *Global Voices Advocacy,* November 26, 2013, http://bit.ly/1JTXPpw.

49 Khalil Abdelmoumen," Jamel Zenkri, DG de l'AT des Télécommunications : «Nos agents sont, dès le départ, soupçonnés d'être malhonnêtes»," [Jamel Zenkri director general of ATT: "Our agents are from the start suspected of dishonesty"] *Webdo*, June 4, 2014, http://bit.ly/1PkCENF.

50 Al Sarah Ben Hamadi, "Tunisie: Jamel Zenkri à la tete de l'Agence Technique des Télécommunications," [Tunisia: Jamel Zenkri to head the Technical Agency of Telecommunications] *Al Huffington Post,* March 3, 2014, http://huff.to/1EFND3Y.

51 Afef Abrougui, "Tunisia: New Big Brother, non-existent reforms," *Global Information Society Watch 2014: Communications surveillance in the digital age,* 248, http://bit.ly/1fZu4rn.

these laws being enforced, their continuing existence underscores the precarious nature of Tunisia's newfound and relatively open internet environment.

Police often seize users' electronic devices or access their online accounts in the course of investigations related to other crimes. For example, police office s pressed 40-year old entrepreneur Ahmed Redissi to provide access to his social media accounts during an investigation into his religious practices on December 7, 2015.[52]

Intimidation and Violence

In addition to legal prosecution, users must also be wary of extralegal attempts to silence them. On September 30, 2015 police assaulted two journalists of the collective blog Nawaat.org while they were covering a protest against a controversial "Reconciliation Law" that would provide some immunity to public officials cha ged with corruption for acts committed under the previous regime.[53] One of the journalists, Ali Mensali, was detained and released the same day after police made sure he deleted footage showing them beating protesters.[54]

Technical Attacks

Since Ben Ali's fall, there have been no reported incidents of cyberattacks perpetrated by the government to silence ICT users. However, other groups and individuals have employed these methods to intimidate activists and organizations with whom they disagree, particularly during major political events such as the 2014 parliamentary and presidential elections. After it published its fi st Panama Papers report mentioning politician Mohsen Marzouk, *Inkyfada* came under a cyberattack that forced the site to go offline for a few days. Hac ers sought to manipulate the site's content, and they managed to publish an article falsely alleging that former president Mohsen Marzouki received 36 million dollars from a Qatari foundation through an offshore company based in Panama.[55]

52 " Etat d'urgence: ni droits, ni lois," *Inkyfada*. December 10, 2015, https://inkyfada.com/2015/12/terrorisme-excuse-droit-liberte-atteinte-police-tunisie/.

53 Farah Samti, "In Tunisia, a New Reconciliation Law Stokes Protest and Conflict Ins ead," *Foreign Policy*, September 15, 2015, http://foreignpolicy.com/2015/09/15/in-tunisia-a-new-reconciliation-law-stokes-protest-and-conflic -instead/.

54 "The attack on journalists during the coverage of the student demonstration against the draft reconciliation bill," [Arabic] Nawaat.org, September 30, 2015, http://bit.ly/2dVrJSf.

55 "Tunisie. Le site Inkyfada piraté après des révélations sur les Panama Papers," *Courrier International,* April 6, 2016, http://www.courrierinternational.com/article/tunisie-le-site-inkyfada-pirate-apres-des-revelations-sur-les-panama-papers.

Freedom House

Turkey

	2015	2016
Internet Freedom Status	Partly Free	Not Free
Obstacles to Access (0-25)	13	13
Limits on Content (0-35)	20	21
Violations of User Rights (0-40)	25	27
TOTAL* (0-100)	**58**	**61**

* 0=most free, 100=least free

Population:	**78.7 million**
Internet Penetration 2015 (ITU):	**54 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- Mobile and internet connections were repeatedly suspended in Yuksekova, Cizre, Sur, Silopi, and other cities in the southeast of the country during raids by security agencies against militants (See **Restrictions on Connectivity**).
- Twitter, Facebook, and YouTube were temporarily blocked on numerous occasions—typically in the aftermath of terrorist attacks—until they restricted access to specific posts or accounts (see **Blocking and Filtering**).
- Turkey accounted for almost 90 percent of all content that was locally restricted by Twitter in the second half of 2015. Turkey's regulator fined the company TRY 150,000 (US$ 51,000) for refusing to remove what it termed "terrorist propaganda" from the site (see **Content Removal**).
- Progovernment trolls have escalated their campaigns to harass opposition voices and organizations on social media through smear campaigns and fake accounts (see **Media, Diversity, and Content Manipulation**).
- Journalists such as Hayri Tunç, Aytekin Gezici, and Bülent Keneş received lengthy prison sentences for "insulting" public officials or spreading "terrorism propaganda" (see **Prosecutions and Detentions for Online Activities**).
- A 14-day cyberattack brought almost 400,000 Turkish websites offline and temporarily suspended retail banking services in the country (see **Technical Attacks**).

Editor's Note:

This report covers events between June 1, 2015 and May 31, 2016. On July 15, 2016, a rogue faction of the Turkish military attempted to overthrow the government. Internet connections were throttled and major social media platforms were blocked. In a bid to reassert control over the country, President Erdoğan ordered the telecommunications regulator to restore internet access and subsequently made a FaceTime video call to a news anchor, who held up her cell phone in front of the camera to allow the president to address the nation.[1] President Erdoğan rallied citizens to take to the streets in a show of support for the government. Government order was eventually restored, but not before some 300 people reportedly died in clashes between pro- and anti-coup forces.[2] Government officials publically blamed exiled Islamic preacher Fethullah Gülen for instigating the coup. Since then a state of emergency has been in place, thousands have been arrested, and hundreds of thousands have faced some form of retribution for alleged connections to Gülen, such as job loss, travel bans, or harassment. In August 2016, one of Turkey's government agencies, the Telecommunication and Communication Presidency (TİB), was closed by decree and all responsibilities were transferred to the ICT Authority. The TİB—described by President Erdoğan as "among the places that has all the dirt"—was closed over suspicions it was used by Gülenists as a "headquarters for illegal wiretapping."[3] These dynamics will be further explored in the 2016-17 edition of Freedom on the Net.

Introduction

Internet freedom declined in Turkey in 2015-16 amid network shutdowns, social media blocking, lengthy prison sentences, and nationwide cyberattacks.

General elections in June and November of 2015 heightened tensions in the country, which were further exacerbated by a series of deadly terrorist attacks. Authorities hastily introduced gag orders on the dissemination of images and videos of the bombings, resulting in the blocking of hundreds of URLs. Access to Facebook, Twitter, and YouTube was repeatedly throttled until the companies removed controversial content. Specific hashtags elated to the bomb sites, like #Istanbul, #Ankara, and #Diyarbakir, were temporarily fil ered from Instagram. Counterterrorism operations in the southeastern region of the country repeatedly resulted in the suspension of 3G networks, affecting millions of residents for days at a time.

Over 100,000 websites were reportedly blocked in the country as of 2016, including a wide variety of political, social, and religious content. Dozens of news agencies and social media accounts covering Kurdish issues have been either blocked or shut down for allegedly promoting terrorist propaganda over the past year. Journalists and even university students have been convicted on spurious terrorism-related charges and sentenced to multiyear prison terms. But the most common charge over the coverage period remained "insulting" public officials, articularly President Recep Tayyip Erdoğan, who has reportedly filed criminal defamation complaints against mo e than 2,000 people since

1 Reuters, "Erdogan addresses Turkey via FaceTime amid attempted coup – video," *The Guardian*, July 15, 2016, https://www.theguardian.com/world/video/2016/jul/15/erdogan-facetime-turkey-coup-attempt.

2 Patrick Kingsley, "Turkey coup: Erdoğan mourns casualties – and vows retribution," *The Guardian*, July 18, 2016, https://www.theguardian.com/world/2016/jul/17/recep-tayyip-erdogan-mourns-coup-casualties-and-vows-retribution.

3 "Turkey shuts down telecommunication body amid post-coup attempt measures," *Hurriyet Daily News*, August 15, 2016, http://www.hurriyetdailynews.com/turkey-shuts-down-telecommunication-body-amid-post-coup-attempt-measures.aspx?pageID=238&nID=102936&NewsCatID=338.

elected to his current office in August 2014.[4] While most users typically receive suspended sentences,[5] several users have been given lengthy prison terms. The government frequently targets political opponents by applying the country's draconian defamation laws to nonviolent, often satirical Twitter posts.

Turkey continued to grapple with significant th eats to cybersecurity. While opposition news sites are frequently targeted by progovernment hackers, a nationwide DDoS attack brought thousands of Turkish websites offline and made it difficult for locals o use retail banking services in December 2015. Furthermore, the addresses, dates of birth, and national identity numbers belonging to around 50 million citizens were leaked in early April 2016 in one of the country's biggest ever data breaches. At the same time, Turkish users must contend with intrusive government surveillance and the proven use of sophisticated malware tools by law enforcement. In a country that reportedly listed social media as one of the main threats to national security,[6] internet freedom is on a very negative trajectory in Turkey.

Obstacles to Access

The most significant obstacle to internet access in Turkey remains the shutting down of telecommunications networks during security operations, mainly in the southeastern part of the country. Internet penetration continues to grow, particularly through mobile broadband, as three companies have begun to offer "4.5G" services.

Availability and Ease of Access

Internet penetration has continued to increase over the last few years. According to the International Telecommunication Union, internet penetration stood at 54 percent at the end of 2015, up from 40 percent in 2010.[7] Mobile broadband subscriptions outpaced those of fi ed broadband by 37.3 million to 9.2 million, according to Turkey's Information and Communications Authority (BTK), the regulator responsible for ICTs.[8]

According to the results of the Turkish Statistical Institute's Household Usage of Information Technologies Survey, the number of households with internet access has risen to 76 percent.[9] For individuals aged 16–74, computer usage stood at 95.9 percent, with internet usage at 93.7 percent.

Mobile phone penetration in Turkey reached 93.7 percent with 73.8 million mobile subscribers in the

4 Chrisopher de Bellaigue, "Welcome to demokrasi: how Erdogan got more popular than ever," *The Guardian*, August 30, 2016, https://www.theguardian.com/world/2016/aug/30/welcome-to-demokrasi-how-erdogan-got-more-popular-than-ever.

5 Generally speaking, an individual avoids prison in a suspended sentence, unless he or she reoffends during a probationary period outlined by the court.

6 The National Security Council allegedly listed social media as one of the main threats to Turkey's national security along with protests and civil disobedience; parallel state structures; communication security; cyber security; organizations exploiting religion, such as the Islamic State militant group; and ethnic-based terrorist groups, such as the Kurdistan Workers' Party (PKK). "National Security Council under Erdogan updates top secret national security 'book,'" *Hurriyet Daily News*, April 30, 2015, http://bit.ly/1UVBcCM.

7 International Telecommunication Union, "Statistics," 2015, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

8 Information and Communication Technologies Authority, "Electronic Communications Market in Turkey – Market Data (2015 Q3)," accessed February 20, 2015, slide 7, http://www.btk.gov.tr/File/?path=ROOT%2f1%2fDocuments%2fPages%2fMarket_Data%2f2015-Q3-En.pdf

9 Turkiye Istatistik Kurumu, "Household Usage of Information Technologies Survey of Turkish Statistical Institute, 2015," [in Turkish] August 18, 2015, accessed October 13, 2016, http://www.tuik.gov.tr/PreTablo.do?alt_id=1028.

fi st quarter of 2016. Although all operators offer third-generation (3G) data connections, only 65.9 million subscribers have access to 3G.[10] Prices remain high in comparison with the minimum wage. Turkey ranked 69th on the global ICT Development Index (IDI) for 2015, or 38th out of 40 European countries.[11]

Restrictions on Connectivity

Poor telecommunications infrastructure, a lack of electricity, and raids by the military or police continue to restrict connectivity in certain areas, especially in the eastern and southeastern regions of the country. For example, counterterrorism or law enforcement activities in the southeastern cities of Yuksekova, Cizre, Silopi, and Sur led to shutdowns of 3G mobile networks and electricity outages.[12] In one case, the outage lasted 60 hours.[13]

Turkey's internet backbone is run by TTNET, a subsidiary of Türk Telekom that is also the largest internet service provider (ISP) in the country. Türk Telekom, which is partly state owned, has 214,395 km of fibe -optic infrastructure, while other operators have a combined total of just 58,155 km. Nearly 124,374 km of this infrastructure is used as backbone, with the remainder dedicated to access distribution.[14]

There are three IXPs owned by private companies, both of which are in Istanbul: IST-IX, established by Terramark in 2009, and TNAP, established by seven leading ISPs in 2013. DEC-IX, a German internet exchange company, has started its operation in Istanbul as "a neutral interconnection and peering point for internet service providers from Turkey, Iran, the Caucasus region and the Middle East."[15]

ICT Market

There are 582 operators providing ICT services in the Turkish market, and a total of 930 were authorized as of late May 27, 2016 according to the BTK.[16] There are around 359 ISPs, though the majority act as resellers for Türk Telekom. TTNET, founded in 2006 by Türk Telekom, dominates the ISP market with 71.2 percent of market share.[17]

Turkcell is the leading mobile phone provider, with 44.2 percent of market share, followed by Voda-

10 Information and Communication Technologies Authority, "Electronic Communications Market in Turkey – Market Data (2016 Q1)," accessed October 10, 2016, slide 3, http://www.btk.gov.tr/File/?path=ROOT%2f1%2fDocuments%2fPages%2fMarket_Data%2f2016-Q1-En.pdf.

11 International Telecommunication Union, *Measuring the Information Society Report*, 2015, http://www.itu.int/net4/ITU-D/idi/2015/.

12 Efe Kerem Sozeri, "Social media throttling in Turkey points to wartime censorship efforts," The Daily Dot, August 27, 2016, http://www.dailydot.com/layer8/turkey-wartime-censorship-syria/.

13 "60 hour internet in the Eastern Province," [translated] Haberler.com, July 26, 2015, http://web.archive.org/web/20150728014051/http://www.haberler.com/dogu-illerinde-60-saattir-internet-sikintisi-7542461-haberi/.

14 Information and Communication Technologies Authority, "Electronic Communications Market in Turkey – Market Data (2016 Q1)," accessed October 10, 2016, slide 13, http://www.btk.gov.tr/File/?path=ROOT%2f1%2fDocuments%2fPages%2fMarket_Data%2f2016-Q1-En.pdf.

15 "DEC-IX Istanbul," accessed February 20, 2015, https://www.de-cix.net/products-services/de-cix-istanbul/.

16 Information and Communication Technologies Authority, "Electronic Communications Market in Turkey – Market Data (2016 Q1)," accessed October 10, 2016, slide 4, Market Data (2016 Q1)," accessed October 10, 2016, slide 3, http://www.btk.gov.tr/File/?path=ROOT%2f1%2fDocuments%2fPages%2fMarket_Data%2f2016-Q1-En.pdf.

17 Information and Communication Technologies Authority, "Electronic Communications Market in Turkey – Market Data (2016 Q1)," accessed October 10, 2016, slide 34, http://www.btk.gov.tr/File/?path=ROOT%2f1%2fDocuments%2fPages%2fMarket_Data%2f2016-Q1-En.pdf.

fone and Avea (which currently operates under the brand Türk Telekom).[18] Although the BTK originally set a deadline of May 26 for the auction of a 4G spectrum, in April 2015 it was announced that the tender could be canceled due to President Erdoğan's insistence that Turkey jump directly from 3G to 5G.[19] An auction of 4G frequency bands was held that August, but the BTK dubbed it "4.5G" in what some said was an effort to placate President Erdoğan.[20] All three companies started offering "4.5G" technology for mobile subscribers on April 1, 2016.

Though all legal entities are allowed to operate an ISP, there are some requirements to apply for authorization, pertaining to issues like the company's legal status, its scope of activity, and its shareholders' qualifications. Fu thermore, implicit obstacles may prevent newly founded companies without political ties or economic clout from entering the market. ISPs are required by law to submit an application for an "activity certifica e" to the BTK before they can offer services. Internet cafes are also subject to regulation. Those operating without an activity certifica e from a local municipality may face fines f TRY 3,000 to 15,000 (US$1,335 to US$6,680). Mobile phone service providers are subject to licensing through the BTK.

Regulatory Bodies

Policymaking, regulation, and operation functions are separated by the basic laws of the telecommunications sector. The Ministry of Transportation, Maritime Affairs, and Communications is responsible for policymaking, while the BTK is in charge of regulation.[21]

The BTK and the Telecommunication and Communication Presidency (TİB), which it oversees, are well staffed and have a dedicated budget. However, the fact that board members are government appointees is a potential threat to the BTK's independence, and its decision-making process is not transparent. Nonetheless, there have been no reported instances of certifica es or licenses being denied. The TİB also oversees the application of the country's website blocking law and is often criticized by advocacy groups for a lack of transparency and its apparent lack of independence from the executive.

The Computer Center of Middle East Technical University has been responsible for managing domain names since 1991. The BTK oversees and establishes the domain-name operation policy and its bylaws. Unlike in many other countries, individuals in Turkey are not permitted to register and own domain names ending with the country extension .tr, such as .com.tr and .org.tr, unless they own a trademark, company, or civil society organization with the same name as the requested domain.

Limits on Content

Limits on content continued to increase in Turkey over the past year. Prompted by a series of deadly terrorist attacks, the government repeatedly blocked or throttled social media platforms in a bid to halt the dissemination of images and videos surrounding the events. In addition, scores of news sites

18 "Electronic Communications Market in Turkey – Market Data (2016 Q2)," page xiii.

19 Ece Toksabay, "Turkey minister says might cancel 4G tender, switch to 5G: newspaper," Reuters, April 28, 2015, http://reut.rs/1GBtvwO.

20 Tulay Karadeniz, "Turkey's 4G tender outstrips predictions with bids for 4.5 billion," Reuters, August 26, 2015, http://www.reuters.com/article/2015/08/26/us-turkey-telecoms-idUSKCN0QV1XI20150826.

21 Information and Communication Technologies Authority, "Establishment," accessed October 11, 2015, http://bit.ly/1QsTRoE.

and Twitter accounts were blocked or removed, particularly those covering the conflict with Kurdish militants. Journalists, scholars, and public figures that are critical of the government faced coordinated harassment by progovernment trolls on Twitter.

Blocking and Filtering

Blocking continues to increase steadily in Turkey. According to the reports of the independent organization Engelli Web, as of May 2016 over 111,000 websites were banned based on civil code–related complaints and intellectual-property rights violations. The number of blocked websites has risen from 43,785 to 111,011 in three years.[22] This figu e includes numerous sites that were blocked for political or social reasons, such as news outlets or online communities that report on LGBTI (lesbian, gay, bisexual, transgender, and intersex) issues, ethnic minorities, specifically p o-Kurdish content, anti-Muslim content, or social unrest.

Authorities specifically ta geted the online accounts of journalists and activists this year. A number of platforms were blocked during the coverage period, frequently for refusing to restrict Turkish users' access to specific ages or posts. The TİB and Turkish courts blocked access to thousands of URLs including but not limited to pro-Kurdish websites such as Rudaw, BasNews, DİHA, ANHA, Özgür Gündem newspaper, Yüksekova Haber, Sendika.org, RojNews, ANF, BestaNuçe, as well as data journalism website Dag Medya,[23] alternative news source Jiyan, Marxist website marksist.org, and most of the outlets' Twitter accounts.[24] The Supreme Electoral Council of Turkey (YSK) blocked access to more than 90 URLs for sharing polls before the elections. After a request by Yaman Akdeniz and Kerem Altiparmak, two law professors, the YSK lifted the ban.[25] The TİB blocked access to fi e of the most commonly used LGBTI websites, namely GayLey, Travestice, Tracesti Sitesi, Turk Gay Bar, and Istanbul Gay.[26]

Furthermore, Turkey has censored atheist and anti-Muslim websites deemed defamatory, according to a court order dated February 27, 2015.[27] The Ankara Golbasi Criminal Court of Peace issued an order to ban 49 URLs, including atheist and anti-Muslim websites; the French satirical magazine *Charlie Hebdo* and its corresponding Wikipedia entry; and Turkish and foreign news articles about a controversial *Charlie Hebdo* cover that caricatured the Muslim prophet Muhammad.[28] Akdeniz and Altiparmak also filed an objection against that decision, but the ebsites remain blocked.

In most of cases, owners of the banned websites were not informed of the order or were not given sufficient time o comply. For example, on August 9, 2015, TİB banned access to Dag Medya, a data journalism website which also operates as a hub organizing events for journalists. Dag Medya re-

22 Engelli Web, "Kurum Bazinda Istatistikler."

23 Efe Kerem Sozeri, "Government bans data journalism website without court order," *Jiyan*, August 15, 2015, http://jiyan.org/2015/08/09/governmetn-bans-data-journalism-website-without-court-order/.

24 Efe Kerem Sozeri, "Turkey declares war on ISIS, censors Kurdish news instead", 2 August, 2015, https://medium.com/@efekerem/turkey-declares-war-on-isis-censors-kurdish-news-instead-3f30a9e5264f#.b5hmjmor2.

25 "Seçim geçti, YSK yasağı kalkmadı: 90 internet sayfası hala engelli," Sendika.org, July 15, 2016, http://sendika10.org/2015/07/secim-gecti-ysk-yasagi-kalkmadi-90-internet-sayfasi-hala-engelli/.

26 Yildiz Tar, "Access to LGBTI related websites was blocked one by one?", KaosGL, June 4, 2015, http://kaosgl.org/page.php?id=19562

27 Golbasi Criminal Court of Peace Decision No 2015/191 D.Is, dated February 27 2015.

28 Efe Kerem Sözeri, "Turkey quietly escalating online censorship of atheism," *The Daily Dot*, March 4, 2015, http://bit.ly/1M9kZpa.

ported that TİB did not send a notice about illegal content in the website, nor did it provide justific - tion or a court order.[29]

Facebook, Twitter, and YouTube were briefly bloc ed or throttled until they complied with court orders to remove "criminal" content, including images and videos related to deadly bombings in Suruç, Ankara, and Istanbul. In all of the following cases, restrictions on social media platforms occurred within 1-2 hours of each incident, indicating authorities may have sent more informal orders to ISPs prior to the official o ders cited below:[30]

- On July 20, 2015, a suicide bombing killed 32 people, mainly student activists, in the southeastern border town of Suruc.[31] Two days after the bombing, a court banned access to a total of 173 URLs, including Facebook, YouTube, Twitter, and 38 news websites as part of a ban on images and footage of the incident.[32] A backlash started immediately using the hashtag #TwitterBlockedinTurkey and Twitter was once again accessible two hours later, following the removal of most of the pictures and videos of the bombing.[33] Later on, the Sanliurfa Judgeship reversed the gag order and lifted the ban on 173 URLs, citing "press freedom."[34]

- A terrorist attack on October 10, 2015 killed more than 100 people at a peace rally in Ankara.[35] Users reported difficulties accessing witter and Facebook, as well as Instagram posts marked with the hashtags #Istanbul, #Ankara, and #Diyarbakir.[36] The Turkish Supreme Board on Radio and Television (RTÜK) imposed a ban on broadcasting pictures and videos of the massacre and, October 14, Ankara's 6th Judgeship issued a gag order, which lasted fi e days,[37] banning "all kinds of news, interviews, criticism and similar publications in print, visual, social media and all kinds of media on the internet" related to the ensuing investigation.[38]

- On January 12, 2016, a suicide bomber in Istanbul's popular Sultanahmet area killed 10 individuals, mostly German tourists.[39] The prime minister's office quickly anned all media

29 Dag Medya, "TİB, "İdari Tedbir" ile "dagmedya.net" Sitesini Kapattı," August 9, 2015, http://dagmedya.net/2015/08/09/internet-sansuru-tib-idari-tedbir-ile-dagmedya-net-sitesini-kapatti/.

30 Efe Kerem Sozeri, "Social media throttling in Turkey points to wartime censorship efforts," *The Daily Dot*, August 27, 2016, http://www.dailydot.com/layer8/turkey-wartime-censorship-syria/.

31 "Suruc massacre: Mass funeral for Turkey bombing victims," BBC News, July 21, 2015, http://www.bbc.com/news/world-europe-33615239.

32 Efe Kerem Sözeri, "Turkey responds to deadly bombing by censoring social media, news sites," *The Daily Dot,* July 22, 2015 http://www.dailydot.com/layer8/suruc-turkey-censorship-facebook-twitter-youtube/.

33 Victoria Richards, "Twitter temporarily blocked by Erdogan government as Turkey bans images of deadly suicide bombing in Suruc", *Independent*, July 22, 2015 http://www.independent.co.uk/news/world/middle-east/twitter-blocked-by-erdogan-government-as-turkey-bans-images-of-deadly-suicide-bombing-in-suruc-10407387.html

34 "Mahkeme 'basın özgürlüğü'nü hatırladı: Suruç katliamıyla ilgili yayın yasağı kalktı," *Diken*, July 22, 2015, http://www.diken.com.tr/mahkeme-basin-ozgurlugunu-hatirladi-suruc-katliamiyla-ilgili-yayin-yasagi-kalkti/.

35 "Nearly 100 dead as Ankara peace rally rocked by blasts," Al Jazeera, October 10, 2015, http://www.aljazeera.com/news/2015/10/explosions-hit-turkey-ankara-peace-march-151010073827607.html.

36 Esra Dogramaci and Damian Radcliffe, "How Turkey Uses Social Media," Reuters Institute for the Study of Journalism, http://www.digitalnewsreport.org/essays/2015/how-turkey-uses-social-media/.

37 Benjamin Harvey, "How a Bomb Blast in Ankara Became Politicized Before Election Day," Bloomberg, October 23, 2015, http://www.bloomberg.com/news/articles/2015-10-22/confusion-reigns-over-ankara-blast-as-turkish-election-day-nears.

38 "Court issues total media ban over Ankara suicide bombings", *Hurriyet Daily News*, October 14, 2015, http://www.hurriyetdailynews.com/court-issues-total-media-ban-over-ankara-suicide-bombings.aspx?PageID=238&NID=89884&NewsCatID=341.

39 Ceylan Yeginsu and Tim Arango, "Istanbul Explosion Kills 10 Tourists, and ISIS Is Blamed," *The New York Times*, January 12, 2016, http://www.nytimes.com/2016/01/13/world/europe/explosion-in-istanbul-tourist-district-kills-at-least-10.html.

coverage of the blast, citing national security concerns. A few hours later, an Istanbul court issued a gag order affecting social media platforms.[40]

- On March 13, 2016 another suicide bombing occurred in Ankara's Guven Park near a bus stop, killing at least 37 people.[41] Within one hour, Turkish authorities censored news coverage and the RTÜK imposed a ban on broadcasting pictures and videos of the massacre. Turkish ISPs throttled traffic to social media sites like Facebook and Twitter, following an order by an Ankara court.[42] Five days later, Ankara's 6th Criminal Judgeship of Peace issued an order banning 214 URLs that included news and footage of the bombing.

- An attack on March 19, 2016 on Istanbul's Istiklal Street killed five people and wounded 36, mainly foreign tourists.[43] Once again, a media ban was immediately issued by the office of the prime minister. The TİB issued a ban order on all content and news on the bombing, and shortly after, access to Facebook and Twitter[44] was restricted for over 24 hours.[45]

The blog-hosting service WordPress was temporarily blocked in July 2015 over five WordPress-hosted sites on Kurdish politics. In a blog post on its transparency page, WordPress's parent company, Automattic, explained that one of the sites targeted by the TİB for allegedly supporting terrorism actually featured content that was critical of the Kurdistan Workers' Party (PKK), a Kurdish militant group that is classified as a terrorist organization by Turkey, the United States, and a number of other governments.[46] As the site employs HTTPS, a connection method that makes blocking a single page technically very difficult, a second order called for the blocking of the entire WordPress.com domain.[47] Access was later reinstated.

Currently, access to a number of well-known sites and services is blocked, including Metacafe and Imgur.

- URL-shortening services Bit.ly and Dld.bz were both temporarily blocked over the coverage period, although they do not host content. The TİB later restored access to Bit.ly and explained that the site had been banned due to a technical error.[48] Access to Dld.bz was also restored, although without a statement.[49]

40 Charlotte Alfred, "Why Turkey Bans News About Terror Bombings", *Huffington Post*, January 13, 2016, http://www.huffingonpost.com/entry/turkey-media-blackout-istanbul-bombing_us_56957080e4b086bc1cd5a364.

41 Raziye Akkoc, "Ankara explosion: Turkish president vows war on terror as officials say one bomber was 'female Kurdish militant'," *The Telegraph*, March 14, 2016, http://www.telegraph.co.uk/news/worldnews/europe/turkey/12192759/Ankara-explosion-Several-wounded-in-centre-of-Turkish-capital-Kizilay.html.

42 "Turkey explosion: Ankara car bomb kills at least 32," BBC News, March 13, 2016, http://www.bbc.com/news/world-europe-35798517.

43 "Istanbul bombing: At least five killed in Turkish city," Al Jazeera, March 19, 2016, http://www.aljazeera.com/news/2016/03/istanbul-taksim-square-area-hit-explosion-160319091702737.html.

44 "Turkey denies right to seek information following Taksim bombing," D8 News, March 20, 2016, https://d8news.com/after-taksim-terror-attack-turkey-denied-citizens-right-seek-information-970

45 "Turkey: central Istanbul hit by suicide bomb", March 19, 2016, http://www.euronews.com/2016/03/19/explosion-hits-central-istanbul-some-people-wounded-turkey-s-dogan-news-agency/.

46 Kevin Koehler, "Trouble in Turkey," *WordPress Transparency Report, Automattic* (blog), July 31, 2015, http://bit.ly/1joCg7a.

47 Efe Kerem Sozeri, "Ban against a single blog post leads Turkish ISPs to censor all of WordPress," *The Daily Dot*, April 1, 2015, http://bit.ly/1LkEJWM.

48 "Turkey Bans Bitly, Turns Out to be By Accident," *BIAnet*, April 19, 2015, http://bit.ly/1Mcikxb.

49 Ulvi Yaman, "Turkiye Sansurunun Son Alti Yili," July 8, 2015, http://www.ulviyaman.com/blog/2015/07/turkiyede-internet-sansurunun-son-6-yili/.

- The TİB blocked Reddit for three days in November 2015 due to obscenity.[50] Tumblr was blocked by a court order in April 2016, while Metacafe and Imgur remain blocked from previous coverage periods.[51]
- Russian social networking site VKontakte and Deviantart were blocked in early 2016, according to reports from Turkish censorship forums.[52]
- Sanliurfa Criminal Judgeship of Peace issued a blocking order to international sports site Goal.com by reason of illegally betting. The decision was reversed and the site is now accessible.[53]
- EngelliWeb reported that encrypted messaging service Wire and VoIP service Viber were blocked in April 2016 for a few hours. The event was later confi med by Viber.[54]
- On April 11, 2016, Slack, Amazon, and many sites using Amazon Web Services were inaccessible on the TTNet ISP, potentially due to a technical error.[55] TTNet blocked Amazon Web Services without any reason, thus application and websites that are using AWS, including but not limited to Slack, a popular cloud based team collaboration tool, were temporarily down.
- The TİB blocked Russian news agency Sputnik in April 2016.[56] Six days later, Sputnik's Turkish bureau chief Tural Kerimov was refused entry into the country and his residence permit and press credentials were seized.[57] The ban was lifted on August 8, 2016, one day before a meeting between President Erdoğan and his Russian counterpart.[58]

The blocking and removal of online content (see "Content Removal" below) is regulated under Law No. 5651, whose full name is "Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publication."[59] It was initially established in 2007 to protect children and prevent access to illegal and harmful internet content. This includes material related to child sexual abuse, drug use, the provision of dangerous substances, prostitution, obscenity, gambling, suicide promotion, and crimes against Mustafa Kemal Atatürk, the founding father of modern Turkey.[60] The responsibilities of content providers, hosting companies, public access providers, and ISPs are delineated in Law No. 5651. Domestically hosted websites with proscribed content can be taken

50 See https://www.reddit.com/r/europe/comments/3soxpk/reddit_just_got_blocked_in_turkey/.

51 "Tumblr da Erisime Engellendi!," Zete, April 6, 2016, https://zete.com/tumblr-da-erisime-engellendi/.

52 See, for example, http://www.r10.net/teknoloji-haberleri/1565111-deviantart-erisime-engellendi.html, https://eksisozluk.com/entry/58542905, and http://www.kizlarsoruyor.com/ara?q=vkontakte&st=0.

53 Engelliweb data on subject: https://engelliweb.com/url/goal-com.

54 Engelli Web statement on subject: https://twitter.com/engelliweb/status/718597048250011648.

55 See https://twitter.com/turkeyblocks/status/719448397942497280.

56 "Russia's Sputnik news website abruptly blocked in Turkey after 'legal consideration'" April 14, 2016, https://www.rt.com/news/339661-sputnik-site-blocked-turkey/.

57 "Erdogan's war on media: Sputnik Turkey chief banned from entering Istanbul, told to fly o Russia," Russia Today, April 20, 2016, https://www.rt.com/news/340320-sputnik-turkey-chief-prohibited/.

58 "Ankara lifts ban on Sputnik Turkey," Sputnik News, August 8, 2016, https://sputniknews.com/world/201608081044044208-turkey-lifts-ban-sputnik/.

59 Law No. 5651 was published in the *Official Gazette* on May 23, 2007, in issue No. 26030. A copy of the law can be found (in Turkish) at World Intellectual Property Organization, "Law No. 5651 on Regulating Broadcasting in the Internet and Fighting Against Crimes Committed through Internet Broadcasting," http://www.wipo.int/wipolex/en/details.jsp?id=11035; Telekomunikasyon Iletisim Baskanligi (TIB), "Information about the regulations of the content of the Internet," in "Frequently Asked Questions," http://bit.ly/1PtuhBN.

60 Human Rights Watch, "Turkey: Internet Freedom, Rights in Sharp Decline," September 2, 2014, http://bit.ly/1r1kJ0F.

down, while websites based abroad can be blocked and filtered through ISPs. The law has already been found to be in contravention of the European Convention on Human Rights.

In December 2015, the European Court of Human Rights ruled that the blocking of YouTube in 2008 violated Article 10 of the European Convention on Human Rights, specifically the right to freedom of expression. The lawsuit was brought to the court by law professors Serkan Cengiz, Yaman Akdeniz, and Kerem Altıparmak.[61]

Law No. 5651 has repeatedly been amended over the past few years to broaden the scope for censorship.[62] A set of amendments enacted in March 2015 authorized cabinet ministers to order the TİB to block content when necessary to "defend the right to life, secure property, ensure national security and public order, prevent crime, or protect public health." The orders are then taken up within four hours by the TİB, which must also submit the decision to a criminal court within 24 hours. If a judge does not validate the decision within 48 hours, the blocking order must be rescinded.[63] A similar bill passed in September 2014 had been overturned by the Constitutional Court in October of that year. While the original version of Law No. 5651 included only notice-based liability and takedown provisions for content that violates individual rights, changes passed in February 2014 extended this provision to include URL-based blocking orders to be issued by a criminal court judge. The February 2014 amendments also entrusted the TİB with broad discretion to block content that an individual or other legal claimant perceives as a violation of privacy, while failing to establish strong checks and balances. These changes came after leaks of the alleged phone conversations of top government officials on December 17, 2013, and they laid the groundwork for the eventual blocking of social media platforms.

The February 2014 amendments to Law No. 5651 also shield TİB staff if they commit crimes during the exercise of their duties. Criminal investigations into TİB staff can only be initiated through an authorization from the TİB director, and investigations into the director can only be initiated by the relevant minister. This process casts serious doubt on the functioning and accountability of the TİB. ISPs are required to set up a new Association for Access Providers, membership in which is compulsory in order to obtain an "activity certificate" to legally operate in the country. ISPs must also comply with blocking orders from the TİB within four hours or face a penalty of up to TRY 300,000 (US$103,000). Failure to take measures to block all alternative means of accessing the targeted site, such as proxy sites, may result in a fine of up to TRY 50,000 (US$22,000).[64]

The vast majority (94 percent) of blocking orders are issued by the TİB,[65] rather than court orders.[66] The procedures surrounding decisions are nontransparent in both cases, creating significant challenges for those seeking to appeal. Judges can issue blocking orders during preliminary investiga-

61 "Human rights court rules block on YouTube violated freedom of expression," *Today's Zaman*, December 1, 2015, http://www.todayszaman.com/anasayfa_human-rights-court-rules-block-on-youtube-violated-freedom-of-expression_405790.html.

62 World Intellectual Property Organization, "Law No.5651 on Regulating Broadcasting in the Internet and Fighting Against Crimes Committed through Internet Broadcasting," May 4, 2007, http://www.wipo.int/wipolex/en/details.jsp?id=11035.

63 "Approved article gives Turkish gov't power to shut down websites in four hours," *Hurriyet Daily News*, March 20, 2015, http://bit.ly/1C3iuA8.

64 For further information on this section, see Representative on Freedom of the Media, "Briefing on Proposed Amendments to Law No. 5651," Organization for Security and Co-operation in Europe, January 2014, http://bit.ly/1X3Z4az; Center for Internet and Society, Stanford Law School, "WILMAP: Turkey," accessed November 6, 2014, http://stanford.io/1YcN8EX.

65 Engelli Web, "Kurum Bazinda Istatistikler," accessed February 28, 2016, http://engelliweb.com/istatistikler/.

66 According to TİB statistics from May 2009, the last date these were available, the courts are responsible for 21 percent of blocked websites, while 79 percent are blocked administratively by the TİB. Reporters Without Borders, "Telecom Authority Accused of Concealing Blocked Website Figures," May 19, 2010, http://en.rsf.org/turkey-telecom-authority-accused-of-19-05-2010,37511.html.

tions as well as during trials. The reasoning behind court decisions is not provided in blocking notices, and the relevant rulings are not easily accessible. As a result, it is often difficult for si e owners to determine why their site has been blocked and which court has issued the order. The TİB's mandate includes executing judicial blocking orders, but it can also issue administrative orders for foreign websites, content involving sexual harassment of children, and obscenity. Moreover, in some cases it successfully asks content and hosting providers to remove offending items from their servers, in order to avoid issuing a blocking order that would affect an entire website. This occurs despite the fact that intermediaries are not responsible for third-party content on their sites. The fil ering database is maintained by the government without clear criteria. A "Child and Family Profiles Cri eria Working Committee" was introduced to address this problem in 2012, but it was largely made up of BTK members or appointees and does not appear to be active.

In addition to these blocks, ISPs offer "child" and "family" fil ering options under rules established by the BTK in 2011, though the fil ering criteria have been criticized as arbitrary and discriminatory.[67] The BTK tried to mandate fil ering for all users in 2011,[68] but withdrew the proposal following a legal challenge.[69] The child fil er obstructs access to Facebook, YouTube, Yasam Radyo (Life Radio), the Armenian minority newspaper *Agos*, and several websites advocating the theory of evolution,[70] even as some anti-evolution websites remain accessible.[71] Internet access is fil ered at primary education institutions and public bodies, resulting in the blocking of a number of minority news sites.[72]

Content Removal

In addition to widespread fil ering, state authorities are proactive in requesting the deletion or removal of content. Social media platforms comply with administrative decisions and court orders as promptly as possible in order to avoid blocking and, more recently, throttling. Like international social media platforms, popular Turkish websites are also subject to content removal orders. Courts issued several orders pertaining to user-generated content websites such as Eksi Sozluk (Sour Dictionary), Inci Sozluk (Pearl Dictionary), and ITU Sozluk (Istanbul Technical University Dictionary).

Turkey has consistently featured among the countries with the highest number of removal requests sent to Twitter. Of all of the tweets "withheld" by Twitter around the world in the second half of 2015, Turkey accounted for almost 90 percent. Requests from courts and government agencies reached 2,211, and rose to 2,493 in the fi st half of 2016. In each reporting period, Twitter indicated it complied in 23 percent of cases. [73]

Some believe Twitter has under-reported its own censorship in Turkey.[74] The company was fined T Y

67 Reporters Without Borders, "New Internet Filtering System Condemned as Backdoor Censorship," December 2, 2011, http://bit.ly/1W3FNp7.

68 Decision No. 2011/DK-10/91 of Bilgi Teknolojileri ve İletişim Kurumu, dated February 22, 2011.

69 On September 27, 2011, the Council of State rejected the "stay of execution" request by BIAnet referring to the annulment of the February 22, 2011.

70 Dorian Jones, "Turkey Blocks Web Pages Touting Darwin's Evolution Theory," Voice of America, December 23, 2011, http://bit.ly/1Lh9DmR.

71 Sara Reardon, "Controversial Turkish Internet Censorship Program Targets Evolution Sites," *Science Magazine*, December 9, 2011, http://bit.ly/1OfyitJ; Haber Merkezi, "Agos'u Biz Değil Sistem Engelledi," [Agos was fil ered through the Ministry of Education fil er], *BIAnet*, January 23, 2012, http://bit.ly/1jzOWr4.

72 "Meclis'te Alevi Sitesine Yanlışlıkla Sansür," *BIAnet*, December 8, 2014, http://bit.ly/1FNfbzb.

73 Twitter, "Turkey," *Transparency Report* https://transparency.twitter.com/en/countries/tr.html.

74 "Known Unknowns: An Analysis of Twitter Censorship in Turkey" http://www.cs.rice.edu/~rst5/twitterTurkey/paper.pdf.

150,000 (US$51,000) by the BTK for failure to remove "terrorist propaganda" from the site in December 2015,[75] although Twitter appealed the fine in a urkish court one month later.[76]

According to Facebook's Government Requests Report for the period of July to December 2015, the company restricted 2,078 pieces of content on orders from both the BTK and Turkish law enforcement, particularly in compliance with Law No. 5651 on the internet.[77] In March 2016, *Yeni Şafak*, a progovernment daily newspaper, claimed that their official acebook page with 10 million "Likes" was removed without notice. The newspaper stated the move was meant to "silence Turkish media" and, along with the TİB, condemned Facebook. In a statement, the company confi med they had noticed "irregularities" in the number of the page's followers, which according to one journalist, had increased by fi e million in only eight months. Facebook reopened the page 10 days later after removing 2.5 million "spurious likes."[78]

Media, Diversity, and Content Manipulation

The climate of fear created by widespread government prosecution of online activities has led to an increase in self-censorship, particularly when it comes to criticism of the government or public officials. Speech on Islam or the p ophet Muhammad, as well as posts about the "Kurdish problem" or even calls for peace can result in death threats and legal battles. Turkish-Armenian relations have become less controversial in recent years, but they remain sensitive, particularly during periods of ethnic tension and violence in the southeast.

Turkish users increasingly rely on internet-based publications as a primary source of news, and despite the country's restrictive legal environment and growing self-censorship, the Turkish blogosphere is still surprisingly vibrant and diverse. There are a wide range of blogs and websites through which citizens question and criticize Turkish politics and leaders, including on issues that are generally viewed as politically sensitive. The majority of civil society groups maintain an online presence.

Numerous[79] reports[80] have revealed that an "army of trolls," numbering around 6,000 individuals, has been enlisted by the ruling AKP to manipulate discussions, drive particular agendas, and counter government critics on social media.[81] Journalists and scholars who are critical of the government have faced orchestrated harassment on Twitter, often by dozens or even hundreds of users.[82] Shortly before the November 2015 elections, progovernment trolls circulated allegations that Oy ve Otesi (Vote and Beyond), the fi st civic election-monitoring initiative in Turkey, was committing fraud and aiding terrorist organizations. A Twitter account named "Vote and Fraud" with 42,000 followers warned supporters not to get involved with the group. Only a week before the smear campaign, it was found that the account had purported to be a young girl sharing romantic quotes, adding to

75 "Turkey fines witter for failure to remove 'terrorist propaganda', " *Hurriyet Daily News*, December 11, 2015, http://www.hurriyetdailynews.com/Default.aspx?pageID=238&nID=92387&NewsCatID=339.

76 "Twitter sues Turkey over 'terror propaganda' fine" Al Jazeera, January 7, 2016, http://www.aljazeera.com/news/2016/01/twitter-sues-turkey-terror-propaganda-fine-160107173150687.htm .

77 Facebook, "Turkey," *Government Requests Report*, July to December 2015, accessed October 15, 2016, https://govtrequests.facebook.com/country/Turkey/2015-H2/#.

78 Efe Kerem Sozeri, " The rotten politics infecting Turkey's social media, " *The Daily Dot*, March 30, 2016, http://www.dailydot.com/politics/turkey-social-media-yeni-safak-facebook-twitter-manipulation/.

79 Dion Nissembaum, "Before Turkish Coup, President's Drive to Stifle Dissent So ed Unrest," *The Wall Street Journal*, July 15, 2016, http://www.wsj.com/articles/before-turkish-coup-presidents-drive-to-stifle-dissen -sowed-unrest-1468632017.

80 Efe Kerem Sozeri, "RedHack leaks reveal the rise of Turkey's pro-government Twitter trolls," *The Daily Dot,* September 30, 2016, http://www.dailydot.com/layer8/redhack-turkey-albayrak-censorship/.

81 "CHP asks if pro-gov't trolls put on AK Party payroll," *Cihan*, September 4, 2014, http://bit.ly/1UWSepJ.

82 Emre Kizilkaya, "AKP's social media wars," *Al Monitor*, November 15, 2013, http://bit.ly/1LhdTCG.

speculation that "Vote and Fraud" was a fake account created solely for the purposes of trolling.[83] Progovernment trolls have also been active amid rising tensions with foreign governments, such as Russia, which recently commenced a propaganda campaign against Turkey after the shooting down of a Russian jet in December 2015. In response, "TrollState Russia" became a trending topic on Twitter in a campaign allegedly orchestrated by Erdoğan's public communication office .[84]

Although a large number of websites are blocked, circumvention tools are widely available, enabling users to avoid fil ers and blocking mechanisms. Each time a new order is issued and a popular website is blocked, articles are published to instruct users on how to access it. As proof of users' tech savviness, YouTube was the eighth-most-accessed site in Turkey in 2010, at a time when it was officially blocked.[85] However, when internet users employed Google's Domain Name System (DNS) service and OpenDNS to evade blocks on both Twitter and YouTube in 2014,[86] Google announced that it had received several credible reports and later confi med that Turkish ISPs had intercepted and hijacked the settings.[87]

Turkish users often turn to the internet to find news on domestic issues not co ered by mainstream broadcast media. According to IAB Turkey Internet Audience Measurement, the most visited online news source is milliyet.com.tr, the online edition of the newspaper *Milliyet*. *Hurriyet*, an influential newspaper is the second-most visited online news source.[88] New models for citizen journalism and volunteer reporting are also gaining traction, such as 140journos, dokuz8haber (literally, "nine-8news"), and Otekilerin Postasi ("The Others' Post") whose editor was arrested in November 2015. News about the southeastern region of the country, heavily populated by Kurds, is heavily infl - enced by the government. Frequent power outages, mobile internet shutdowns, and censorship of prominent local news sites make information gathering even more difficult in that a ea.

On March 4, 2016, Gülen-linked newspapers *Zaman* and *Today's Zaman*, as well as Cihan News Agency, were seized and new progovernment[89] editorial boards were established by a court order.[90] The online archives of each paper were deleted, as well as Zaman's previous Twitter activity.[91]

Digital Activism

Digital activism has played a significant ole in the country, particularly after the Occupy Gezi protests of 2013. In March 2016, mobile operator Turkcell came under fi e on social media for its sponsorship of the Ensar Foundation, which was allegedly involved in a child sex abuse scandal. After the

83 Efe Kerem Sozeri, "How pro-government trolls are using a sexy Twitter bot to sway Turkey's election, " *Daily Dot*, October 31, 2015, http://www.dailydot.com/politics/turkey-election-twitter-troll-vote-and-beyond-vote-and-fraud/.

84 Efe Kerem Sozeri, "Inside the great troll war between Russia and Turkey, " *Daily Dot*, December 14, 2015, http://www.dailydot.com/politics/russia-turkey-missle-turkey-troll-war-twitter/.

85 Alexa, "Turkey," in "Top Sites," accessed August 26, 2010, http://www.alexa.com/topsites/countries/TR.

86 Emre Peker, Joe Parkinson, and Sam Schechner, "Google, Others Blast Turkey," *Wall Street Journal*, March 31, 2014, http://on.wsj.com/1KgtnVD.

87 "Google says Turkey intercepting its Web domain," *Hurriyet Daily News*, April 31, 2014, http://bit.ly/1iPtvlX.

88 IAB Turkey Internet Audience Measurement, February 2016, http://www.iabturkiye.org/sites/default/files/in ernet_audience_toplist_02_2016_son.pdf.

89 "Zaman newspaper: Seized Turkish daily 'now pro-government'," BBC News, March 6, 2016, http://www.bbc.com/news/world-europe-35739547.

90 "Istanbul court to appoint trustees for Zaman, Today's Zaman editorial board," Committee to Protect Journalists, March 4, 2016, https://cpj.org/2016/03/istanbul-court-to-appoint-trustees-for-zaman-today.php.

91 Zaman's Twitter account has been renamed "@AnalizMerkez." See to Efe Kerem Sozeri's statement: https://twitter.com/efekerem/status/706282702861942784?lang=en and https://web.archive.org/web/20160306005700/https:/twitter.com/analizmerkez.

company refused to cut ties with the foundation, it also sought help from the courts to censor 862 tweets from 743 accounts in order to curb critical coverage.[92] As a result, hashtags such as #Tecavüz-Cell (RapeCell), #EnsarCell, and #SansürCell (CensorCell) started trending on Twitter. Twitter refused to comply with a court order to remove the tweets and emailed users stating that the company will appeal the decision in a higher court.[93] Digital rights lawyers Yaman Akdeniz and Kerem Altiparmak also filed an appeal befo e the Constitutional Court.[94] Turkcell continued to call for the removal of hundreds,[95] and later thousands[96] of additional tweets throughout the month of April and even filed a lawsuit for TRY 10,000 (approximately US$3,000) of damages from 124 Twitter users.[97]

Organizations such as Oy ve Ötesi (Vote and Beyond), the fi st civic election-monitoring initiative, used social media tools to enlist over 60,000 volunteers to monitor more than 130,000 ballot boxes during the general elections of November 2015,[98] despite unsuccessful attempts to ban the organization.[99] Dogruluk Payi ("Share of Truth"), Turkey's fi st and only political fact-checking website, was also a popular source for information during the elections.[100]

Violations of User Rights

While prison sentences for online speech have been rare, several individuals were sentenced to lengthy terms over the past year for allegedly insulting public officials or spreading terrorist propaganda. Journalists, public figures, and young students have been targeted for nonviolent speech that is critical of the government or touches on controversial issues of Kurdish identity. Surveillance remains a key issue, but cybersecurity made headlines over the past year amid a massive leak of Turkish citizens' personal data and a nationwide cyberattack that brought down thousands of websites, including retail banking infrastructure.

Legal Environment

The Turkish constitution includes broad protections for freedom of expression. Article 26 states that "everyone has the right to express and disseminate his thought and opinion by speech, in writing or in pictures or through other media, individually or collectively."[101] Turkish legislation and court judgments are subject to the European Convention on Human Rights and bound by the decisions of

92 Daghan Irak, "Sparks Fly with Turkcell under the 'Spotlight'," Research Turkey April 13, 2016, http://researchturkey.org/sparks-fly-with-tur_cell-under-the-spotlight/.

93 Efe Kerem Sozeri, "Turkish court orders 860 tweets censored after ISP boycott sparked by child-rape scandal," *The Daily Dot,* April 12, 2016, http://www.dailydot.com/politics/turkcell-twitter-censorship-protest-ensar-foundation/.

94 Press Relase, "Turkcell'in Ensar Vakfı Eleştirileri ile ilgili Aldırdığı Sansür Kararını Anayasa Mahkemesi'ne taşıdık," May 31, 2016, http://privacy.cyber-rights.org.tr/?p=1611.

95 "#SansürCell seriye bağlandı: Turkcell 423 tweete daha erişim engeli getirtti," Diken, April 28, 2016, http://www.diken.com.tr/mahkeme-turkcelle-tepkinin-onunu-yine-kesti-423-tweete-erisim-engeli/.

96 Efe Kerem Sozeri, "A Turkish mobile provider got 13 court orders to erase this hashtag from the Internet," *The Daily Dot*, May 20, 2016, http://www.dailydot.com/layer8/turkcell-tecavucell-twitter-censorship/.

97 "Turkcell'den yeni hamle: 124 kişiye 10 bin lira manevi tazminat davası," Diken, June 4, 2016, http://www.diken.com.tr/turkcellden-tepkilere-karsi-yeni-hamle-124-kisiye-10-bin-lira-manevi-tazminat-davasi/.

98 Oy ve Ötesi Derneği, "Seçim Sonuç Değerlendirmeleri" [in Turkish], news release, June 10, 2015, http://oyveotesi.org/1-kasim-2015-genel-secimleri/1-kasim-2015-secim-sonuc-degerlendirmeleri/.

99 "Top election body rejects banning civilian group from monitoring elections", October 31, 2015, *Today's Zaman,* http://www.todayszaman.com/national_top-election-body-rejects-banning-civilian-group-from-monitoring-elections_403027.html.

100 Riada Ašimović Akyol, "Will new Turkish fact-checking site be able to hold politicians accountable?," *Al Monitor*, February 3, 2016, http://www.al-monitor.com/pulse/originals/2016/02/turkey-politics-meet-fact-checking.html#.

101 The Constitution of the Republic of Turkey, accessed April 22, 2013, https://global.tbmm.gov.tr/docs/constitution_en.pdf.

the European Court of Human Rights. The constitution also seeks to guarantee the right to privacy, though there are limitations on the use of encryption devices, and surveillance by security agencies is highly prevalent. There are no laws that specifically criminalize online activities li e posting one's opinions, downloading information, sending email, or transmitting text messages. Instead, many provisions of the criminal code and other laws, such as the Anti-Terrorism Law, are applied to both online and offline activit .

Defamation charges have been frequently used to prosecute government critics. According to Article 125 of the Turkish criminal code, "anyone who undermines the honor, dignity or respectability of another person or who attacks a person's honor by attributing to them a concrete act or a fact, or by means of an insult shall be sentenced to imprisonment for a term of three months to two years, or punished with a judicial fine" Defaming a public official carries a minimum one ear sentence, while insults to the president entails a sentence of one to four years according to Article 299. Several courts deemed Article 299 unconstitutional in the fi st half of 2016 and requested the matter be taken up by the Constitutional Court.[102] Cases related to insulting the president have seldom resulted in jail sentences, although some defendants have been jailed while awaiting trial.

According to Article 7 of the Anti-Terror Law, "those who make propaganda of a terrorist organization by legitimizing, glorifying or inciting violent methods or threats" are liable to prison terms of one to fi e years. The law has been widely criticized for its broad definition f terrorism, which has been exploited by courts to prosecute journalists and academics with no affiliation o terrorism for the simple act of criticizing the government.[103]

Prosecutions and Detentions for Online Activities

Arrests and prosecutions for social media posts have increased in recent years, and in some cases, individuals have been imprisoned. Over the past year, hundreds of Twitter users faced charges of insulting government officials, defaming P esident Erdoğan, or sharing propaganda in support of terrorist organizations.

Several journalists were charged for their social media activities, including:

- Journalist Hayri Tunç, who works for the news site *Jiyan*, was arrested on February 2, 2016 and later sentenced to two years in prison for "terrorism propaganda," "abetting criminal acts," and "glorifying criminal acts." He was targeted for posting tweets, Facebook posts, and YouTube videos that mainly covered fighting bet een the security services and Kurdish militants.[104] He appealed the decision shortly after his June 2016 sentencing.[105]
- In September 2015, journalist and writer Aytekin Gezici received a combined prison sentence of fi e years and nine months, in addition to a judicial fine equi alent to 21 months

102 "Local court applies to Turkey's top court to annul article on 'insulting president'," *Hurriyet Daily News*, March 30, 2016, http://www.hurriyetdailynews.com/local-court-applies-to-turkeys-top-court-to-annul-insulting-president-law.aspx?pageID=238&nID=97103&NewsCatID=509.

103 "Why Turkey's terror law is the 'Achilles heel' of the EU-Turkey visa deal," France 24, May 13, 2016, http://www.france24.com/en/20160513-why-turkeys-terror-law-achilles-heel-eu-turkey-migrant-deal.

104 Efe Kerem Sozeri, "Kurdish Reporter Faces Jail Time in Turkey for Twitter and Facebook Posts, " *Global Voices*, March 9, 2016, https://globalvoices.org/2016/03/09/kurdish-reporter-faces-jail-time-in-turkey-for-twitter-and-facebook-posts/.

105 "Gazeteci Hayri Tunç'a 2 yıl hapis cezası!," Birgun, June 7, 2016, http://www.birgun.net/haber-detay/gazeteci-hayri-tunc-a-2-yil-hapis-cezasi-115140.html.

in prison, for "insulting" President Erdoğan, former deputy prime minister Bulent Arinç, and former justice minister Bekir Bozdağ on Twitter.[106] He was acquitted of similar charges against two other public officials. Gezici had been detained in Oc ober 2014 in Adana after a police raid on his home.[107] Although he was not immediately imprisoned (likely due to an appeal), he was detained in July 2016 for alleged links to the failed coup.[108]

- Bülent Keneş, editor-in-chief of *Today's Zaman*, was arrested in October 2015 for allegedly insulting President Erdoğan on Twitter.[109] In March, he was sentenced to over 2.5 years in prison, although he was not yet imprisoned, likely due to an ongoing appeal.[110]

- Journalist and anchorwoman Sedef Kabaş was acquitted in October 2015 of "menace" and "targeting public officials in olved in counter-terrorism."[111] Earlier, she had her home raided and was detained for a tweet that alluded to a cover up of a government corruption scandal."[112]

- In April 2016, journalist Hamza Aktan was arrested after retweeting a request from the BBC for people in Cizre to send pictures to the BBC. He faced a one- to fi e-year prison sentence.[113]

Journalists were not the only ones targeted for the social media activity. Prominent figu es and even lesser known citizens were charged over the past year, including:

- Merve Büyüksaraç, a former "Miss Turkey," was given a 14-month suspended prison sentence in May 2016.[114] She had been on trial since 2015 for sharing a satirical poem on Instagram related to President Erdoğan's corruption scandal that had originally appeared in the Turkish comic *Uykusuz*.[115]

- Bercan Aktas, a 22-year-old media student and member of the opposition People's Democratic Party (HDP), was arrested in August 2015 for a tweet stating "A special forces police officer was neutralized" rather than using the erm "martyred." "Neutralized" is the term employed by the mainstream media to describe the death of alleged Kurdish militants. He was detained for over one month and later received a suspended prison sentence of one year and three months.[116]

106 "Gazeteci Aytekin Gezici'ye Erdogan'a hakareten 6 yil hapis," *Birgün,* September 17, 2015, http://bit.ly/1Lb26UR.

107 "Turkey's journalists challenged by growing judicial, political pressure," *Today's Zaman,* May 28, 2015, http://bit.ly/1iPzx61.

108 Gündem Haberi, "Aytekin Gezici tutuklandı, Yüksel Evsen Adli Kontrolle serbest...," Ajans Adana, July 25, 2016, http://ajansadana.com/haber-8406-aytekin_gezici_tutuklandi..._yuksel_evsen_adli_kontrolle_serbest....html.

109 "Editor-in-chief arrested over tweet," *Todays's Zaman*, October 9, 2015, http://www.todayszaman.com/national_editor-in-chief-arrested-over-tweet_401136.html.

110 "Bülent Keneş'e 'Cumhurbaşkanına hakaret'ten hapis cezası," Anadolu Ajansi, March 24, 2016, http://aa.com.tr/tr/turkiye/bulent-kenese-cumhurbaskanina-hakaretten-hapis-cezasi/543362.

111 "Journalist Sedef Kabaş acquitted in trial over critical tweet by İstanbul court," *Today's Zaman,* October 6, 2015, http://bit.ly/1joEtPW.

112 "Twitter Transparency Report: Turkey Tops Censorship List by Margin," *Today's Zaman,* February 6, 2015, http://bit.ly/1Qi8Sta.

113 "Journalist detained in Turkey over tweets," Hurriyet Daily News, April 30, 2016, http://www.hurriyetdailynews.com/journalist-detained-in-turkey-over-tweets.aspx?pageID=238&nID=98552&NewsCatID=341.

114 "Ex-Miss Turkey sentenced for insulting Erdogan," BBC, May 31, 2016, http://www.bbc.com/news/world-europe-36419723.

115 Adam Taylor, "How a single Instagram post could end up sending a former Miss Turkey to jail," *Washington Post*, February 25, 2015, http://wapo.st/1LyEfMm.

116 Efe Kerem Sozeri, "Turkish student detained for terrorism after tweeting about a dead soldier, " *Daily Dot*, August 19, 2015, http://www.dailydot.com/politics/can-you-go-to-jail-for-tweeting/.

- A 14-year-old schoolboy was held overnight at a police station in October 2015 for "insulting" President Erdoğan on Facebook.[117]

- Bilgin Çiftçi, a family doctor in the province of Aydin, shared a popular meme comparing President Erdoğan's facial expressions to a character in the Lord of the Rings movies. He was charged with insulting the president in December 2015 and faces up to two years in prison. In defense of Çiftçi, the films' di ector Peter Jackson claimed that the picture did not portray Gollum, but rather his alternate ego "sweet Smeagol," and therefore should not be considered insulting.[118] Another person, Rifat Çetin, shared a similar content in 2014 and was handed a suspended prison sentence of one year. The judge had assembled a panel of film experts to determine whether or not the image was insulting.[119]

- In February 2016, 23-year-old university student Gizem Yerik was pulled from a lecture and taken into custody on charges of defaming the president and spreading PKK propaganda through her social media posts. Alleging that there was no ward for women in the jail, she was reportedly kept in solitary confinement for six days until she was sent o Gebze prison. She was released on probation on May 11, 2016 and later sentenced to 11 months and 20 days for insulting the president, in addition to a prison term of 3 years and 9 months for spreading propaganda in support of terrorist organizations.[120]

President Erdoğan has reportedly filed criminal complaints against mo e than 250 people for "insulting" him online and more than 2,000 people for "insulting" him by any means since he was elected president in August 2014.[121] Speaking on July 30, 2016, after the failed coup, President Erdoğan announced he would withdraw all such lawsuits.[122] Nevertheless, Article 125(3) and Article 299 of the penal code remained in place as of writing.

Surveillance, Privacy, and Anonymity

Government surveillance, the bulk retention of user data, and limitations on encryption and anonymity are all concerns in Turkey. Leaked emails revealed a contract between the Italian surveillance software company Hacking Team and the General Directorate of Security (GDS), a civilian police force, for the use of Hacking Team's "Remote Control System" from June 2011 to November 2014.[123] Under Turkish law, the interception of electronic communications falls under the purview of the TİB, and questions remain over the legality of the GDS using software that can infiltra e targets' computers. The prominence of so-called Gülenists in the police and judiciary has been a major point of

117 Avi Asher-Schapiro, "Teen Arrested for 'Insulting' Erdogan on Facebook as Crackdown in Turkey Continues," Vice News, October 23, 2015, https://news.vice.com/article/teen-arrested-for-insulting-erdogan-on-facebook-as-crackdown-in-turkey-continues.

118 Efe Kerem Sozeri, "Turkish court hires Gollum witnesses after doctor compares LOTR character to president," *Daily Dot*, December 2, 2015, http://www.dailydot.com/politics/turkey-gollum-meme/.

119 "Turkey guilty verdict for depicting Erdogan as Gollum, " BBC, June 23, 2016, http://www.bbc.com/news/world-europe-36610000.

120 "Üniversite öğrencisi Gizem Yerik'e hapis cezası," HaberTurk, May 13, 2016, http://www.haberturk.com/gundem/haber/1238957-universite-ogrencisi-gizem-yerike-hapis-cezasi.

121 Finkel, "Miss Turkey on Trial for Allegedly Insulting President Erdogan." and "Cumhurbaskanina Hakaret Davalarinda Patlama" in Turkish, *Aktif Haber*, November 22, 2015, http://www.aktifhaber.com/cumhurbaskanina-hakaret-davalarinda-patlama-1263244h.htm.

122 "President Erdoğan withdrawing lawsuits filed for insult" *Hurriyet Daily News*, July 30, 2016, http://www.hurriyetdailynews.com/president-erdogan-withdrawing-lawsuits-filed-fo -insult.aspx?pageID=238&nID=102278&NewsCatID=338.

123 Efe Kerem Sözeri, "Turkey paid Hacking Team $600k to spy on civilians," *The Daily Dot*, July 7, 2015, http://www.dailydot.com/politics/hacking-team-turkey/.

discussion in the country in recent years, particularly after Gülenists were widely blamed for leaked wiretaps that led to various government corruption scandals in 2013 and 2014. Further scandals prompted high-level sackings and reshuffling within the police and judicia y, apparently aimed at removing suspected Gülenist officials [124]

According to Article 22 of the constitution, "everyone has the right to freedom of communication, and secrecy of communication is fundamental." This right can only be violated under a court order in cases of "national security, public order, prevention of the commission of crimes, protection of public health and public morals, or protection of the rights and freedoms of others, or unless there exists a written order of an agency authorized by law in cases where delay is prejudicial."[125] For the most part, any action that could interfere with freedom of communication or the right to privacy must be authorized by the judiciary. For example, judicial permission is required for technical surveillance under the Penal Procedural Law. Before the passage of the Homeland Security Act in March 2015, the law allowed Turkish security forces to conduct intelligence wiretapping for 24 hours without a judge's permission in urgent situations. However, with the new law the time limit was increased to 48 hours, with a new requirement that wiretapping officials noti y their superiors. In addition, only the Ankara High Criminal Court is authorized to decide whether the wiretapping is legitimate. Despite constitutional guarantees, most forms of telecommunication continue to be tapped and intercepted.[126]

Furthermore, Turkey's National Intelligence Organization (MİT) received expanded powers to conduct surveillance in April 2014. Law 6532 on Amending the Law on State Intelligence Services and the National Intelligence Organization grants intelligence agents unfettered access to communications data without a court order. The law forces public and private bodies—including but not limited to banks, archives, private companies, and professional organizations such as bar associations—to provide the MİT any requested data, documents, or information regarding certain crimes, such as crimes against the security of the state, national security, state secrets, and espionage. Failure to comply is punishable by prison. In a clause related to the MİT's ability to intercept and store private data on "external intelligence, national defense, terrorism, international crimes, and cyber-security passing through telecommunication channels," no requirement to procure a court order is mentioned.[127] The law also limits MİT agents' accountability for wrongdoing. Courts must obtain the permission of the head of the agency in order to investigate agents, and journalists or editors who publish leaks on MİT activities via media channels may be imprisoned for three to nine years. Some observers have argued that the bid to shield the MİT from judicial investigations was intended to provide legal cover for the agency's negotiations with the PKK, which is officially ecognized as a terrorist organization; it also facilitated the crackdown on government opponents such as the Gülenists.[128] The opposition Republican People's Party (CHP) objected to the MİT law and filed an appeal with the Constitutional Court.

In 2013, the daily newspaper *Taraf* filed a complaint at the Constitutional Cou t against the MİT for illegally tapping journalists' phones. Lawyers had initially filed a complaint with the Istanbul Public

124 "Turkish court accepts indictment of TIB over illegal spying," *TRT World,* June 2, 2015, http://bit.ly/1FgTTyZ.

125 The Constitution of the Republic of Turkey.

126 For a history of interception of communications, see Faruk Bildirici, *Gizli Kulaklar Ulkesi* [The Country of Hidden Ears] (Istanbul: Iletisim, 1999); Enis Coskun, *Kuresel Gozalti: Elektronik Gizli Dinleme ve Goruntuleme* [Global Custody: Electronic Interception of Communications and Surveillance] (Ankara: Umit Yayincilik, 2000).

127 Human Rights Watch, "Turkey: Internet Freedom, Rights in Sharp Decline," September 2, 2014, http://bit.ly/1r1kJ0F.

128 See Sebnem Arsu, "Turkish Leader Signs Bill Expanding Spy Agency's Power," *New York Times*, dated April 25, 2014, http://nyti.ms/1McuXsn; and Fehim Taştekin, "Is Turkey reverting to a 'muhaberat' state?" *Al-Monitor*, April 17, 2014, http://bit.ly/1NDF1h7.

Prosecutor's Office in 2012, but since MİT agents can only be p osecuted with the permission of the prime minister, the prosecutor's office decided not o pursue the case.[129] In May 2015 the Constitutional Court ruled that issuing such wiretapping orders was a violation of constitutional rights, particularly the right to privacy.[130]

The constitution states that "secrecy of communication is fundamental," and users are allowed to post anonymously online. However, the anonymous purchase of mobile phones is not allowed; buyers must provide official identification. Acc ding to a Council of Ministers decision dated 2000, Turkish citizens may only import one mobile phone per two years. Imported devices can be registered at mobile phone operators' subscription centers and an e-government website, for a fee of TRY 131.50 (US$45). Devices that are not registered within 60 days are shut off from telecommunications networks. In 2011, the BTK imposed regulations on the use of encryption hardware and software. Suppliers are required to provide encryption keys to state authorities before they can offer their products or services to individuals or companies within Turkey. Failure to comply can result in administrative fines and, in cases elated to national security, prison sentences.

Under Law No. 5651, hosting and access providers must retain all traffic info mation for one year and maintain the accuracy, integrity, and confidentiality f such data. In addition, access providers must file the data ogether with a time stamp and provide assistance and support to the TİB in monitoring internet traffic. On December 8, 2015, the Constitutional Cou t nullified a set f amendments passed in February 2014, including a requirement that hosting providers must store data for up to two years.[131] However, the decision will not enter into force until December 2016.

Public-use internet providers hold different responsibilities depending on their status as either commercial or noncommercial. Commercial providers are defined as entities that p ovide internet service upon a certain payment, such as internet cafes. Noncommercial public-use internet providers are defined as entities that p ovide internet service at a certain venue for a certain period of time, such as in hotels and restaurants. While all public-use internet providers are expected to take measures to prevent access to criminal content and store internal IP distribution logs, commercial providers must also receive permission from the local administration, use a content-fil ering service approved by the TİB, and keep accurate daily records of internal IP distribution logs using software supplied by the TİB, which must be stored for a period of one year. In addition, these commercial providers are required to install a video surveillance system so as to identify users, and retain such records for seven days. All data must be made available to the TİB upon request—and without the need for a court order—under penalty of TRY 10,000 to 100,000 (US$4,400 to 44,000) in fines[132]

In a largely positive note, a new Data Protection Law was passed and entered into force on April 7, 2016, aligning the country's legislation with EU standards.[133]

129 "Taraf daily to take MİT's wiretapping to Constitutional Court," *Today's Zaman*, August 25, 2013, http://bit.ly/1KnwFDj.

130 "Top court rules against Turkish intelligence over wiretapping journalists," *BGN News*, May 10, 2015, http://bit.ly/1OfTWhm.

131 Burçak Unsal, "The Constitutional Court's decision on internet law," *Hurriyet Daily News*, December 14, 2015 http://www.hurriyetdailynews.com/the-constitutional-courts-decision-on-internet-law.aspx?pageID=238&nID=92470&NewsCatID=. 396

132 For further information on this section, see Representative on Freedom of the Media, "Briefing on P oposed Amendments to Law No. 5651," Organization for Security and Co-operation in Europe, January 2014, http://www.osce.org/fom/110823?download=true; Center for Internet and Society, Stanford Law School, "WILMAP: Turkey," accessed November 6, 2014, http://stanford.io/1YcN8EX.

133 Naz Degirmenci, "Turkey's First Comprehensive Data Protection Law Comes Into Force," Inside Privacy, April 8, 2016, https://www.insideprivacy.com/data-security/turkeys-fi st-comprehensive-data-protection-law-comes-into-force/.

Intimidation and Violence

Citizen journalists and reporters for online news outlets operate in an environment in which media workers have often been physically assaulted for their reporting.[134] Online journalists have been targeted while at protests; for example, police attempted to detain Bianet reporter Beyza Kural during a demonstration in November 2015.[135] Social media users—particularly public figu es, journalists, and intellectuals—face online harassment for their posts.

Technical Attacks

Popular news organizations such as *Zaman*, *Today's Zaman*, *Cihan*, *Rotahaber*, *Radikal*, *Sözcü*, and *Taraf* reported cyberattacks against their websites during the November 2015 elections. The arts-and-culture news website Sanatatak.com experienced technical attacks after publishing a letter supporting Turkish actress Füsun Demirel, who declared that she "wanted to be to be a [Kurdish] guerrilla" in her youth. The website was inaccessible for around 48 hours on March 21, 2016 due to distributed denial of service (DDoS) attacks.[136] The HDP's website was attacked two days before the June 2015 elections and could not be accessed for over 24 hours.

Starting on December 14, 2015, Turkey suffered a 14-day long cyberattack to its official domain name servers, disconnecting almost 400,000 Turkish domains belonging to companies, government institutions, schools, e-mail services, and many other online services. On the fi st day of the attack, Turkey's National Response Center for Cyber Events (USOM) cut all incoming foreign traffic o nic.tr, an administrative nongovernmental authority run by the Computer Center of Middle East Technical University, making Turkish websites with .tr domain names unreachable from the rest of the world.[137] On December 24, three of Turkey's largest banks were targeted, disrupting online banking, ATM, and POS services. Although some suspected the attack to have originated in Russia, Anonymous claimed responsibility for the DDoS attack, accusing Turkey of supporting the so-called Islamic State.[138]

Furthermore, in March 2016, the addresses, identity numbers, and other personal information of almost 50 million Turkish citizens were uploaded onto a website titled the "Turkish Citizenship Database" in a massive data leak. The website stated that the personal information of prominent public figu es such as the president and prime minister could be found in the 1.5 gigabyte file and taun ed President Erdoğan. According to Transport and Communication Minister Binali Yildirim, the breach appeared to date back to at least 2010. An expert stated that the data was taken from the government's official opulation Governance Central Database (MERNIS) around 2009 and later illegally sold to foreclosure fi ms. [139]

134 "Hurriyet columnist Ahmet Hakan injured in 'organized assault'," *Hurriyet Daily News*, October 1, 2015, http://www.hurriyetdailynews.com/hurriyet-columnist-ahmet-hakan-injured-in-organized-assault.aspx?pageID=238&nID=89212&NewsCatID=509.

135 "Detainment Effort by Handcuffing Behind bianet eporter Beyza Kural," Bianet, November 6, 2015, http://bianet.org/english/media/169024-detainment-effort-by-handcuffing-behind-biane -reporter-beyza-kuralturkcel.

136 "In Turkey, technical attacks imperil digital media survival," International Press Institute, April 12, 2016, http://www.freemedia.at/in-turkey-technical-attacks-compromise-digital-media-sustainability/.

137 Efe Kerem Sözeri, "Turkish Internet hit with massive DDoS attack," *Today's Zaman*, December 17, 2015, http://www.dailydot.com/politics/turkey-ddos-attack-tk-universities/.

138 "Suspected cyber-attack hits Turkish banks, transactions," *Today's Zaman*, December 24, 2015, http://www.todayszaman.com/national_suspected-cyber-attack-hits-turkish-banks-transactions_407865.html.

139 Can Sezer "Turkey launches inquiry into leak of 50 million citizens' data," Reuters, April 6, 2016, http://www.reuters.com/article/us-turkey-cyber-idUSKCN0X31ZK.

Freedom House

United Arab Emirates

	2015	2016
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	14	14
Limits on Content (0-35)	22	22
Violations of User Rights (0-40)	32	32
TOTAL* (0-100)	**68**	**68**

* 0=most free, 100=least free

Population:	**9.2 million**
Internet Penetration 2015 (ITU):	**91 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- Authorities issued blocking orders against several overseas news websites over the past year, including *Middle East Eye*, *The New Arab*, and *al-Araby al-Jadeed* for unfavorable coverage of the country's human rights abuses. Two Iran-based news sites were also blocked in a reflection f mounting tensions between the two countries (see **Blocking and Filtering**).
- A July 2015 law designed to combat discrimination and hate speech also outlines jail terms of six months to over 10 years and fines f om US$ 14,000-550,000 for online posts deemed to insult "God, his prophets, apostles, holy books, houses of worship, or graveyards" (see **Legal Environment**).
- In June 2015, Nasser al-Faresi was sentenced to three years in jail for tweets found to have insulted the Federal Supreme Court and the ruler of Abu Dhabi. The court convicted him of "spreading rumors and information that harmed the country" (see **Prosecutions and Detentions for Online Activities**).
- Academic and activist Dr. Nasser Bin Ghaith was arrested and held incommunicado until April 2016, when it was announced he was held on numerous charges, including "committing a hostile act against a foreign state" for tweets that criticized Egypt's treatment of political detainees (see **Prosecutions and Detentions for Online Activities**).
- Leaked invoices from up until 2015 showed the government paid cybersecurity fi m Hacking Team over US$ 634,500 to deploy spyware on 1,100 devices (see **Surveillance, Privacy, and Anonymity**).

Introduction

Internet freedom remained highly restrictive in the United Arab Emirates over the past year, with prominent critics imprisoned for political tweets and ordinary users arrested in often absurd circumstances.

The country's information and communication technology (ICT) industry continues to grow, with the UAE now ranked third among Arab states in the ICT Development Index. However, the telecommunications industry remains tightly controlled by the government, which directly or indirectly owns large stakes in the country's two service providers. Close ties between the government and telecommunications companies may be a reason for consumer-unfriendly practices, such as restrictions on Voice-over-IP (VoIP), rampant censorship, and pervasive surveillance.

The state blocks access to political, social, or religious content that differs from the state's narrative, from pornography and gambling to political discussions and LGBT content. Self-censorship is pervasive on social media and state-run news sites generally refuse to cover controversial issues. Despite several laws that routinely violate the right of users to freely express themselves online, the families of political detainees often take to Twitter to highlight human rights abuses and communicate on behalf of their loved ones.

Just as with cybercrime and antiterrorism laws introduced in years' past, a July 2015 anti-hate speech law includes disproportionate penalties. Users face prison terms of up to 10 years and US$ 550,000 fines for crimes such as insulting eligious figu es, holy books, and prayer sites. Due to these broad laws and a judiciary that lacks independence, nonviolent opposition activists are sometimes targeted under laws designed for terrorists and cybercriminals. For example, activist and academic Nasser Bin Ghaith has been detained since August 2015 for, among other charges, "committing a hostile act against a foreign state" after tweeting about Egypt's unfair treatment of political detainees. Meanwhile, both locals and foreigners were arrested or deported for social media posts, often in absurd circumstances. Recent reports revealed how security services have targeted 1,100 devices with sophisticated spyware, reinforcing fears among dissidents that they are being watched.

Obstacles to Access

Emirati users enjoy a robust ICT infrastructure and high connection speeds. However, the major telecom companies are either fully or partially owned by state-owned, resulting in high prices, weak competition, and consumer unfriendly practices, such as the blocking of popular VoIP services.

Availability and Ease of Access

The United Arab Emirates (UAE) is one of the world's most connected countries. The number of internet users has risen rapidly from a penetration rate of 68 percent in 2010 to 91 percent at the end of 2015 according to the International Telecommunication Union. As of October 2015, there were 1,163,449 internet subscribers in the country, 99 percent of whom had broadband connections.[1] The UAE has one of the highest mobile phone penetration rates in the region at 187 percent, represent-

1 Telecommunications Regulatory Authority, "Latest Statistics," accessed Feb 10, 2016, http://www.tra.gov.ae/latest-statistics.html.

ing almost 18 million subscriptions at the end of 2015.[2] The country ranked 32nd in the 2015 Internet Development Index, up from 49th in 2010 and third among Arab States behind Bahrain and Qatar.[3]

While broadband use is widespread, the country has one of the most expensive broadband rates in the world, with high-end subscriptions costing more than AED 8,000 (US$2,178) a year. However, the UAE ranked 22nd in the ITU's 2014 ICT Price Basket Index, in which local broadband prices are measured against gross national income (GNI) per capita.[4] This reflects a sense that despi e the high prices, the internet remains affordable for most Emiratis, though not necessarily to the country's large population of expatriate workers.

On two recent occasions in September 2014 and April 2015, provider Etisalat upgraded broadband speed for 100,000 business clients.[5] In November 2015, broadband speeds were doubled for home customers at no extra charge.[6] In January 2016, provider Du announced upgraded internet speed for its home users.[7] In addition, the Emirates is set to be the fi st country to see a nation-wide rollout of the 5G network in time for the Expo 2020 exhibition.[8]

According to UNICEF, literacy in the Emirates was reported at 94 percent among males and 97 percent among females, and thus does not constitute a strong obstacle to internet use.[9] Emirati schools are now among the top 25 worldwide for online connectivity. There are over 200 smart-learning schools, compared with only 14 in 2012.[10] The program currently benefits 34,513 students, who a e also equipped with tablets as part of the scheme.[11] Principals are also enrolled in international computer literacy training programs.[12] By 2017, the country expects its Smart Learning Program to be installed in all K-12 government school classes, replacing textbooks with tablets and allowing students to interact with educators through an online platform.[13]

Restrictions on Connectivity

Most popular Voice-over-Internet-Protocol (VoIP) services are restricted over mobile connections. Etisalat and Du are the only two operators licensed to provide VoIP services, which are costlier than international alternatives. Snapchat's new voice and video calling feature was blocked upon its

2 International Telecommunication Union, "Percentage of individuals using the internet, Percentage of individuals with mobile-cellular subscriptions," 2015, http://bit.ly/1cblxxY.

3 International Telecommunications Union, *Measuring the Information Society Report 2015*, http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf.

4 International Telecommunications Union, *Measuring the Information Society Report 2014*, http://bit.ly/1FlOBfF.

5 "Etisalat freebie: 50% broadband speed boost," *Emirates 24/7*, April 18, 2015, http://bit.ly/1OEvJk2.

6 "Etisalat doubles broadband speeds for home customers for free," *Emirates 24/7*, November 16, 2015, http://www.emirates247.com/business/etisalat-doubles-broadband-speeds-for-home-customers-for-free-2015-11-16-1.610706.

7 "Dubai-based telco doubles broadband speed – for free," *Emirates 24/7*, January 19, 2016, http://www.emirates247.com/news/emirates/dubai-based-telco-doubles-broadband-speed-for-free-2016-01-19-1.617862.

8 "UAE set to become world's fi st nation to roll out 5G network," *Emirates 24/7*, October 21, 2015, http://www.emirates247.com/business/technology/uae-set-to-become-world-s-fi st-nation-to-roll-out-5g-network-2015-10-21-1.607562.

9 UNICEF, "United Arab Emirates: Statistics," December 31, 2013, accessed at June 25, 2013. http://uni.cf/lgxga0.

10 "UAE classrooms go from chalk board to smart board," *Khaleej Times*, February 22, 2016, http://www.khaleejtimes.com/nation/education/from-chalk-board-to-smart-board.

11 "Now,tablets to replace laptops in Dubai public schools," Khaleej Times. February 15, 2016, http://www.khaleejtimes.com/nation/education/10000-devices-to-be-given-under-smart-learning-programme.

12 "2013 a banner year in UAE education," *The National*, January 1, 2014, http://bit.ly/JBsX1i.

13 Roberta Pennington, "Smart Learning Programme transforms education in UAE's government schools," *The National*, January 13, 2014, http://bit.ly/1RcvDiz.

launch in April 2016.[14] Similarly, WhatsApp's voice feature was blocked shortly after it was introduced in March 2015.[15] Two months after that, Facebook's video-calling feature was also blocked.[16] Similar products such as Viber or Apple's Facetime have been banned since 2013;[17] in fact, Apple agreed to sell its iPhone products to UAE mobile phone companies without the Facetime application preinstalled.[18] Users in the UAE reported that Skype and Viber only work over Wi-Fi and Apple's Facetime video-calling feature can only be used if the iPhone was purchased outside the country.[19]

Despite these limitations, circumvention software and proxies are commonly used by Emiratis to access blocked content[20] and VoIP services.[21] Due to a UAE law that specifically criminalizes the use of VPNs in order to commit illegal activities, there have been fears that using VoIP services through VPNs could be punishable by law.[22]

There were no known government orders to shut down ICT connectivity over the coverage period. However, internet service providers (ISPs) in the UAE are either fully or partially owned by the state, allowing for authorities to exert control over the flow f information in the country. Seeking to improve connectivity within the country, the country's two internet service providers—Etisalat and Du—have launched their own carrier-neutral international internet exchange points, Smarthub and Datamena, respectively.[23] Etisalat maintains its nationwide fiber optic ackbone, while in May 2015 the company selected TeliaSonera International Carrier (TSIC) as its preferred global internet backbone provider under a framework deal.[24]

Cuts to undersea cables have disrupted internet access for Emirati users on several occasions, though government-instituted outages are not known. In January 2016, Du warned customers of slower internet due to cuts at three submarine cable operators – EIG, FEA and Falcon.[25]

ICT Market

Both Etisalat and Du are, directly or indirectly, owned by the state. The UAE government maintains a 60 percent stake in Etisalat through its ownership in the Emirates Investment Company,[26] while a majority of Du is owned by various state companies.[27] Du pays a percentage of its profit and evenue as a dividend to the UAE federal government, which owns 39.5 per cent of the telecom operator

14 Robert Anderson, "Snapchat Voice and Video Calling Blocked in UAE," *Gulf Business*, April 10, 2016, http://gulfbusiness.com/snapchat-voice-and-video-calling-blocked-in-uae/.

15 Vicky Kapur, "Still can't get free WhatsApp voice calls in UAE? This is why," *Emirates 24/7*, March 17, 2015, http://bit.ly/1VU9hUw.

16 Joseph George, "Facebook Messenger video calls blocked in UAE?" *Emirates 24/7*, May 21, 2015, http://bit.ly/1KbtMVG.

17 Dow Jones, "Viber seeks to circumvent ban in Middle East," *The National*, June 10, 2013, http://bit.ly/1LQ4unr.

18 Reporters Without Boarders, "Countries Under Surveillance: United Arab Emirates."

19 Etisalat Care, Twitter Post, April 21, 2014, 11:58 PM, http://bit.ly/1LmpBIK.

20 Stuart Turton, "Dubai's dubious internet "censorship"," *alphr*, September 6, 2010, http://bit.ly/1Pjil6g.

21 Triska Hamid, "Telecoms revenues threatened by Skype," *The National*, April 10, 2013, http://bit.ly/1G7E1Qi.

22 Haneen Dajani, "Use of VPN in the UAE still confusing despite recent law change," *The National*, August 9, 2016, http://www.thenational.ae/uae/government/use-of-vpn-in-the-uae-still-confusing-despite-recent-law-change.

23 "Etisalat launches internet exchange hub," *CommsMEA*, November 19, 2012, http://bit.ly/1hfcJEE.

24 "Etisalat selects TeliaSonera International Carrier as global internet backbone provider," *Telegeography*,March 11, 2015, http://bit.ly/1LOBrKN.

25 "Du says may take longer to repair damaged submarine cable," *Emirates 24/7*, January 26, 2016, http://www.emirates247.com/business/technology/du-says-may-take-longer-to-repair-damaged-submarine-cable-2016-01-26-1.618802.

26 Maher Chmaytelli, "Etisalat Plans to Allow Foreigners 'Soon,' Khaleej Says," *Bloomberg Business*, July 29, 2012, http://bloom.bg/1NJ7wdM.

27 du, "Shareholders structure," accessed June 7, 2013, http://www.du.ae/en/about/corporate-governance/shareholders.

through its sovereign wealth fund the Emirates Investment Authority.[28] In June 2015, the government announced a decision to allow up to 20 percent of Etisalat shares to be held by foreign investors.[29] The two companies are also the major mobile phone operators.

Regulatory Bodies

Providers fall under the laws and regulations set by the Telecommunications Regulatory Authority (TRA). The authority was established in 2003 and is responsible for the management of "every aspect of the telecommunications and information technology industries in the UAE." Its objectives include ensuring quality of service and adherence to terms of licenses by licensees, encouraging telecommunications and IT services within the UAE, resolving disputes between the licensed operators, establishing and implementing a regulatory and policy framework, and promoting new technologies.[30]

In March 2015, the TRA and Dubai police launched the "Digital Blackmail" campaign calling on users to report incidents of cybercrime and blackmailing, which are punished with up to ten years in jail. An official f om the Department of Cybercrime at Dubai Police said the police handled 1,820 cybercrimes in 2015, 239 more than 2014.[31] Following up from its "My Number, My Identity" campaign launched back in June 2012, the TRA called on users to "reregister their SIM cards before documents expire" to avoid cancellations. The authority said the move was "the result of studies that suggested an increase in civil and criminal cases related to the misuse of SIM cards."[32]

Limits on Content

Authorities keep strict control over the online media landscape, blocking websites that criticize the government or tackle social taboos. Self-censorship is pervasive on social media and state-run news sites refuse to cover controversial issues. Nonetheless, the families of political detainees often take to Twitter to highlight human rights abuses and communicate on behalf of their loved ones, at great risk to their safety.

Blocking and Filtering

Over the past year, the UAE blocked several overseas news websites for content that ran against the state's political narrative. The UK-based, English-language news site Middle East Eye was blocked in December 2015 after it published articles exposing the country's harsh surveillance practices and poor human rights record.[33] That same month, authorities blocked the Arabic-language news site *al-Araby al-Jadeed* and its English equivalent *The New Arab*, both based in the UK and funded by

28 Alexander Cornwell, "Du says royalty payments to federal government unlikely to change," Gulf News, February 9, 2016, http://gulfnews.com/business/economy/du-says-royalty-payments-to-federal-government-unlikely-to-change-1.1669331.

29 Rory Jones, "UAE to Allow Foreign Ownership of Etisalat Shares," *Wall Street Journal*, June 23, 2015, http://on.wsj.com/1LvnOo0.

30 Telecommunications Regulatory Authority, "Brief History," accessed Oct 1st, 2015, http://www.tra.gov.ae/brief-history.html.

31 "Police handle 1,820 cyber crime cases last year," Gulf News, February 6, 2016, http://gulfnews.com/news/uae/crime/police-handle-1-820-cyber-crime-cases-last-year-1.1666948.

32 "Re-register your SIM cards before documents expire," *Khaleej Times*, July 28, 2015, http://yhoo.it/1k6ZvT7.

33 "UAE Escalates its Crackdown on News Portal, Blocks Fars News Agency" ANHRI, July, 11, 2016 http://anhri.net/?p=169056&lang=en.

Qatar, although the sites were unblocked in February.[34] News agencies based in Iran, such as Fars News and Al Alam TV, had their Arabic-language sites blocked during the coverage period over allegations they disseminated antigovernment propaganda, according to the Arabic Network for Human Rights Information.[35]

The TRA instructs ISPs to block content related to terrorism, pornography, and gambling, as well as websites that contain political speech threatening to the ruling order. However, in reality, the UAE censors a wide variety of topics. Although YouTube, Facebook, Twitter, and international blog-hosting services are freely available, controversial terms are often fil ered from search results within these sites. According to Herdict, the crowdsourcing tool that lets users report blocked content, internet users from the UAE have reported several social, political, LGBTQ, dating, and proxy sites are blocked.[36] In December 2014, a website run by anonymous employees of Emirates airlines was reported to be blocked in the country.[37] The website of Beirut-based NGO Gulf Center for Human Rights was blocked in January 2015.[38] On Reddit, users reported the blocking of archive.today, a tool that keeps snapshots of URLs entered in case content disappears or gets modified [39] iHerb.com, an online retailer of nutritional supplements and wellness products, was reported to have been banned in June 2015.[40] Worldstar, a website for entertainment and media news, was reported blocked in November 2015,[41] as well as the Arabic entertainment website Akoam.[42] Twitter's livestreaming app Periscope was blocked for 48 hours in August 2015 reportedly due to a technical problem, according to a tweet by the TRA.[43]

Using the hashtag #blocked_sites_in_uae, blogger and human rights activist Ahmed Mansoor has asked users to help reveal which websites are being blocked. Users have reported the blocking of Twitter hashtags relating to political detainees,[44] as well as sites related to the Muslim Brotherhood and regional NGOs.[45] Arabic websites and political blogs such as Noonpost, Sasapost, Arabi21, and twsela.com were all reportedly blocked in 2015-16.[46] Skype's download page and online forum continued to be blocked during the coverage period, alongside several proxy websites. Earlier in 2015, the dating app Tinder was blocked.[47]

The Lebanese queer and feminist e-magazine *Bekhsoos*[48] and the U.S.-based Arab Lesbian e-magazine *Bint El Nas* are both blocked.[49] Many websites displaying religious content are blocked, includ-

34 "United Arab Emirates blocks The New Arab website," Al Araby, December 22, 2015, http://www.alaraby.co.uk/english/news/2015/12/29/united-arab-emirates-blocks-the-new-arab-website.

35 "UAE authorities block website of Alalam," Al Alam, October 26, 2015, http://www.alalam.ir/news/1753262.

36 Herdict, "Quick Stats: United Arab Emirates," accessed January 14, 2014, http://www.herdict.org/explore/indepth?fc=AE.

37 Blog no longer active: *Emirati Illuminati* (blog), http://www.emirates-illuminati.org/uae-blocks-emirates-illuminati/.

38 Gulf Center For Human Rights (GC4HR), "United Arab Emirates: GCHR website blocked in UAE," January 29, 2015, http://bit.ly/1hGc1as.

39 Reddit, "Archive.today blocked in UAE (United Arab Emirates," November 21, 2014, http://bit.ly/1VU6LTA.

40 Expat Woman Forum, "iHerb website blocked?!" Forum Thread, June 18, 2015, http://bit.ly/1LQiE8m.

41 See https://twitter.com/DJUCH/status/660862153184841728.

42 See https://www.facebook.com/photo.php?fbid=442553789284235.

43 Kevin Sebastian, "Twitter's livestreaming app, Periscope is not blocked in the UAE" AbsoluteGeeks.com, August 25, 2015, http://www.absolutegeeks.com/2015/08/25/periscope-livestreaming-not-blocked/.

44 Salloh, Twitter Post [in Arabic], May 5, 2015, 7:01 AM, http://bit.ly/1hGrqYg.

45 Twitter, Hashtag, #Blocked_sites_in_UAE, http://bit.ly/1RK5Q2a.

46 See: https://twitter.com/search?f=tweets&vertical=default&q=%23blocked_sites_in_uae%20&src=typd.

47 "Tinder app blocked by UAE's Etisalat," *Arabian Business*, January 19, 2015, http://bit.ly/1GeQuRG; "'Tinder-like': two expats launch new app for meeting people in the UAE," *Albawaba Business*, April 3, 2015, http://bit.ly/19Sp3hs.

48 *Bekhsoos Magazine*, http://www.bekhsoos.com/.

49 *Bin El Nas Magazine*, http://www.bintelnas.org.

ing an Arab-Christian online forum named The Church Network.[50] A number of secular and atheist websites and forums in Arabic continue to be blocked such as 3almani.org, secularkuwait.freeforums.org, nadyelfik .net, alawan.org, "Modern Discussion," [51] ladeenyon.net, and ladeeni.net.[52] The Emirati atheist blog of "Ben Kreishan" continues to be inaccessible in the UAE.

Authorities continue to ban inactive sites such as the political forum UAE Hewar and the blogs Secret Dubai Diary[53] and UAE Torture.[54] The latter had posted a torture video taken in 2004 in which a member of the ruling family was shown to have tortured an Afghan man. The suspect was acquitted in 2010 in a case that was widely believed to be a show trial.[55] A request to unblock UAE Hewar was rejected by the Federal Supreme Court in July 2012, [56] and its Facebook page is also blocked due to its criticism of the regime and state corruption.[57]

As part of a 2013 verdict in which fi e users were sentenced to 7 to 15 years on charges of violating the constitution and cooperating with foreign political organizations (see "Prosecutions and Detentions"), a court ordered the blocking of fi e websites: the Emirates Media and Studies Center (EMASC); the Seven Emirates, which focuses on the seven activists who had their citizenship revoked for their political activities; the California-based Arabic news site *Watan*; the Islah political group website; and the Yanabeea.net educational network.[58] In January 2016, *Watan* said the TRA has threatened to sue the company hosting its domain, referring to a "court order against the website."[59]

In 2013, a website disseminating news of the trial of 94 Emirati political detainees was also blocked.[60] The anonymous website UAE University Watch[61] and UAE Prison, which exposes violations against jailed expatriates, have both been blocked.[62] Emaraty Bedoon, the blog of the stateless individual Ahmed Abdulkhaleq who was deported to Thailand in July 2012 for his political activism, is also blocked.[63]

Pages of political significance, such as the Arab-American news ebsite *Arab Times* and the anonymous Secret Dubai blog continue to be blocked. In January 2014 alone, Twitter users have reported the blocking of ProxTube which unblocks censored YouTube content,[64] the chatting website Omelga, and the image-based social network We Heart It.[65]

The telecommunications company Du details what criteria it uses to block websites in a document available on its website. Prohibited content includes information related to circumvention tools, the

50 Arab Church, http://www.arabchurch.com/.

51 Modern Discussion, http://www.ahewar.org/.

52 "Help us document blocked Internet Sites in UAE," http://bit.ly/1e00dxW.

53 *Secret Dubai diary* (blog), http://secretdubai.blogspot.com/.

54 OpenNet Initiative, "United Arab Emirates," August 7, 2009, https://opennet.net/research/profiles/uni ed-arab-emirates.

55 Robert Mackey, "Abu Dhabi Royal Acquitted in Torture Trial," *The Lede* (blog), *New York Times,* January 11, 2010, http://nyti.ms/1ZFP1e1.

56 Human Rights Watch, "UAE: Investigate Threats against 'UAE 5'," November 25, 2011, http://bit.ly/1RcVXsR; Human Rights Watch, "UAE: Trial of Activists 'Fundamentally Unfair'," October 2, 2011, http://bit.ly/1GIzEWw.

57 Reporters Without Boarders, "Countries Under Surveillance: United Arab Emirates," March 11, 2011, http://bit.ly/1k7ek8a.

58 "68 members of Islah jailed for terrorism," [in Arabic] *AlShahed Newspaper*, July 3, 2013, http://bit.ly/1LQ3lfF.

59 Arabic "Emirates threatens hosting company to shut down website," *Watan*, January 27, 2016, http://bit.ly/2fiwt1 .

60 ANHRI, Facebook Post, April 18, 2013, https://www.facebook.com/AnhriHr/posts/506587829404624.

61 UAE University Watch, http://www.uaeuniversitywatch.net/.

62 http://uaeprison.com.

63 *Emaraty Bedoon* (blog), http://www.emaratybedoon.blogspot.com/.

64 Dr. Cool, Twitter Post, January 11, 2014, 10:12 PM, http://bit.ly/1RK8nJx.

65 Romina Chiara Torres, Twitter Post, January 14, 2014, 12:29 AM, http://bit.ly/1Lc8B9X.

promotion of criminal activities, the sale or promotion of illegal drugs, dating networks, pornography, homosexuality, gambling, phishing, spyware, unlicensed VoIP services, terrorism, and material that is offensive to religion.[66] No similar list was made available by Etisalat, although the company does have a space on its website where users can request that a website be blocked or unblocked.[67] In 2005, an Etisalat spokesman clarified that the com any is not responsible for internet blocking and revealed that all complaints and requests are passed on to the Ministry of Information. He also claimed that a list of websites to be blocked is compiled by an American company and then implemented through a proxy server.[68] According to a report from Citizen Lab in January 2013, ISPs in the UAE have used tools such as SmartFilter and NetSweeper to censor content. Citizen Lab also found fi e installations of Blue Coat ProxySG in the country's network linked to Etisalat.[69] Another report from CitizenLab in November 2013 listed websites that are blocked in the UAE because both SmartFilter (used by Etisalat) and NetSweeper (used by Du) have miscategorized them as nudity or pornographic content.[70]

When Twitter users have complained about a site being wrongfully blocked, Etisalat and Du responded by asking users to complete an unblocking request via online forms. However, neither provide information on whether bans have been lifted in response to such requests.[71] In May 2015, Twitter users reported the blocking and later unblocking of the social platform Wattpad.[72] Similarly, Emirati columnist Sultan al-Qassemi noted the unblocking of the news website The New Arab in February.[73] The TRA has also called on users to help report "suspicious" content for blocking.

The TRA, working with the Ministry of Communications, blocks at least fi e hundred search terms.[74] The TRA claimed the number of blocked websites is unknown "due to the nature of blocking operations".[75] In a previous statement, TRA stated that 82 percent of the websites blocked during the period from January to March 2015 were blocked for nudity and dating content, 8 percent for violating UAE laws, and 9 percent for containing phishing, hacking, and spyware content.[76]

Content Removal

The removal of online content often lacks procedural transparency or judicial oversight. Under the 2012 cybercrime law, website owners and employees "may be held liable" for any violations occurring on their sites, including defamation charges.[77] An official f om the TRA stated in 2015, "We try

66 Du, "Prohibited Content Categories," July 29, 2008, http://bit.ly/1LmaBKL

67 Etisalat, "Blocking and Unblocking Internet Content," accessed on April 28, 2013, http://bit.ly/1Lc6l2u.

68 Piers Grimley Evans, "Etisalat doesn't block websites," *Gulf News*, July 21, 2005, http://bit.ly/1Lc6piU.

69 Greg Wiseman et. al., "Appendix A: Summary Analysis of Blue Coat 'Countries of Interest'," CitizenLab, January 15, 2013, http://bit.ly/1ZFRSna.

70 Bennett Haselton, "Smartfil er: Miscategorization and Filtering in Saudi Arabia and UAE," CitizenLab, Novermber 28, 2013, http://bit.ly/1P1PLas.

71 See Etisalat_Care, Twitter Post, December 30, 2015, 5:52 AM, http://bit.ly/1LmlQD2; and https://twitter.com/dutweets/status/414787641620430848Evans [offline

72 See https://twitter.com/MayraRahab/status/596619001272209408.

73 See https://twitter.com/SultanAlQassemi/status/704050010003021828.

74 Reporters Borders, "Countries Under Surveillance: United Arab Emirates," accessed in June 25, 2013, http://bit.ly/1LvCJyw.

75 "TRA calls on users to report content," *Emarat alYoum*, January 29, 2015. http://www.emaratalyoum.com/business/local/2016-01-29-1.864215.

76 Telecommunications Regulatory Authority, http://www.tra.gov.ae/iam.html.

77 Awad Mustafa, "Cyber-crime law to fight in ernet abuse and protect privacy in the UAE," *The National,* November 13, 2012, http://bit.ly/1VUaATh.

to get the page or profile down or emove the violation as soon as possible and report the case to police if it is a criminal case."[78]

According to Google's Transparency Report for the second half of 2015, the company received a request from the TRA to remove a YouTube video showing an Emirati royal family member torturing Sudanese workers at his farm.[79] The company did not remove the video out of respect for the public interest. In 2014, Google had reported two requests from the UAE to remove Google+ posts that violated the 2012 cybercrime law. The posts were blocked locally because they "contained obscene language and political satire against members of the ruling family of the UAE."[80]

Twitter received one removal request from the UAE over the coverage period and did not withhold any content in response.[81] In November 2015, Dubai Authorities reported the termination of 202 Instagram accounts and 218 websites "for selling and promoting fake products."[82]

Media, Diversity, and Content Manipulation

In addition blocking and content removal, Emirati authorities also use financial means o limit the ability of antigovernment websites to produce content online. For example, the government reportedly pressured Dubai-based advertising agency Echo to end its advertising contract with the U.S.-based news outlet *Watan*. A complaint was also allegedly submitted to the FBI against the website, claiming it calls for the assassination of UAE rulers.[83] Nonetheless, users have access to a variety of local and international news outlets, even if there are disparate reports of the blocking of specific UAE-related articles from these sites.[84]

Local news websites, many of which are owned by the state, employ a large degree of self-censorship in accordance with government regulations and unofficial " ed lines." *Gulf News*, *The National*, and *Emirates 24/7* are among the different online media outlets facing restrictions. The overall press freedom environment in traditional media is dire, with foreign journalists and scholars often denied entry or deported for expressing their views on political topics.[85] In February 2016, the Federal National Council passed a bill regulating responsibilities of the new National Media Council, a federal government body affilia ed with the cabinet that "has a corporate character and a mandate to undertake the responsibilities of overseeing and supervising media in the UAE." The council will

78 "UAE in crackdown on social media abuse," *Arabian Business*, March 10, 2015, http://bit.ly/1FKCiuW.

79 Google, "United Arab Emirates," in *Transparency Report,* July to December 2015. https://www.google.com/transparencyreport/removals/government/notes/?hl=en#authority=AE

80 Google, "United Arab Emirates," in *Transparency Report,* January-June 2014, http://bit.ly/1OEYHQE.

81 Twitter's Transparency Report is available at https://transparency.twitter.com/en/removal-requests.html#removal-requests-jan-jun-2016.

82 "Dubai shuts down 202 Instagram accounts for promoting fake goods," *Emirates 24/7*, November 4, 2015, http://www.emirates247.com/news/emirates/dubai-shuts-down-202-instagram-accounts-for-promoting-fake-goods-2015-11-04-1.609242.

83 ANHRI. "UAE Continues its Serious Violations Against the Freedom of Opinion and Expression due to Blocking "Watan" Website," September 24, 2012, http://bit.ly/1GIvcH8.

84 ECHRigts, Twitter Post, July 31, 2012, 9:10 AM, http://bit.ly/1RKb5Pf.

85 See for example, "Egyptian journalist freed from UAE detention," *Aljazeera*, August 4, 2013, http://bit.ly/1PjjQ4o; "Palestinian journalist detained at a secret prison in the UAE," *Middle East Monitor*, December 4, 2013, http://bit.ly/1QwYlL7, Hrag Vartanian, "Artist Walid Raad Denied Entry into UAE, Becoming Third Gulf Labor Member Turned Away," *Hyperallergic*, May 14, 2015, http://bit.ly/1ME91Z3, and Migrant-Rights, "UAE Censors Author of Book Criticizing Migrant, Race Issues," June 17, 2014, http://bit.ly/1Oxn2JH.

be responsible for proposing regulations and "accrediting media outlets and their staff and activities including e-publishing."[86]

Nonetheless, since the regional uprisings of 2011, Emiratis have begun to tackle sensitive issues more boldly over the internet, particularly on social media. Users express their opinions, share information on arrests and trials, and even attempt to organize protests. However, most users remain anonymous when criticizing state officials or eligion out of fear of legal action or harassment. In 2014, The United Arab Emirates spent more than $12 million on public relation fi ms, which some observers suspect have been deployed to counter negative images of the country's human rights abuses online.[87] A large number of anonymous Twitter users appear dedicated to harassing and intimidating political dissidents and their families online.

Digital Activism

Some Emiratis have continued to push back against government repression and intimidation by channeling their strong digital literacy into online activism, writing blogs, and calling for political reform on social networks. In the face of prosecution, activists still use online tools to highlight human rights violations and pass on messages from relatives in prison. Families of political prisoners still rely on Twitter to speak on behalf of detainees, explaining their cases, spreading information about violations of their rights, and calling for their release. There are several examples of relatives who are active online, including Mariam al-Mansouri,[88] the wife of detained blogger Rashid al-Shamsi, and Aysha al-Thufiri, the daugh er of detainee Salih al-Thufiri [89] Nonetheless, the online environment in the UAE is not free, and users face many challenges to freedom of expression online. For instance, three sisters were secretly detained for three months for tweets calling for the release of their detained brother Issa al-Suwaidi.[90]

Violations of User Rights

Several laws, including the penal code, the publishing law, and the cybercrime law, are commonly exploited to deter free expression and violate the rights of users. Several prominent online activists were jailed over the coverage period, while both locals and foreigners were targeted for social media posts, often in absurd circumstances. Finally, there is a general feeling among those who reside in the UAE that online tools are monitored and that surveillance is widely practiced with little judicial oversight.

Legal Environment

Article 30 of the UAE constitution states that "Freedom of opinion and expressing it verbally, in writing or by other means of expression shall be guaranteed within the limits of law."[91] However, the Emi-

86 "UAE's FNC passes bill on Media Council," *Emirates 24/7*, February 17, 2016, http://www.emirates247.com/news/uae-s-fnc-passes-bill-on-media-council-2016-02-17-1.621241.

87 Akbar Shahid Ahmed. "How Wealthy Arab Gulf States Shape The Washington Influence Game" *Huffington Post*, February 9, 2015, http://www.huffing onpost.com/entry/arab-gulf-states-washington_us_55e62be5e4b0b7a9633ac659.

88 Marian Mansori, Twitter Account, https://twitter.com/MariamMansori.

89 Aysha_75, Twitter Account, https://twitter.com/Aysha_75.

90 Amnesty International, "UAE: Three sisters released after three months in secret detention for tweeting," May 15, 2015, http://bit.ly/1PvghYe.

91 "Constitution of the United Arab Emirates," Refworld, accessed August 1, 2013, http://bit.ly/1k7kUvC.

rati judicial system lacks independence, and prosecutions are often pursued for political reasons.[92] Since the 2011 uprisings throughout the region, the countries making up the Gulf Cooperation Council made a collective effort to pass legislation criminalizing criticism of the authorities.[93]

Several legislative amendments further restricted free speech, particularly on sensitive topics such as religion. Citing the need to curb hateful rhetorical and promote tolerance in order to defend against terrorism, authorities passed Federal Decree Law No. 2/2015 in July 2015. However, several provisions in the law go beyond the punishment of hate speech or incitement to violence. By including insults to "God, his prophets or apostles or holy books or houses of worship or graveyards," the law paved the way for further punishment of individuals for expressing nonviolent opinions on religion. Penalties under the law range from jail terms of 6 months to 10 years and/or fines f AED 50,000 to 2,000,000 (approximately US$ 14,000 to 550,000).[94] Furthermore, while the law's scope bans discrimination on the basis of "religion, caste, doctrine, race, color, or ethnic origin," it does not protect those persecuted on the basis of gender or sexuality.[95] The law specifically includes speech made o er online media.

Amendments to the cybercrime law were proposed this February[96] and later passed July 2016 as Federal Law No. 12/2016.[97] The act of using "a fraudulent computer network protocol address" in order to "commit a crime or prevent its discovery" was raised from a misdemeanor to a crime now punishable by temporary imprisonment, and fines ere raised from AED 150,000–500,000 to AED 500,000–2,000,000. While the cybercrime law provided a sounder legal basis to combat online fraud, money laundering, hacking, and other serious cybercrimes, the law also criminalized a wide range of online activity commonly accepted within international norms. For example, hefty fines and jail sentences await users who engage in online gambling, disseminate pornographic material, or violate another person's privacy through posting their photograph or making statements about them online, regardless of the accuracy of the accusations. Intermediaries, such as domain hosts or administrators, are also liable if their websites are used to "prompt riot, hatred, racism, sectarianism, or damage the national unity or social peace or prejudice the public order and public morals."[98] The cybercrime law also contains punishments for offending the state, its rulers, and its symbols, or for insulting Islam and other religions. Calls to change the ruling system are punishable by life imprisonment. Authorities have repeatedly warned foreign nationals that they must also follow the country's restrictive laws.[99]

The Terrorism Law No. 7, passed in 2014, includes punishments such as life imprisonment, death, and fines up o AED 100 million (US$27 million) for terrorism offenses.[100] Under the law, citizens may be

92 Human Rights Watch, "UAE: Investigate Threats against 'UAE 5'," November 25, 2011, http://bit.ly/1ZFUdyh.

93 Human Rights Watch, "GCC/US: Obama Should Press Gulf Rulers," May 12, 2015, http://bit.ly/1IO8K2l.

94 "UAE Anti-discriminatory Law bans hate speech, promotion of violence," *Emirates 24/7*, July 22, 2015, http://www.emirates247.com/news/government/uae-anti-discriminatory-law-bans-hate-speech-promotion-of-violence-2015-07-22-1.597389.

95 See Human Rights Watch, "United Arab Emirates," World Report 2016, https://www.hrw.org/world-report/2016/country-chapters/united-arab-emirates, and Amnesty International, "United Arab Emirates 2015/2016," Annual Report, https://www.amnesty.org/en/countries/middle-east-and-north-africa/united-arab-emirates/report-united-arab-emirates/.

96 Haneen Dajani, "FNC mulls tougher cybercrime laws and increased legal fees," *The National*, February 14, 2016. http://www.thenational.ae/uae/fnc-mulls-tougher-cybercrime-laws-and-increased-legal-fees.

97 "UAE federal laws tackle media governance, cybercrime" *Khaleej Times*, July 23, 2016, http://www.khaleejtimes.com/UAE-federal-laws-NMC-media-governance-cybercrime.

98 See Federal Decree-Law no. (5) of 2012 on Combating Cybercrimes, August 13, 2012, http://bit.ly/1gDnVCj.

99 "New UAE cyber crime laws: Jail for indecent posts," *Emirates 24/7*, November 14, 2012, http://bit.ly/1EPrBtK.

100 AFP, "UAE toughens anti-terrorism laws," *Al Arabiya,* August 21 2014, http://ara.tv/j8cc4.

charged with such broad crimes as undermining national unity, possessing materials counter to the state's notion of Islam, and "publicly declaring one's animosity or lack of allegiance to the state or the regime."[101]

Articles 8 and 176 of the penal code are used to punish public "insults" against the country's top officials, although these a ticles are also widely used to prosecute any users that express a desire for political reform.[102] Articles 70 and 71 of the 1980 publishing law prohibit criticism of the head of the state and of Islam or any other religion.[103] In February 2016, Dubai police reiterated that posting pictures of others without permission can lead to six months in jail and a fine bet een AED 150,000 and 500,000 (USD 41,000 and 136,000).[104]

Several court decisions over the past year negatively impacted internet freedom. In June 2015, the Federal Supreme Court ordered the retrial of an individual for making insults over WhatsApp messages, increasing the original fine f AED 3,000 (around US$ 800) to AED 250,000 (US$ 68,000), as well as ordering his/her deportation.[105] Later, in December 2015, Dubai's Court of Cassation overturned a lower court's acquittal in a defamation case over a Facebook posting. The lower court had acquitted the defendant based on the fact that his post was in a private Facebook group that was not accessible to the general public. However, the prosecutor successfully appealed the verdict, arguing that "even if the Facebook page is not accessible to general public, posting derogatory comments defames a person and damages his or her reputation."[106] The defendant, who is accused of insulting a woman on Facebook, will now have his case reheard by a new panel of judges.[107]

Prosecutions and Detentions for Online Activities

The UAE routinely jails individuals for posting political, social, or religious opinions online. Numerous incidents were witnessed over the coverage period, while several individuals remain behind bars from lengthy prison sentences past in previous years.

Several Emiratis were sentenced to prison over the coverage period for criticizing state institutions:

- In August 2015, Dr. Nasser Bin Ghaith was arrested and held in arbitrary detention until April 2016, when it was announced he was held on numerous charges, including "committing a hostile act against a foreign state" for tweets that criticized the Egyptian judiciary's treatment of political detainees.[108] Bin Ghaith, who remained in detention as of late 2016, is a human rights activist and former lecturer at the Abu Dhabi branch of the Paris-Sorbonne

101 Human Rights Watch, "UAE: Terrorism Law Threatens Lives, Liberty," December 3, 2014, http://bit.ly/1NdV6st.

102 Human Rights Watch, "UAE: Free Speech Under Attack," January 25, 2012, http://bit.ly/1k7mjSI.

103 Federal Law No. 15 of 1980 Governing Publications and Publishing, http://bit.ly/1VUyHGE.

104 "Fines and jail for posting pictures of others without permission," *al-Bawaba*, February 25, 2016, http://bit.ly/2exHKJI.

105 "New UAE Online Law: Dh250,000 fine for s earing on WhatsApp," Emirates 24/7, June 16, 2015, http://bit.ly/1MHqpJv, and "UAE man faces $68,000 fine for s earing on WhatsApp," BBC News, June 16, 2015, http://www.bbc.com/news/world-middle-east-33152898.

106 Marie Nammour, "Man's acquittal over FB post reversed," *Khaleej Times*, December 8, 2015. http://www.khaleejtimes.com/nation/crime/mans-acquittal-over-fb-post-reversed.

107 Ryan Stultz, "Dubai court rules even 'private' Facebook posts subject to prosecution," Stepfeed.com, December 8, 2015, http://stepfeed.com/more-categories/big-news/dubai-court-rules-even-private-facebook-posts-subject-prosecution/#.V7kYkZMrLBJ.

108 "Free Emirati human rights defender Dr. Nasser Bin Ghaith, on trial for online posts in violation of his right to free expression," Gulf Center for Human Rights, June 1, 2016, http://www.gc4hr.org/news/view/1260.

University.[109] He was previously arrested in 2011 for signing an online petition demanding political reform.[110] His trial has been repeatedly adjourned and he states he was tortured while in detention, for which authorities have also charged him with damaging the reputation of the UAE. [111]

- In June 2015, Nasser al-Faresi was sentenced to three years in jail for a tweet insulting the Federal Supreme Court and the ruler of Abu Dhabi. The court charged him with "spreading rumors and information that harmed the country."[112]

Several foreigners were also targeted for social media posts under the country's harsh cybercrime laws:

- Jodi Magi, an Australian national, was fined AED 10,000 (US$2,700) and depo ted in July 2015 after posting a picture to Facebook showing her neighbor's vehicle parked across two parking spaces reserved for the disabled.[113] Magi was found to have violated the cybercrime law by taking photos without the consent of the vehicle's owner as well as using offensive remarks against the owner.[114]

- In January 2016, the Federal Supreme Court sentenced a Palestinian man to three years in jail and a fine f AED 50,000 (US$ 13,500) for "insulting the UAE on social media." The man, who pleaded not guilty, told the judge the incident in question was a private interaction with another Facebook user.[115]

- In March 2016, an Omani man was sentenced to three years in jail and fine f AED 50,000 (US$ 13,500) for describing UAE soldiers killed in Yemen as "cowards" over WhatsApp messages. He will be deported after serving his sentence.[116]

Other cases from the coverage period include:

- In March 2016, Marwan Mohamed Ateej was sentenced to fi e years imprisonment and a fine f AED 1,000,000 (US$ 272,000) for online posts in support of the Muslim Brotherhood. Court documents claimed he "legitimised [sic] the work of the Muslim Brotherhood calling them peaceful, unarmed heroes and rallied on people to support them."[117]

- In June 2016, the Abu Dhabi Court sentenced an expat man to six months in jail and an AED

109 Naser al Remeithi, "Former university lecturer appears in court accused of inciting hatred in UAE," The National, May 2, 2016, http://www.thenational.ae/uae/courts/former-university-lecturer-appears-in-court-accused-of-inciting-hatred-in-uae.

110 "Emirates arrests Nasser Bin Ghaith," Al Bawaba, August 19, 2015. http://bit.ly/2ed2k7c.

111 "UAE: Human rights defender Dr. Nasser Bin Ghaith remains in prison as trial continues," Gulf Center for Human Rights, June 23, 2016, http://www.gc4hr.org/news/view/1295.

112 Reuters, "UAE man jailed for tweets critical of high court: newspaper," *Yahoo! News,* June 30, 2015, http://yhoo.it/1VUf0cJ.

113 "Australian woman deported from UAE after Facebook post," *Aljazeera*, July 15, 2015, http://bit.ly/1M5Y9Ck.

114 Haneen Dajani, "Tough UAE social media law could see expats deported for saving someone's photo," *The National*, July 19, 2015, http://bit.ly/1L9kTT1.

115 Naser Al Remeithi, "Man who insulted UAE on social media gets three-year jail term," *The National*, January 10, 2016, http://www.thenational.ae/uae/man-who-insulted-uae-on-social-media-gets-three-year-jail-term.

116 "Man jailed for insulting UAE on WhatsApp," *Arabian Business*, March 1, 2016, http://www.arabianbusiness.com/man-jailed-for-insulting-uae-on-whatsapp-623405.html#.V7k0RJMrLBL.

117 Naser al Remeithi, "Man jailed for fi e years for supporting Muslim Brotherhood," *The National*, March 27, 2016, http://www.thenational.ae/uae/courts/man-jailed-for-fi e-years-for-supporting-muslim-brotherhood.

50,000 (US $13,500) fine for upl ading torrents to a pirate streaming website. He will also be deported after serving his sentence.[118]

- In April 2016, an Emirati woman was tried for insulting her maternal uncle and his religious sect over WhatsApp. The woman pleaded guilty and, under the antidiscrimination law, could face a minimum fi e years in jail and/or a fine that ranges bet een AED 500,000–1,000,000 (US$ 135,000–272,000).[119]

- In January 2016, two men were briefly ar ested and questioned for posting a selfie in f ont of a Dubai hotel which had caught fi e.[120]

- In January 2016, two Emirati soldiers were arrested after a video of them performing a Saudi hip-hop dance went viral. The two were charged with disrespecting the UAE army and its uniform.[121]

Numerous Emirati users continue to serve long prison sentences for their online activities, mainly related to the UAE94 trials directed against alleged members of the banned opposition movement al-Islah. [122]

- Blogger Khalifa Al-Nuaimi[123] and Twitter users Rashid al-Shamsi[124] and Musabeh al-Rumaithy[125] were arrested for their online activities and sentenced to 10 years imprisonment in July 2013.

- Blogger Abdullah al-Hajri[126] and Twitter user Omran al-Radhwan[127] are serving seven-year sentences.[128]

- In November 2014, online activist Osama Al-Najjar was sentenced to three years in prison and fined US$136,000 for t eets alleging that his father, who was imprisoned as part of the UAE94 trials, was tortured by security forces. [129] He was found guilty of belonging to

118 "UAE court jails man for uploading torrents," *Emirates 24/7*, June 28, 2016, http://www.emirates247.com/news/emirates/uae-court-jails-man-for-uploading-torrents-2016-06-28-1.634340.

119 "Teacher accused of inciting sectarian strife on WhatsApp," *Gulf News*, April 10, 2016, http://gulfnews.com/news/uae/courts/teacher-accused-of-inciting-sectarian-strife-on-whatsapp-1.1707820#.VwwNE11bngM.twitter.

120 "Dubai police releases the selfie men" *al-Bawabha News*, January 9, 2016, http://www.albawabhnews.com/1707532.

121 Sudarsan Raghavan, "This Saudi dance is all the rage in Arab world, but it could get you arrested," *The Washington Post,* April 11, 2016, https://www.washingtonpost.com/news/worldviews/wp/2016/04/11/this-saudi-dance-is-all-the-rage-in-arab-world-but-it-could-get-you-arrested/.

122 Emirates Centre for Human Rights (ECHR), "Current political prisoners," accessed March 18, 2014, http://www.echr.org.uk/?page_id=207.

123 Al-Nuaimi had previously written about "the UAE 5" and had been consistently threatened prior to his arrest: "الدرغام (بوصمصبح) .. يكشف عن التنظيم قبل 35 يوم !!" *Kalnuaimi* (blog), July 15, 2012, http://bit.ly/1jqEuCW.

124 Al-Shamsi had tweeted news of arrests and written blog posts related to politics and free speech. See *Rashed Al Shamsi* (blog), http://bit.ly/1hGA88O.

125 al-Rumaithy was arrested for his online writings in which he expressed support for the Islamist Islah party. He had been handed a travel ban one month before his arrest. See GC4HR, "UAE- Travel bans imposed against human rights activists as restriction on freedom of movement increases," July 1, 2012, http://www.gc4hr.org/news/view/187.

126 Al-Hajri was arrested over the contents of his blog, http://alhajria.wordpress.com, in which he called for more government action to combat public immorality.

127 Al-Radhwan had tweeted about "the UAE 5" detainees and wrote several posts on his website, http://omran83.tumblr.com, promoting Islah and criticizing state violations of Shariah law.

128 Amnesty International, "UAE: Grossly unfair trial of government critics," July 2, 2013, http://bit.ly/1X6DVMP.

129 GC4HR, *Hear their Voices: Alarming Times for Human Rights Defenders in the Gulf Region & Neighboring Countries,* February 2015, http://bit.ly/1GIwKkA.

the banned political group al-Islah, spreading lies, and instigating hatred against the state through Twitter.[130]

- Abdulrahman Bajubair was sentenced to fi e years in jail for running a blog and Twitter accounts reporting on the mistreatment of political detainees in December 2013.[131]
- In March 2014, Khalifa Rabeiah and Othman al-Shehhi were fined and a e currently serving a fi e-year sentence for tweets critical of the judiciary system.[132]

Surveillance, Privacy, and Anonymity

The high amount of prosecutions and physical harassment of users in the UAE is, in part, due to the obstacles they face in using ICT tools anonymously. Emirati activists have consistently faced spyware attacks. In May 2016, a report from the *New York Times* stated the UAE government paid the cybersecurity fi m "Hacking Team" more than $634,500 to target 1,100 devices with spyware able to track their owners' activities.[133] Through a forensic investigation by cybersecurity expert Bill Marczak, Emirati human rights activist Ahmed Mansoor discovered he had been repeatedly targeted with sophisticated spyware from FinFisher and Hacking Team. A May 2016 report by CitizenLab demonstrated fi e cases where arrests or convictions of users followed malware attacks against their Twitter accounts from 2012 to 2015.[134]

Internet and mobile providers are not transparent about the procedures taken by authorities to access their data and users' information. Incidents of providers demanding warrants or legal permissions for security bodies to gain access to user data are not known. In February 2016, an official from Dubai police said the country monitors users on 42 social media platforms.[135] Ghaith Al Mazaina, acting manager at the security quality service at the TRA, stated: "We have started monitoring all the social media channels – all websites and profiles a e monitored."[136]

Cybercafe customers are also required to provide their ID and personal information.[137] In April 2014, the Ministry of Interior announced plans to link ID cards with internet services and cellphones "to crackdown on child abusers." An official sta ed "by linking ID cards with internet service providers, people's identities will be linked to the websites they visit."[138] In March 2015, the TRA announced the establishment of an alert system that detects certain keywords relating to "nudity, sexual cyber-extortion and insulting members of the ruling families." Mobile phone users re-registered their per-

130 Gulf Center for Human Rights, *Torture and Abuse in Prisons in the United Arab Emirates,* March 5, 2015, http://bit.ly/1OF61f5; Human Rights Watch, "UAE: Terrorism Law Threatens Lives, Liberty," December 3, 2014, http://bit.ly/1NdV6st.

131 Reporters Without Borders, "United Arab Emirates: Tracking "cyber-criminals"," March 11, 2014, http://bit.ly/1OF6kXh.

132 "Digital Citizen 1.5," *Global Voices,* April 1, 2014, https://advocacy.globalvoicesonline.org/2014/04/01/digital-citizen-1-5/.

133 Nicole Perlroth. "Governments Turn to Commercial Spyware to Intimidate Dissidents" *New York Times,* May 29, 2016, http://www.nytimes.com/2016/05/30/technology/governments-turn-to-commercial-spyware-to-intimidate-dissidents.html?_r=0.

134 Bill Marczak, John Scott-Railton, "Keep Calm and (Don't) Enable Macros: A New Threat Actor Targets UAE Dissidents," Citizen Lab, May 29, 2016, https://citizenlab.org/2016/05/stealth-falcon/.

135 "Emirates operate online police to monitor users," Cairo Portal, Feb 24, 2016, http://bit.ly/2ebBVlh.

136 "UAE in crackdown on social media abuse," *Arabian Business*, March 10, 2015, http://bit.ly/1FKCiuW.

137 Morgan Marquis-Boire, et. al., *Planet Blue Coat: Mapping Global Censorship and Surveillance Tools*, Citizen Lab, January 15, 2013, http://bit.ly/1d0bWVr.

138 Caline Malek, "UAE ministry to link ID cards with the internet to crack down on child abusers," *The National*, April 5, 2014, http://bit.ly/1LPc4J0.

sonal information as part of a 2012 TRA campaign "My Number, My Identity."[139] In January 2013, the country's two mobile phone providers issued a final wa ning to their users to register their SIM cards or have their lines cut.[140]

Intimidation and Violence

Online activists in the UAE face arbitrary detention, enforced disappearances, and in some cases torture.[141] In December 2015, Jordanian journalist Taysir al-Najar was detained at the airport before leaving to Jordan for a family visit. As of mid-2016, al-Najar remained in arbitrary detention for a 2014 Facebook comment critical of the authorities. For two months, his family did not know his whereabouts.[142] Omani blogger Muawiyah Alrawahi was arrested as he entered the country by car and held in arbitrary detention for 13 months. He has a vocal critical of both Omani and UAE authorities online.[143] Human rights defender Ahmed Mansoor has faced continual harassment by the authorities, and is subject to a travel ban.[144]

Technical Attacks

The UAE remains one of the top countries facing hacking attempts worldwide. According to a 2015 study by Kaspersky Lab, the UAE is the second most attacked country online in the Middle East and the 15th most attacked worldwide.[145] In January 2016, two foreign men were each sentenced to one year in prison and fined AED 500,000 (US$ 135,000) for hacking in o the computer system of a support services company. The duo were found to have divulged secret information to the company's competitors.[146] In July 2015, several UAE banks were hit by a coordinated cyberattack crippling e-banking operations and websites.[147] That same month, the cybersecurity company Symantec uncovered a new corporate espionage group that has compromised a string of major corporations in recent years, including three organizations located or headquartered in the UAE.[148]

139 The TRA's statement reads: "Your mobile phone number is an extension of your identity. Sharing or giving away your SIM-Card to others can cause unwanted consequences, including being held accountable for any improper conduct or misuse associated with the mobile phone subscription by the authorities as well as being liable for all charges by the licensees." Telecommunications Regulatory Authority, "My Number My Identity," accessed April 28, 2013, http://bit.ly/1LPbs66; and Nadeem Hanif, "Every mobile phone user in the UAE must re-register SIM card," *The National,* June 28, 2012, http://bit.ly/1k7pFoY.

140 Nadeem Hanif, "Du and Etisalat brace for UAE users last chance to re-register Sim card," *The National,* January 16, 2013, http://bit.ly/1GeZoig.

141 Human Rights Watch, "United Arab Emirates," World Report 2016, https://www.hrw.org/world-report/2016/country-chapters/united-arab-emirates.

142 "Jordanian journalist arrested at Dubai airport," *Albosala*, January 22, 2016, http://bit.ly/2fN8trs.

143 "Omani bloggers returns home after his release from UAE prison" *Watan*, March 19, 2016. http://bit.ly/2fiuPw .

144 GC4HR, *Hear their Voices: Alarming Times for Human Rights Defenders in the Gulf Region & Neighboring Countries.*

145 Helen Gaskell, "UAE is top-two victim of regional cyber attacks," *Arabian Business*, March 22, 2015, http://bit.ly/1EJaRC1.

146 Bassam Za'za', "Duo fined Dh500,000 each for digital fraud" *Gulf News*, January 28, 2016, http://gulfnews.com/news/uae/courts/duo-fined-dh500-000-each-fo -digital-fraud-1.1661968.

147 Stephen McBride, "Anonymous cyber hackers hit UAE banking websites," *Arabian Business*, July 2, 2015, http://www.arabianbusiness.com/anonymous-cyber-hackers-hit-uae-banking-websites-598214.html.

148 Stephen McBride, "Three UAE fi ms targeted by 'sophisticated' cyber-bandits," *Arabian Business*, July 12, 2015, http://bit.ly/1LQge9G.

Freedom House

Uganda

	2015	2016
Internet Freedom Status	Partly Free	Partly Free
Obstacles to Access (0-25)	11	13
Limits on Content (0-35)	7	11
Violations of User Rights (0-40)	18	18
TOTAL* (0-100)	**36**	**42**

* 0=most free, 100=least free

Population:	**39 million**
Internet Penetration 2015 (ITU):	**19 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Partly Free**

Key Developments: June 2015 – May 2016

- Access to Facebook, Twitter, WhatsApp, and mobile money services were blocked ahead of the February 2016 presidential and parliamentary elections and during the May inauguration of President Museveni for another contested fi e-year term (see **Blocking and Filtering**).
- Pro-government Twitter bots mimicking human users manipulated online conversations during the elections period and skewed discussions in favor of incumbent candidate President Museveni (see **Media, Diversity and Content Manipulation**).
- Despite the blockings, Ugandans used social media and communications tools for digital advocacy campaigns throughout the year to demand better governance and expose electoral irregularities (see **Digital Activism**).
- An individual was arrested in June 2015 and charged with "offensive communications" for allegedly running a Facebook page under the alias Tom Voltaire Okwalinga that was known for its criticism of the government. Two other Facebook users were arrested for posting a photo depicting the president as dead (see **Prosecutions and Detentions for Online Activities**).

Introduction

Internet freedom in Uganda experienced a precipitous decline in the lead up to and aftermath of contentious general elections in February 2016. Unprecedented violations and restrictions included blocks of popular social media platforms and communications tools on two separate occasions, observations of pro-government commentators manipulating the online information landscape, a weakening judiciary coopted by the ruling party, and arrests of social media users for posting critical content.

Prior to this coverage period, Ugandans enjoyed a relatively open internet with few blatant incidents of censorship. Among the country's growing internet user population, who access the web primarily on mobile devices, social media use has proliferated in recent years, fueling greater citizen engagement with and information sharing about their country's affairs. As the country prepared for the 2016 general elections, in which the incumbent President Yoweri Museveni was seeking a seventh term, citizens ramped up their social media activity with the hopes of fostering a more democratic and accountable elections process. Their efforts were stifled when the go ernment ordered service providers to shut down access to Facebook, Twitter, and WhatsApp for four days during the February elections, and again for one day during the president's inauguration to another contested fi e-year term in May.

A few arrests for posting or sharing content critical of the president on social media were reported during the coverage period, indicating the government's growing intolerance of critical online commentary. Robert Shaka was arrested in June 2015 and charged with "offensive communications" for allegedly running a Facebook page under the alias Tom Voltaire Okwalinga that was known for its criticism of the government. Two other Facebook users were arrested for posting a photo depicting the president as dead. Meanwhile, a series of surveillance revelations strengthened suspicions of unchecked government monitoring, though there were no incidents of abuse reported in the past year. Technical attacks against members in LBGTI community continued.

Obstacles to Access

ICTs uptake expand marginally in the past year, and costs, though improving, are still relatively high for the majority of Ugandans, especially those in rural areas.

Availability and Ease of Access

Internet access increased marginally in the past year, up from 18 percent in 2014 to 19 percent in 2015, though mobile phone penetration remained stagnant, at approximately 51 percent in 2015, according to the International Telecommunication Union (ITU).[1] Government data from the Uganda Communications Commission (UCC), the communications regulatory body, estimated an internet penetration rate of approximately 40 percent as of March 2016, which included mobile data alongside fi ed-line internet subscriptions.[2] The steady growth in internet users can be attributed to the increasing use of mobile broadband for browsing, with 3G and 2G coverage reaching 27 percent

1 International Telecommunication Union, "Percentage of Individuals Using the Internet," 2000-2015, http://bit.ly/1FDwW9w.

2 Uganda Communications Commission, "Postal, Broadcasting and Telecommunications Annual Market & Industry Report 1st Quarter January – March 2016," http://www.ucc.co.ug/files/downl ads/Q1-Market-Report-for-Jan-March-2016-Mbaga.pdf

and 81 percent of the population, respectively, as of October 2015.[3] However, internet speeds are still very slow, averaging 1.9 Mbps (compared to a global average of 6.3 Mbps), according to data from Akamai's "State of the Internet" 2016 first quarter report.[4]

While internet access has become more affordable, particularly on mobile phones, costs remain relatively expensive for the majority of Ugandans. In its 2015/16 Affordability Report, the Alliance for Affordable Internet estimated that 500MB of mobile broadband costs over 15 percent of the country's GNI per capita of US$670, which is well above the target of 5 percent or less set by the UN Broadband Commission in 2011 as a goal for broadband affordability.[5]

Limited access to electricity further impedes access to ICTs and is mostly concentrated in urban areas. Meanwhile, only 18 percent of Ugandans live in urban areas,[6] resulting in a significant urban-rural divide in access.[7]

New investments in Uganda's ICT infrastructure aim to close the digital divide, with some assistance coming from global technology companies. In December 2015, Google launched its first Wi-Fi network in Kampala as part of "Project link."[8] Uganda's ICT ministry through the National Information Technology Authority – Uganda (NITA –U) has been developing the National Data Transmission Backbone Infrastructure since 2007, which aims to ensure the availability of high bandwidth data connections in all major towns at reasonable prices.[9] In October 2016, the government began offering a free trial of wireless internet access in Kampala Central Business District and parts of Entebbe.[10]

Restrictions on Connectivity

There were no reports of deliberate government interference with mobile phone or internet networks during the coverage period. However, in a negative development, the government restricted access to social media platforms and communications tools for the first time, ordering the shutdown of Facebook, Twitter, WhatsApp, and mobile money services on February 17, 2016—the eve of the 2016 elections. The shutdowns lasted four days. Platforms were blocked again in the lead up to incumbent President Museveni's inauguration on May 11, 2016 (see Blocking and Filtering).

ICT Market

Uganda's backbone connection to the international internet is privately owned in a competitive market.[11] The country's national fiber backbone is connected to the EASSy international

3 Uganda Communications Commission, "A Study into Communication Services and Infrastructure across the Country," October 2015, http://bit.ly/2aBwso9

4 Akamai, "Average Connection Speed: Uganda," map visualization, *The State of the Internet Q1* (2016), http://bit.ly/1WRjumM

5 "The 2015-16 Affordability Report," Alliance for Affordable Internet, 2016, http://bit.ly/2epYu5r

6 Uganda Bureau of Statistics, "2015 Statistical Abstract," June 2015, http://bit.ly/1ZHSG8g.

7 Uganda's national literacy rate stands at 71 percent among persons aged 10 years and above. See: Uganda Bureau of Statistics, "2015 Statistical Abstract," June 2015.

8 Google, "Bringing Better Wi-Fi to Kampala with Project Link," December 3, 2015, http://bit.ly/1OyL7dq

9 Ministry of Information and Communications Technology, "National Data Transmission Backbone and e-Government Infrastructure Project," Republic of Uganda, http://bit.ly/1OEBpMj

10 NITA-U, Free Public Internet Access (WIFI), http://www.nita.go.ug/media/free-public-internet-access-wifi

11 Econ One Research, "A Case Study in the Private Provision of Rural Infrastructure," July 30, 2002, http://bit.ly/1jxsMXc.

submarine fibe -optic cable system that runs along the east and southern coasts of Africa.[12] Telecommunications providers are also hooked to TEAMS (The East African Marine System) and SEACOM marine fibe s through Kenya. As of 2016, 23 ISPs are connected to the Uganda Internet Exchange Point (UIXP).[13]

The number of industry players has grown over the years, and many now offer comparable prices and technologies. There are no known obstacles or licensing restrictions placed by the government on entry into the ICT sector, and new players have entered the market with ease in recent years.

Currently, there are 22 telecommunications service providers that offer both voice and data services, including MTN Uganda, Uganda Telecom, Airtel, Smart Telecom, Africell Uganda (former Orange Uganda), Vodafone, Afrimax, among others.[14] All of these telecoms offer 4G LTE network speeds. Aside from the state-owned Uganda Electricity Transmission Company Limited, which is a licensed public infrastructure provider that has part ownership of Uganda Telecom, all of the licensed service providers are privately owned.

Regulatory Bodies

Uganda's telecommunications sector is regulated by the Uganda Communications Commission (UCC), which is mandated to independently coordinate, facilitate, and promote the sustainable growth and development of ICTs in the country. The UCC also provides information about the regulatory process and quality of service, and issues licenses for ICT infrastructure and service providers.[15] The commission's funds come mainly from operator license fees and a 1 percent annual levy on operator profits.

There is a general perception, however, that comprehensive and coherent information about the commission's operations is not always accessible, and that the body is not entirely independent from the executive branch of the government. For example, the ICT minister has the authority to approve the new regulator's budget and appoint members of its board with approval from the cabinet. There are no independent mechanisms in place to hold the regulator accountable to the public.

In March 2016, the government launched an effort to remove parliamentary approval of regulations made by the ICT ministry by introducing the Uganda Communications (Amendment) Bill, 2016 to Parliament, which amends section 93(1) of the Uganda Communications Act, 2013.[16] The amendment, if approved, would effectively eliminate the system of checks and balances on the minister's supervision of the communications sector.[17]

12 Eassy maps, accessed August 28, 2016, http://www.eassy.org/map.html#

13 The Uganda Internet Exchange Point, "Connected Networks," http://uixp.co.ug/networks.

14 UCC, "Annual Report 2014/2015," Pg.15

15 UCC, "Communications Licensing Application Guidelines" Pursuant to the telecommunications (licensing) regulations 2005, UCC issues two types of licenses: Public Service Provider (PSP) and Public Infrastructure Provider (PIP). The application fee for both license types is $2,500 dollars (a PIP license requires a one-off initial fee of $100,000), and annual fees range from $3,000-$10,000. These licenses allow holders to either set up telecommunications infrastructure or provide telecommunications services. The UCC levies a 1 percent charge on providers' annual revenue, http://bit.ly/1Qi87iX.

16 Parliament of Uganda, "Govt seeks to amend UCC Act," press release, http://bit.ly/2auovS3

17 Robert Sempala, "Parliament should disregard UCC Bill of 2016," The Observer, March 25, 2016, http://bit.ly/2aAMOQz

Limits on Content

Following repeated threats to shut down social media platforms in the previous year, the government ordered service providers to block access to Facebook, Twitter, WhatsApp, and mobile money services in February 2016, as citizens prepared to head to the polls, citing "security reasons." The blocks were repeated in May, a day before President Museveni's inauguration to another five-year term. Pro-government Twitter bots mimicking human users manipulated online conversations during the elections period and skewed discussions in favor of incumbent candidate President Museveni. Despite the social media blocks, Ugandans actively used the tools for digital advocacy campaigns throughout the year to demand better governance and expose electoral irregularities.

Blocking and Filtering

Social media and communications platforms were shut down by the government on two separate occasions in 2016, both relating to the contentious general elections.

On February 17, 2016, as Ugandans prepared to vote for a new president and parliamentary representatives on February 19, citizens found their access to the Facebook, Twitter, WhatsApp, Instagram, and mobile money services completely inaccessible.[18] Telecom provider MTN confi med in a Twitter post (even though blocked) that it had been instructed by the regulatory authority to block access to the platforms due to "security concerns."[19] President Museveni also confi med the temporary blocking, declaring it a necessary measure to stop people using the platforms for "telling lies."[20]

Nearly 1.5 million users subsequently floc ed to VPN services to bypass the blockade, demonstrating the futility of the restriction.[21] Access to the platforms was restored on February 21, 2016, four days later after the blockade, but was obstructed again for a day, on May 11, 2016, the day before President Museveni inauguration to another contested fi e-year term in office, again for security reasons.[22]

Following the fi st blocking incident, the UCC regulatory authority issued an apology on February 23, 2016 for any inconveniences caused to Ugandans in a post on their Facebook page but cited that their decision was in line the Uganda Communications Act, 2013,[23] which allows the regulatory body to "monitor, inspect, license, supervise, control and regulate communications services" and to monitor and enforce compliance relating to content.[24] While the UCC was somewhat transparent about their actions, the blocking of widely-used social media and communications platforms was disproportionate to the aims and lacked avenues for appeal.

Meanwhile, the 2014 Anti-Pornography Law threatens to hold service providers criminally liable

18 "Uganda election: Facebook and WhatsApp blocked," BBC, February 18, 2016, http://www.bbc.com/news/world-africa-35601220; Morgan Winsor, "Uganda elections 2016 social media: Facebook, Twitter, Instagram, WhatsApp blocked during voting," International Business Times, February 18, 2016, http://bit.ly/1Q6UHWV

19 MTN Uganda, Twitter post, February 18, 2016, https://twitter.com/mtnug/status/700286134262353920

20 Tabu Butagira, "Museveni explains social media, mobile money shutdown," http://bit.ly/1PTKux9.

21 CIPESA, Ugandans Turn to Proxies, VPN in Face of Social Media Shutdown, http://bit.ly/1QieVgG.

22 James Propa, "Social Media Blocked in Uganda Ahead of President Museveni's Inauguration," Global Voices (blog), May 11, 2016, http://bit.ly/2aCLJFd.

23 Section 5(1) (b) and (x), Uganda Communications Commission Act, 2013, http://bit.ly/2fUA3SM

24 Uganda Communications Commission, Facebook post, February 23, 2016, http://on.fb.me/21kSIcf

for uploading or downloading vaguely defined po nographic material on their systems,[25] with penalties of up to fi e years in prison and fines f US$4,000. In August 2016, the minister of ethics announced that it had purchased a "pornography detection machine" from a South Korean company that would be able to monitor and potentially block pornographic material on electronic devices.[26] The announcement led to concerns that blocking and fil ering would be employed to target not only pornography, which the authorities often confla e with LGBTI content, and other objectionable content. There have been no further updates as to whether the technology had been implemented as of October 2016.

Content Removal

In contrast to the government's targeting of social media and communications platform during this report's coverage period, there were no known instances of formal or informal content removal requests for political or social content online.

Media, Diversity, and Content Manipulation

The 2016 election period was characterized by an intensified go ernment crackdown against the traditional media, which saw the shutdown of print and broadcast media houses perceived to be too critical of the government, as well as police attacks and journalist arrests. While online news media outlets remained relatively unscathed compared to their print and broadcast counterparts, the targeted crackdown engendered a culture of self-censorship among journalists both off and online.[27] Taboo topics include the military, the president's family, the oil sector, land-grabs, and presidential term limits. Nonetheless, critical commentary and opposition voices have become more vibrant online in recent years.

Despite the government's repeated threats against the use of social media over the past few years, which culminated in the days-long shutdown of several platforms during the February 2016 elections, candidates relied heavily on social media to engage with citizens and win their votes.[28] Research on social media trends during the 2016 elections found that auto-generated Twitter bots mimicking human users worked to manipulated online conversations by skewing discussions in favor of incumbent candidate President Museveni, leading to suspicions of paid pro-government trolling.[29]

Content available online in Uganda is somewhat diverse, though news websites provided by the Vision Group, a media company that is partly owned by the government, are only available in four local languages (out of 40 languages and 56 native dialects). Newspapers such as *Bukedde*, *Etop*, *Rupiny,* and *Orumuri* have created online platforms. Other news sites of major privately owned

25 "Pornography" defined in the law as "any epresentation through publication, exhibition, cinematography, indecent show, information technology or by whatever means, of a person engaged in real or stimulated explicit sexual activities or any representation of the sexual parts of a person for primarily sexual excitement." Anti-Pornography Act, 2014, http://bit.ly/PeaDyk.

26 Yomi Kazeem, "Uganda's morals police are investing $88,000 in a 'porn-detection machine,'" Quartz Africa, August 3, 2016, http://bit.ly/2ateX95; Martin Kitubi, "Pornography detection machine arrives September - Lokodo," The New Vision, August 2, 2016, http://bit.ly/2elxjKZ.

27 Freedom House, "Uganda," *Freedom of the Press 2015*, https://freedomhouse.org/report/freedom-press/2015/uganda. Human Rights Watch, "Uganda: Intimidation of Media, Civic Groups," January 10, 2016, http://bit.ly/1ZfWDRd.

28 John Semakula and Carol Natukunda, "Presidential Aspirants Take Battle To Social Media," October 13, 2015, http://www.elections.co.ug/new-vision/election/1385966/presidential-aspirants-battle-social-media

29 CIPESA, "Analysis of Twitter Activity During the 2016 Presidential Debates in Uganda," February 2016, http://www.cipesa.org/?wpfb_dl=210

newspapers are only accessible in English, which is not widely spoken across Uganda. The Google Uganda domain is available in fi e local languages,[30] while the Firefox web browser can be accessed in two languages, Luganda and Acholi.[31] As of early 2016, Wikipedia can be accessed in Luganda with 709 articles translated.[32]

Blogging continues to be popular among young Ugandans who have boldly taken to the internet to push the boundaries on controversial issues such as good governance and corruption.[33]

Digital Activism

Internet use is steadily enhancing citizen participation in democratic processes as well as increasing public scrutiny of government actions. Crowdsourcing and crowd-mapping tools have given citizens the ability to monitor elections, and a number of civil society groups are increasingly using communications platforms and social media for advocacy and to call for protests.

For example, in June 2015, a two-day Twitter campaign under the hashtags #FreeDanny and #ImpunityUg were carried out to demand the release of an online youth activist Daniel Turitwenka (alias Danny-T), who had been detained by police as he visited a friend in prison.[34] He was released on the third day.

Digital activism was particularly profound during the 2016 elections period. A week before the elections in February, two bloggers identified oter-register discrepancies exposing 20,000 ghost voters in the national voter register.[35] Although initially denied by the electoral commission, it later admitted the discrepancy and addressed the concern.[36]

Activists also took onto the internet to call for peace during the elections period using the hashtag #IPledgePeaceUg, while #UGDebate16 trended during the live broadcast of the presidential debate, attached to Twitter conversations about key political issues discussed by the candidates. Significantl , the hashtags #UgandaDecides was widely used to monitor and discuss election issues, cover the campaign trail, and condemn election malpractices such as vote rigging and the intimidation of opposition leaders and journalists. Following the social media block, #UgandaDecides was used to share tips on how to bypass the blockade using VPNs.[37] Another popular hashtag, #FreeBesigye,[38] was used to demand for the release of the lead opposition candidate, Kizza Besigye, who was continuously arrested during the election period, including on Election Day.

Such forms of engagement with new digital platforms drew the attention and ire of government officials, who op ed to restrict access to several platforms multiple times in 2016, though the blocks failed to deter users from accessing the platforms. In an impressive demonstration of digital activism

30 Tabitha Wambui, "Google Uganda Launches Two New Local Language Domains," *The Daily Monitor*, August 4, 2010, http://bit.ly/1QMW3Yk.

31 Mozilla, "Interview: Mozilla Uganda translates Firefox into Acholi," February 16, 2013, http://mozilla-uganda.org/?p=173.

32 Wikipedia, "Olupapula Olusooka," accessed February 1, 2016, https://lg.wikipedia.org/wiki/Olupapula_Olusooka

33 Joseph Elunya, "Controversial Ugandan Blogger Won't Budge," *All Africa*, August 26, 2012, http://bit.ly/1W2t7Cb. Ugo News. "Top 10 Ugandan Facebook Pages With Content That Will Change Your Life Forever," http://bit.ly/21vfz1s.

34 Prudence Nyamishana, After Youth Activists' Arrest, Ugandans Speak Out Against Police Impunity, http://bit.ly/1WRxPPp

35 Evelyn Namara, "Exposing voter-register discrepancies, a few days to Uganda's Presidential and Parliamentary Elections," February 10, 2016, http://bit.ly/1THFGAV

36 The Observer, "EC apologises for 20,000 'ghosts' on voters register," February 13, 2016, http://bit.ly/1OyRq0E.

37 CIPESA, "Ugandans look to bypass election social media ban," February 18, 2016, http://bit.ly/2avOiJp

38 Twitter, #freebesigye, https://twitter.com/hashtag/freebesigye

against online censorship, millions of VPNs were downloaded the day of the blocking, information about which was shared virally on Twitter (see Blocking and Filtering).

Violations of User Rights

An individual was arrested in June 2015 and charged with "offensive communications" for allegedly running a Facebook page under the alias Tom Voltaire Okwalinga that was known for its criticism of the government. A series of surveillance revelations strengthened suspicions of unchecked government monitoring in the past year. Technical attacks targeting LGBTI individuals continued.

Legal Environment

The Ugandan Constitution provides for freedom of expression and speech, in addition to the right to access information. However, several laws—including the Press and Journalist Act, 2000, sections of the Penal Code Act, 1950, and the Anti-Terrorism Act, 2002—appear to negate these constitutional guarantees for freedom of expression. For example, the Press and Journalist Act of 2000 requires journalists to register with the statutory Media Council, whose independence is believed to be compromised by the government's influence o er its composition. The penal code contains provisions on criminal libel and the promotion of sectarianism, imposing penalties that entail lengthy jail terms. While none of these laws contain specific p ovisions on online modes of expression, they could arguably be invoked for digital communications and generally create a "chilling effect" on freedom of expression both online and offline.

The 2011 Computer Misuse Act includes provisions that can specifically limit f eedom of expression online. Under Article 2 of the law, the dissemination of "offensive communication" is prohibited alongside child pornography and cyber harassment, and is vaguely defined as the use f "electronic communication to disturb or attempts to disturb the peace, quiet or right of privacy of any person." Offenses under this provision of the Act are considered misdemeanors and subject to fines, imprisonment of up to one year, or both.[39]

Meanwhile, the 2002 Anti-Terrorism Act criminalizes the publication and dissemination of content that promotes terrorism, which is vaguely defined, and convictions can car y the death sentence.[40] Amendments to the act enacted in June 2015 may impact internet freedom in its broad criminalization of the "indirect" involvement in terrorist activists and the "unlawful possession of materials for promoting terrorism, such as audio or video tapes or written or electronic literature."[41]

The independence of Ugandan judiciary has become more tenuous in recent years. As part of his efforts to consolidate power in the led up to the 2016 elections, the president promoted new judges to both the Constitutional and Supreme Court in September 2015. The process was criticized for lacking transparency and undermining judicial independence, while other critics called for more public scrutiny in the appointment of new judges.[42]

39 Computer Misuse Act, 2011, http://www.ulii.org/content/computer-misuse-act.

40 Art.9 (b), The Anti-Terrorism Act, 2002, http://bit.ly/1ZRELPH.

41 The Anti-Terrorism (Amendment) Act, 2015, http://bit.ly/1LNgFg1.

42 Sulaiman Kakaire & Kiyonga D, "Museveni's choice of judges for promotion raises questions," The Observer, September 16, 2015, http://bit.ly/2aCxZNR

Prosecutions and Detentions for Online Activities

A few arrests for posting or sharing content critical of the president on social media were reported during the coverage period, indicating the government's growing intolerance of critical online commentary.

In June 2015, a man named Robert Shaka was arrested on charges of disseminating "offensive communication" under the 2011 Computer Misuse Act. Police suspected Shaka of running the popular Facebook account called Tom Voltaire Okwalinga (TVO),[43] which was well known for its politically charged posts that often accuse the Ugandan president and other senior leaders of corruption and incompetence.[44] He was released on bail.[45] Before his court hearing in February 2016, Shaka filed a petition o the Constitutional Court challenging the constitutionality of Article 25 of the Computer Misuse Act under which we was charged,[46] leading a judge to suspend his trial in April 2016 until his petition against the Computer Misuse Act can be heard."[47]

In March 2016, two Facebook users were arrested for posting a picture depicting the president as dead.[48]

Surveillance, Privacy, and Anonymity

There is a strong sense that government surveillance of citizens' communications has heightened in recent years, particularly as the government attempts to address the threat of terrorism in the region. A series of surveillance revelations strengthened such suspicions in the past year.

In July 2015, email leaks from the Italian surveillance fi m Hacking Team revealed that the Ugandan government began talks in April 2015 with the company to purchase its sophisticated spyware known as Remote Control System (RCS).[49] While the leaked emails did not confi m the sale, they point to the government's intent to acquire such technologies that can monitor and intercept user communications.

A report by Privacy International released in October 2015 detailed the government's deployment of FinFisher intrusion malware under a secret operation codenamed Fungua Macho ("open your eyes" in Swahili).[50] According to the report, the malware was planted in the WiFi of several hotels in Kampala, Entebbe, and Masaka to illegally spy on targeted activists, opposition politicians, and journalists between 2011 and 2013. It is unclear whether FinFisher was still being deployed during this report's coverage period.

Another report from January 2016 by Unwanted Witness Uganda, a local internet rights organization,

43 Tom Voltaire Okwalinga, Facebook Page, https://www.facebook.com/tom.okwalinga.

44 Douglas Mpuga,"Social Media Critic Arrested in Uganda," Voice of America, June 13, 2015, http://bit.ly/1RkEaQx.

45 Tony Bath, "Social Media Critic Robert Shaka Released on Bail," Uganda Radio Network, June 15, 2015, http://bit.ly/1RSBOcG.

46 Betty Ndagire, "Museveni social media critic seeks stay of trial," Daily Monitor, February 4, 2016, http://bit.ly/1THsPgS

47 "Court suspends trial of Museveni critic," The Insider, April 22, 2016, http://bit.ly/2fvYVQv

48 "Two arrested over 'dead' Museveni picture," The Daily Monitor, March 7, 2016, http://bit.ly/2aoNVhL

49 Mujuni Raymond Qatahar, "Wikileaks Emails: Uganda To Buy 3bn Surveillance Equipment," Qataharray (blog), July 21, 2015, http://bit.ly/1XfOAok; Wikileaks, "Hacking Team," July 8, 2015, http://bit.ly/1jQARWv; Sadab Kitatta Kaaya, "Police in Shs 5bn spy deal," The Observer, July 22, 2015, http://bit.ly/1NR8x3t.

50 Privacy International, "For God and My President: State Surveillance In Uganda," October 2015, http://bit.ly/2aEfs3C

alleged that the telecoms service provider MTN Uganda shared the data of its 10 million subscribers to the ruling party's communication center, which the party subsequently used to send unsolicited messages on behalf of President Museveni's campaign.[51] Telephone companies reportedly "face undue influence and p essure from [the] government demanding for print-outs of phone calls made by any citizen without court orders… [which] have been used against activists or human rights defenders to justify their arrests, arbitrary detention or at times used as evidence in courts of law."[52]

The government's surveillance powers are governed by the 2010 Regulation of Interception of Communication (RIC) Act, which was hurriedly passed following the July 2010 Al-Shabaab terrorist attack in Kampala. Under the RIC Act, telecommunication companies are required to install equipment that enables real-time electronic surveillance of suspected terrorists. The RIC Act also gives the government permission to tap into personal communications for national security concerns,[53] which can be requested by the security minister and granted after an order by a High Court judge.[54] Service providers are further required to retain metadata for an unspecified amount of time,[55] as well as disclose the personal information of individuals suspected of terrorism to the authorities upon issuance of a court warrant or notice from the security minister on matters related to national security, national economic interests, and public safety.[56] Failure to comply with the provisions in the RIC Act can entail penalties of up to fi e years in prison for intermediaries, in addition to license revocations.[57] It is unclear the extent to which these provisions in the 2010 RIC Act has been implemented or operationalized.

In addition to the RIC Act, clauses in the 2002 Anti-Terrorism Act give security office s, appointed by the interior minister, the power to intercept communications of individuals suspected of terrorism and to keep them under surveillance, without judicial oversight.[58]

Anonymous communication is compromised by mandatory registration for mobile phone SIM cards and mobile internet subscriptions. Launched in March 2012, the process requires subscribers to provide a passport photo and ID, both residence and workplace addresses, and next of kin, among other personal details.[59] Civil society groups cited concerns that "the mandatory SIM card registration was carried out to enable the use of surveillance equipment purchased and installed by telecom companies."[60] In October 2015, the regulatory body issued a directive to telecom companies to deactivate all unregistered SIM cards by November 2015, which may have been linked to

51 Unwanted Witness Uganda, "Press Statement on MTN Uganda sharing Subscribers' data with ruling NRM party for Campaigns," press release, December 18, 2015, http://bit.ly/2anU7cL

52 Unwanted Witness Uganda, *The Internet: They Are Coming For It Too*, January 17, 2014, 39, http://bit.ly/1fTb1rH. These allegations were denied by the security minister, who claimed that any phone tapping is done in compliance with the law, upon issuance of a court order, and for a limited period against users suspected of "subversive activities" and criminal activity. See: Deo Walusimbi, "Muruli Mukasa: I replace Sejusa," The Observer, March 5, 2014, http://bit.ly/1kkKQUB.

53 Amnesty International, "Uganda: Amnesty International Memorandum on the Regulation of Interception of Communications Act, 2010," December 14, 2010, http://bit.ly/1MPUDx8.

54 Lawful interception is granted after issuance of a warrant by a judge if "there is an actual threat to national security or to any national economic interest, a potential threat to public safety, national security or any national economic interest, or if there is a threat to the national interest involving the State's international relations or obligations." See, Regulation of Interception of Communications Act, 2010 Section 5, September 3, 2010, http://bit.ly/1jQAVpl.

55 The Regulation of Interception of Communications Act, 2010, Section 11.

56 The Regulation of Interception of Communications Act, 2010, Section 8.

57 The Regulation of Interception of Communications Act, 2010, Section 62.

58 The Anti-Terrorism Act, 2002, Part VII—Interception of Communications.

59 Unwanted Witness Uganda, *The Internet: They Are Coming For It Too*.

60 Unwanted Witness Uganda, *The Internet: They Are Coming For It Too*.

government efforts to consolidate control in the lead up to the February 2016 elections.[61]

In response to growing concerns over infringements on users' right to privacy in Uganda, civil society pushed for data protection legislation in 2014,[62] which led to the drafting of the Data Protection and Privacy Bill, 2016 by year's end.[63] While the bill was initially well received, it was later criticized for being open to misinterpretation due to the broad and vague conditions in which personal data may be collected, such as for "national security" reasons.[64] Approved by cabinet, the Bill received its fi st hearing in parliament in 2016 but has not been passed as of the time of writing.[65]

Intimidation and Violence

While print journalists have long faced a high degree of harassment and occasional violence for their reporting, these types of violations are still relatively rare for the online sphere.

The Uganda Police Force established a Cyber Crimes Unit to fight malicious echnical attacks in 2014,[66] which was criticized by observers as an effort to intimidate users and encourage self-censorship online.[67] The unit reportedly worked to profile "dozens of internet users, particularly those deemed to be opponents of the government,"[68] worrying activists as the country headed to the general elections in early 2016. In mid-2015, the Cyber Crimes Unit publicly stated its mandate includes "threats that could destabilize the country" committed on social media platforms.[69]

Technical Attacks

Technical attacks against vulnerable groups and marginalized communities, particularly the LGBTI community, remained a growing concern in Uganda in the past year. According to an LGBTI activist in Uganda,[70] a Ugandan social worker at the Most at Risk Populations Initiative had their email and Facebook account hijacked. The activists believe this may have been perpetrated the government given the sheer amount of information the social worker possessed about the LGBTI community through their work and private communications.

Hacking attacks against gay individuals for the purposes of blackmail were also reported. In one recent incident, the Facebook account of a closeted gay celebrity was hacked with screenshots taken of private messages pointing to his sexual orientation that were used to blackmail him.[71]

61 Fredric Musis, "Unregistered Sim cards to be disconnected in 30 days – UCC," The Daily Monitor, October 31, 2015, http://bit.ly/2aDY1AB

62 Solomon Lubambula, "Phone users demand for Data Protection law," Unwanted Witness, March 21, 2014, http://bit.ly/1MPWxh6.

63 Government of Uganda, The Data Protection and Privacy Bill, 2014, http://bit.ly/1GM36LD.

64 CIPESA, "Reflections on Uganda s Draft Data Protection and Privacy Bill, 2014," February 2015, http://bit.ly/1KkFgXg.

65 Interview with a Ministry of ICT official, Ma ch 1, 2016.

66 Taddeo Bwambale and Raymon Baguma, "Uganda sets up unit to fight cybe crime," The New Vision, August 6, 2013, http://bit.ly/1kkHaSA.

67 Andrew Bagala, "Activists cry foul as police set up cybercrime unit," The Daily Monitor, March 19, 2014, http://bit.ly/1KkCzom; Unwanted Witness, "Police establishes cybercrimes unit to curtail online freedoms," March 18, 2014, http://bit.ly/1rDT1uz.

68 Unwanted Witness Uganda, *The Internet: They Are Coming For It Too*, 38, http://bit.ly/1fTb1rH.

69 Bagala Andrew, "Crackdown on social media crime starts," The Daily Monitor, June 22, 2015, http://bit.ly/1LGN76A.

70 Anonymous interview with Freedom House in September 2016.

71 Anonymous interview with Freedom House in September 2016.

Freedom House

Ukraine

	2015	2016
Internet Freedom Status	Partly Free	Partly Free
Obstacles to Access (0-25)	8	8
Limits on Content (0-35)	10	11
Violations of User Rights (0-40)	19	19
TOTAL* (0-100)	**37**	**38**

* 0=most free, 100=least free

Population:	**45.2 million**
Internet Penetration 2015 (ITU):	**49 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Partly Free**

Key Developments: June 2015 – May 2016

- Pressure from separatist militants resulted in the temporary blocking of dozens of websites within the eastern regions of the country (see **Restrictions on Connectivity**).
- Ukrainian authorities clamped down on so-called "separatist" and "extremist" expression online, with many users detained, fined, and e en imprisoned for such activities (see **Prosecutions and Detentions for Online Activities**).
- Ukrainian nationalist hackers leaked the personal information of thousands of journalists working in eastern Ukraine, deliberately compromising their privacy and safety (see **Intimidation and Violence**).

Editor's Note

On March 16, 2014, a referendum held in Crimea resulted in Russia's annexation of the territory from Ukraine. On March 27, the General Assembly of the United Nations issued a non-binding resolution calling the referendum invalid and urging member states and international organizations not to recognize any such change in Crimea's status.

Freedom on the Net focuses on internet freedom developments as they pertain to internet users within each of the 65 countries under study. This report focuses primarily on the overall status of internet freedom in Ukraine from June 2015 through May 2016. Due to the ongoing crises in the region, events in Crimea during this time may be excluded from this report.

Introduction

Ukraine's internet freedom declined due to increasing arrests against netizens for expressing "separatist" views on social media, while users in the Donbass region were barred from accessing dozens of blocked sites.

While the online media sphere flourished in the wa e of the Euromaidan movement of 2014, the ongoing conflict bet een Ukrainian forces and Russian-backed separatists in eastern Ukraine has undermined user rights online and fostered an environment of self-censorship. Ukrainian authorities have become less tolerant of online expression perceived as critical of Ukraine's position in the conflict, and the go ernment has been especially active this year in sanctioning social media users for "separatist" and "extremist" activities, with many users detained, fined and e en imprisoned for such activities. Meanwhile, separatist forces in the east have stepped up efforts to block content online perceived to be in support of Ukrainian government or cultural identity.

Ukrainian internet users continue to face external threats to their digital security and physical wellbeing. Within the coverage period, key infrastructure in Ukraine, including a power plant, was targeted in a series of debilitating cyberattacks which appear to have originated from within Russia. Meanwhile, Ukrainian nationalists targeted journalists working within the conflict zone, leaking the personal details of thousands of accredited journalists online.

Despite the challenges posed by the ongoing conflict and info mation war, Ukrainian civil society continues to have an important presence online. Activists use social media to organize and promote ideas such as coordinating volunteer support for the military, aiding efforts to assist internally displaced populations, encouraging oversight of government, as well as exposing instances of biased or manipulative information.

Obstacles to Access

Internet penetration continued to grow in 2015-2016, and access to the internet remains affordable for most of the population. The ICT market is diverse, and state-owned providers no longer dominate the market. Inevitably, Ukraine's telecommunications market has suffered during the reported period due to economic hardships in the country and the crisis following Russia's annexation of Crimea and later,

the upheaval in eastern Ukraine. Other obstacles to access, such as damage to infrastructure in the eastern region, have obstructed internet and mobile access for parts of the country.

Availability and Ease of Access

Internet penetration in Ukraine continues to grow steadily, due in part to diminishing costs and the increasing ease of access, particularly to mobile internet. According to the International Telecommunication Union (ITU), Ukraine had an internet penetration rate of 49 percent in 2015,[1] compared to 43 percent in 2014, and 41 percent in 2013.[2] At the same time, local research indicates that the share of regular Internet users among Ukrainian adults has reached the 62 percent mark.[3] According to the Pew Research Center, 53 percent of Ukrainian adults accessed the internet at least occasionally or owned a smartphone as of 2015.[4] The Pew Research Center also found that 73 percent of Ukrainian adults who do have access to the internet use it on a daily basis.[5] For fi ed-line broadband subscriptions, the penetration rate was approximately 11.8 percent at the end of 2015,[6] while mobile broadband had a penetration rate of 7.5 percent.[7] Meanwhile, according to Akamai, the average broadband connection speed in Ukraine was 11.2 Mbps in the fourth quarter of 2015 (compared to 9.3 Mbps in the fourth quarter of 2014),[8] and access to broadband internet in Ukraine is fairly affordable. A monthly unlimited data plan with a 1 Mbps broadband channel costs UAH 80–120 (US$3.20-4.80), while the average monthly wage in the country was UAH 4,920 (US$196) in March 2016.[9]

The level of infrastructure differs between urban and rural areas, contributing to an urban-rural divide. Most people access the internet from home or work, though many middle- and higher-end cafes and restaurants also provide free Wi-Fi. Access is also common in public libraries, schools, shopping malls and airports. Internet cafes still exist but are gradually losing popularity.

According to the World Bank, mobile phone penetration reached 144 percent in 2015.[10] Use of mobile internet is gaining in popularity, with 5.6 million Ukrainians accessing the internet on their smartphones or mobile phones.[11] Cost continues to be the main barrier to higher mobile internet use. In February 2015, mobile operators finally gained access o the military's share of third-

1 International Telecommunication Union, "Percentage of individuals using the Internet," 2013, 2014, 2015, accessed May 2016, http://bit.ly/1cblxxY.

2 International Telecommunication Union, "Percentage of individuals using the Internet," 2013, 2014, 2015, accessed May 2016, http://bit.ly/1cblxxY.

3 Maya Yarovaya, "Уанет 2016: интернет-проникновение преодолело 60%, а 35% заходов пришлись на мобайл" [UaNet 2016: Internet penetration breaks 60%, 35% come from mobile] *AIN*, March 28, 2016. Accessed on April 20, 2016, http://ain.ua/2016/03/28/640413.

4 Pew Research Center, "Communications Technology in Emerging and Developing Nations," March 19, 2015, accessed on March 20, 2016, http://pewrsr.ch/18LK8tw.

5 Pew Research Center, "Online Activities in Emerging and Developing Nations, Pew Research Center," March 19, 2015, accessed on March 20, 2016, http://pewrsr.ch/1MR57bp.

6 International Telecommunication Union, "Fixed broadband 2000-2015," 2015, accessed March 2016, http://bit.ly/1cblxxY.

7 Broadband Commission, *The State of Broadband 2015: Universalizing Broadband,* September 2015, http://bit.ly/ICdQnO.

8 Akamai, "State of the Internet, Q1 2016 Report," https://goo.gl/TQH7L7.

9 State Statistics Service of Ukraine, "Average monthly wage by region in 2016," [in Ukrainian] accessed on April 5, 2016, http://www.ukrstat.gov.ua/operativ/operativ2016/gdn/reg_zp_m/reg_zpm16_u.htm.

10 The World Bank, "Mobile Cellular Subscriptions (per 100 people) 2015," Ukraine, http://data.worldbank.org/indicator/IT.CEL.SETS.P2?locations=UA.

11 Oleh Dmytrenko, "5,6 млн українців заходять в інтернет через смартфон або мобільний телефон," [5.6 million Ukrainians access the internet through a smartphone or mobile phone], Watcher, November 2, 2015, http://watcher.com.ua/2015/11/02/5-6-mln-ukrayintsiv-zahodyat-v-internet-cherez-smartfon-abo-mobilnyy-telefon/.

generation (3G) mobile phone frequencies.[12] All three companies started commercial use of the frequencies in the summer of 2015 and 3G mobile internet access is currently priced at 100-150 UAH ($4.50-7) for 2-3 GB of traffic per month [13]

Restrictions on Connectivity

In late spring and summer of 2014, Russian and pro-Russian forces occupied the Crimean peninsula, and later took control of parts of the Donetsk and Luhansk regions. Along with gaining political control, those forces also attempted to disrupt or regulate access to telecommunications. While some disruptions in internet and mobile connectivity were caused by military activity, especially in eastern Ukraine (for example, cell towers or internet cables damaged by explosions),[14] in some cases there was direct pressure on internet service providers (ISPs) from rebel militias and Russian-supported authorities, causing them to take down or block particular services, such as city web cameras in Luhansk,[15] or Ukrainian news websites in Donetsk,[16] Luhansk[17], and Crimea[18] (see "Blocking and Filtering"). As of May 2015, none of the Ukrainian mobile providers are operating in Crimea.[19]

The backbone connection to the international internet is not centralized, and major ISPs each manage their own channels independently. Ukraine's backbone internet exchange, UA-IX, allows for traffic e change and connection to the wider internet for Ukrainian ISPs. Ukraine's internet infrastructure is diverse, with more than 200 domestic autonomous systems purchasing direct international transit service (out of a total of more than 1,650 domestic autonomous system numbers). The country has a well-developed set of at least eight regional internet exchanges, as well as direct connections over diverse physical paths to the major Western European exchanges.[20]

ICT Market

The Ukrainian telecommunications market is fairly liberal and undergoing gradual development. The state previously owned 93 percent of the largest telecom company and top-tier ISP, Ukrtelecom, but the company was privatized in March 2011.[21] Though no longer state-owned, Ukrtelecom is still the largest ISP in the country and possesses Ukraine's primary network, trunk, and zone telecom

12 Olga Karpenko, "МТС Украина, Киевстар, и life:) получили 3G-лицензии (обновлено)" [MTS Ukraine, Kyivstar and life:) receive 3G licenses (updated)] *AIN*, February 23, 2015, http://ain.ua/2015/02/23/565866.

13 "Во сколько обойдется 3G-интернет: сравнение тарифов,"[How much will 3G Internet cost: comparing the prices] *BigMir net*, June 11, 2015, http://bit.ly/1LmpZMo.

14 "Війна за зв'язок: що відбувається на сході України," [War for connectivity: what is happening in eastern Ukraine] *Tech Today*, *MTS Productions*, September 19, 2014, http://bit.ly/1RiaEeO.

15 "В Луганске отключены все веб-камеры," [All webcameras switched off in Luhansk] *Informator*, June 25, 2014, http://informator.lg.ua/?p=4125.

16 "В "ДНР" ввели цензуру в интернете," ["DNR" Introduces Internet Censorship] *ZN.ua*, May 30, 2015, http://bit.ly/1PQ7yO3.

17 Tetyana Lokot, "Ukrainian Separatists Block 100+ News Websites in 'Lugansk People's Republic'," *Global Voices*, January 14, 2016. https://globalvoices.org/2016/01/14/ukrainian-separatists-block-100-news-websites-in-lugansk-peoples-republic/.

18 "В Крыму отключают украинские новостные сайты," [Ukrainian news websites blocked in Crimea] *Hromadske Radio*, August 12, 2014, http://bit.ly/1L6Ym8j.

19 Vadym Karpus, "«Интертелеком» уйдёт из Крыма с 1 ма," ["Intertelecom" to leave Crimea starting on May 1] *ITCua*, April 15, 2015, http://bit.ly/1P7x4QI.

20 Jim Cowie, "Syria, Venezuela, Ukraine: Internet Under Fire," Dyn Research, February 26, 2014, http://www.renesys.com/2014/02/internetunderfi e/.

21 92.8 percent of shares sold to ESU, a Ukrainian subsidiary of the Austrian company EPIC. See "Укртелеком продан," [Ukrtelecom Sold] *Dengi.Ua*, March 11, 2011, http://bit.ly/1Vq9ALT.

lines.[22] Other telecommunications providers are dependent on leased lines, since Ukrtelecom owns the majority of the infrastructure, and many alternative providers do not have sufficient esources to build their own networks. However, Ukrtelecom does not exert any pressure or regulatory control over other ISPs.

Other major ISPs in Ukraine include Volia, Triolan, Vega, and Datagroup; however, major mobile service providers, like Kyivstar and MTS, also provide broadband internet access.[23] There are about 400 ISPs in Ukraine, according to the National Commission for the State Regulation of Communications and Informatization (NCCIR).[24] Regional ISPs are usually smaller local businesses, and regional dominance largely depends on business and other connections in a specific egion, making the market prone to corruption.

Ukrchastotnagliad, the Ukrainian frequencies supervisory center, reports that 86 operators have licenses to provide satellite communication services in Ukraine. Companies providing internet access using satellite technologies in Ukraine include Ukrsat, Infocom-SK, Spacegate, Adamant, LuckyNet, Ukrnet, and Itelsat. With the exception of Infocom-SK,[25] all of these companies are privately owned.[26] The three major players in the mobile communications market are Kyivstar (owned by Dutch VimpelCom Ltd.), MTS Ukraine (owned by Russian AFK Sistema) which since October 2016 has been operating under the Vodafone brand as part of a partnership agreement, and "lifecell" (formerly "life"), owned by Astelit, whose main shareholders are the Turkish company Turkcell and Ukrainian System Capital Management. Together, these companies hold 94.6 percent of the mobile communications market.[27]

There are no obvious restrictions or barriers to entry into the ICT market, but any new business venture, whether an ISP or an internet cafe, faces obstacles including bureaucracy and corruption, as well as the legal and tax hurdles common to the Ukrainian business environment. In particular, the Ukrainian ICT market has been criticized for its difficult licensing p ocedures for operators—under the 2003 Law on Communications, operators are required to have a license before beginning their activities.

Regulatory Bodies

The ICT sector is regulated by the National Commission for the State Regulation of Communications and Informatization (NCCIR). Members of the NCCIR are appointed by the president of Ukraine.[28] Due to widespread corruption in the political system and the lucrative nature of business in the ICT sector, appointments to the commission have lacked transparency. The NCCIR's work has often been obstructed by claims of nontransparent decisions and operations. Furthermore, the 2003

22 OpenNet Initiative, "Ukraine," *Country Profile*, December 21, 2010, http://opennet.net/research/profiles/ukrain .

23 "Количество пользователей широкополосного доступа в Украине достигло 5,6 млн," [Number Of Broadband Internet Users in Ukraine Reaches 5.6 Million] *AIN*, December 16, 2011, http://ain.ua/2011/12/16/68574.

24 "Во 2 квартале количество абонентов провайдеров Интернет увеличилось на 6,4%," [In Second Quarter Number Of Subscribers Of Internet Providers Grew By 6.4%] *Delo*, July 26, 2007, http://bit.ly/18A2eL4.

25 Infocom-SK was founded in 1991 jointly by state-owned Ukrtelecom and Controlware, a German telecommunications company. Infocom, "History," accessed on June 15, 2012, http://bit.ly/1FIrp1N.

26 OpenNet Initiative, "Ukraine," https://opennet.net/research/profiles/ukrain .

27 Olga Karpenko, "В Украине почти 55 млн абонентов мобильной связи," [Ukraine has almost 55 million mobile subscribers] *AIN*, July 31, 2012, http://bit.ly/1FKMuIE.

28 National Commission on Regulation of Communications and Informatization, accessed on January 10, 2012, http://bit.ly/1OaChbb.

Law on Communications does not guarantee the independence of the NCCIR. However, the newly appointed head of the NCCIR has vowed to reform the regulator in 2015, and is working on a bill that will guarantee both the financial independence f the NCCIR and its independence from the executive branch of state power.[29]

Limits on Content

Unlike traditional media, access to online content in government-controlled Ukraine remains largely unaffected by the Russian occupation of Crimea and Russian involvement in the conflict in parts of eastern Ukraine, though dozens of Ukrainian websites have been censored in the rebel controlled Donetsk and Luhansk regions. Furthermore, online discussion forums and social media continued to be impacted by partisan voices from both sides, Russian-paid commenting, and self-censorship out of fear.

Blocking and Filtering

The Ukrainian government does not engage in blocking websites or fil ering online content, although separatist authorities in the eastern regions of Donetsk and Luhansk did restrict access to news sites over the coverage period. YouTube, Facebook, Twitter, and blog-hosting services such as WordPress and LiveJournal are freely available and have gained significantly mo e users since the Euromaidan protests in 2013-2014.[30]

Russian-backed separatist militants in eastern Ukraine have been more proactive in blocking Ukrainian resources, and have cracked down on Ukrainian news websites in Donetsk.[31] In May 2015, the self-proclaimed "Donetsk People's Republic" followed Russia's example in instituting an official blacklist f websites banned on its territory, though the list is not public and it is unclear to what extent DPR officials ould be able to enforce it.[32] In January 2016, separatist authorities in the neighboring "Luhansk People's Republic" blocked access to over 100 news and media websites by pressuring local ISPs to implement censorship orders.[33]

Since the start of the crisis in eastern Ukraine, Ukrainian authorities have attempted to pressure ISPs to introduce selective blocking of websites containing "separatist" or "terrorist" content, but ISPs have refused wholesale blocking,[34] and insist that court orders must be provided in each case in order for a website to be blocked or taken down. However, individuals have faced legal repercussions for allegedly sharing alleged calls to "separatism" or "extremism" (see "Prosecutions and Detentions for Online Activities"). In October 2015, with the announcement of a new cyberpolice

29 "НКРСИ должна стать независимой — глава ведомства," [NCCIR must become independent—head of regulator] *Delo*, May 26, 2015, http://bit.ly/1Lmv5Iy.

30 Olga Minchenko, "Близько 6 млн українців в січні хоча б 1 раз відвідували Facebook та 11 млн – ВКонтакте," [About 6 million Ukrainians in Jaunary visited Facebook at least once, 11 million – Vkontakte] *Watcher*, February 26, 2014, http://bit.ly/1JGBCGF.

31 "Боевики «ДНР» блокируют интернет-сайты, выступающие против терроризма и сепаратизма," ["DNR" figh ers block internet websites speaking against terrorism and separatism] *CRiME*, September 30, 2014, http://crime.in.ua/node/6462.

32 "В "ДНР" ввели цензуру в интернете," ["DNR" Introduces Internet Censorship] *ZN.ua*, May 30, 2015, http://bit.ly/1PQ7yO3.

33 Tetyana Lokot, "Ukrainian Separatists Block 100+ News Websites in 'Lugansk People's Republic'," *Global Voices*, January 14, 2016. https://globalvoices.org/2016/01/14/ukrainian-separatists-block-100-news-websites-in-lugansk-peoples-republic/.

34 Oleg Pilipenko,"ИнАУ: блокировка сепаратистских сайтов «попахивает» провокацией или непрофессионализмом," [InAU: Blocking separatists websites "smells" of provocation or unprofessionalism] *imena* (blog), August 8, 2014, http://bit.ly/1iOxW07.

unit, the Interior Minister Arsen Avakov also announced plans to create a banned websites registry[35] that would register and block websites and webpages containing "forbidden content" such as child pornography, malware, and content that violates copyright.

Content Removal

In April 2015, in an attempt to block fi e allegedly anti-Ukrainian websites, the Ukrainian Security Service office s seized hosting servers at four data centers in Kyiv of the web-hosting company NIC.ua, also the largest domain registrar in Ukraine.[36] As a result, 30,000 Ukrainian websites that had nothing to do with the targeted websites were also taken offline. It tu ned out that all but one of the fi e websites suspected of separatism only used NIC.ua as a registrar, and hosted their content on servers in Russia. The Security Service claimed that it had officially equested that NIC.ua block the targeted websites, but the company did not comply. NIC.ua denied the fact that they received any official equests and noted that it is illegal in Ukraine to block websites based on a scanned request or warrant, and that proper procedure would require original court documents. Within a few weeks, over 90 percent of the websites had been restored.

Ukraine's criminal code currently mandates punishments for "unsanctioned actions with information stored on computer devices or networks." [37]In some cases, such laws obligate ISPs to remove or block the offensive or illegal content within 24 hours or, if such content is found to be hosted outside of Ukraine, ISPs would have to limit Ukrainian users' access to such content, effectively introducing a practice of fil ering content.

Media, Diversity, and Content Manipulation

Online media in Ukraine is generally less constrained by economic pressure and owner interests than traditional media, and the ubiquitous use of social networks such as Facebook and VKontakte by journalists, politicians and activists for disseminating opinions and promoting media stories further levels the playing field. Ho ever, amid the conflict in eas ern Ukraine, online journalists, commentators and internet users have been pressured to self-censor, especially on topics directly related to the Russia-backed insurgency in the east, and on the themes of separatism, terrorism and patriotism. Self-censorship has been more pronounced in the parts of eastern Ukraine occupied by pro-Russian forces and in Crimea, where internet users and journalists have faced attacks,[38] abuse, and intimidation for their pro-Ukrainian positions. However, the media landscape remains varied, and different viewpoints are readily available to users online, especially on social media.

Journalists continued to experience challenges reporting on the conflict as access o occupied parts of eastern Ukraine remained limited. Online media outlets such as Luhansk's Realnaya Gazeta,[39] as

35 Tetyana Lokot, "Ukraine's New Banned Websites Registry: Security Measure or Censorship Tool?," *Global Voices*, October 22, 2015. https://globalvoices.org/2015/10/22/ukraines-new-banned-websites-registry-security-measure-or-censorship-tool/.

36 Anna Poludenko-Young, "Ukraine's Security Service Takes Down 30,000 Websites to Fight 'Pro-Russian Propaganda'," *Global Voices*, April 28, 2015, http://bit.ly/1M47yqs.

37 Articles 361, 362, 363 of Ukraine's Criminal Code, http://zakon1.rada.gov.ua/laws/show/2341-14/.

38 "У Луганську сепаратисти викрали журналіста і пограбували офіс інтернет-сайту," [In Luhansk, separatists kidnap journalist, rob internet website office] *Radio Svoboda*, July 16, 2014, http://bit.ly/1MKcSSA.

39 Realnaya Gazeta [Реальная Газета], http://realgazeta.com.ua Accessed on August 1, 2016.

well as blogs[40] and social media accounts[41] of users living in occupied territories, provided important framing and information about the state of human rights and freedom of speech in eastern Ukraine, with local users often risking their safety to provide up-to-date reports.

Attempts to manipulate the online landscape have mostly been external, emanating from Russia, in the form of mass commenting and paid posts on social media,[42] as well as fake websites,[43] and social media groups and networks run by pro-Russian internet users.[44] The Ukrainian Ministry of Information has attempted to respond in kind to the organized Russian information manipulation efforts by creating its own "internet army,"[45] but its actions have not received much praise from Ukrainian internet users. Grassroots initiatives to debunk fake news and propaganda from Russia and elsewhere, such as StopFake,[46] have operated consistently on the Ukrainian internet for the past several years.

A new Ministry of Information Policy was created in December 2014,[47] which aims to promote information security, regulate information policy, and protect Ukraine in the information war with Russia, including online. Although the concrete regulatory powers of the new ministry remain unclear, media advocates and journalists have branded the department "Orwellian,"[48] and have expressed concern that the agency will only hinder freedom of speech and set a dangerous precedent in granting the new government a greater measure of control over Ukrainian media.

Digital Activism

The Ukrainian social media sphere, which expanded dramatically during the Euromaidan protests, continued to thrive and Facebook and Twitter played host to lively debates about Ukrainian politics, reforms, and civil society. By the end of 2015, the Facebook audience in Ukraine grew by 30 percent (1.2 million users) and reached 5 million users for the fi st time.[49]

With the annexation of Crimea and the start of the conflict in eas ern Ukraine, activists and volunteers mobilized during Euromaidan[50] and found new uses for online platforms and their networks,[51] switching their efforts over to help fundraise for the needs of the military and volunteer

40 Radio Liberty, *Letters from Donbas*, a series of blog posts from citizens in occupied territories, http://www.radiosvoboda.org/z/17330.html.

41 Citizen data verification ebsite Bellingcat recommends the English Lugansk Twitter account among others as a good source of information from occupied territories in Eastern Ukraine. https://bellingcat.checkdesk.org/en/report/589.

42 Aric Toler, "Inside the Kremlin Troll Army Machine: Templates, Guidelines, and Paid Posts," *Global Voices*, March 14, 2015, http://bit.ly/1j3kMNw.

43 Aric Toler, "Fake 'Ukrainian' News Websites Run by Russian 'Troll Army' Offshoots," *Global Voices*, November 19, 2014, http://bit.ly/1P7EkfB.

44 "Тролесфера," [The Troll Sphere] *Texty.org.ua*, October 4, 2016, http://texty.org.ua/d/fb-trolls/.

45 Tetyana Lokot, "Ministry of Truth' Recruits Ukrainians for 'Internet Army," *Global Voices*, February 25, 2015, http://bit.ly/1OJEyua.

46 StopFake, http://www.stopfake.org. Accessed on August 1, 2016.

47 Ministry of Information Policy of Ukraine, accessed on May 20, 2015, http://mip.gov.ua/en/.

48 Tetyana Lokot, "Ukraine's New "Ministry of Truth" Ridiculed on Social Media," *Global Voices*, December 4, 2014, http://bit.ly/1JGBkzD.

49 Olga Minchenko, "Українська аудиторія Facebook за рік виросла на 30%, і вперше досягла 5 млн користувачів" [Ukrainian Facebook audience grows 30% reaches 5 million users for the fi st time], *Watcher*, January 25, 2016, http://watcher.com.ua/2016/01/25/ukrayinska-audytoriya-facebook-za-rik-vyrosla-na-30-i-vpershe-dosyahla-5-mln-korystuvachiv/.

50 Tetyana Bohdanova, "How #EuroMaidan and War with Russia Have Changed Ukraine's Internet," *Global Voices*, January 9, 2015, http://bit.ly/1M49gI8.

51 Tymur Vorona, "Украина — родина волонтеров, или как IT-добровольцы помогали стране в 2014 году," [Ukraine—the land of volunteers, or how IT-volunteers helped the country in 2014] *AIN*, Jaunary 8, 2015, http://ain.ua/2015/01/08/556357.

battalions, provide information and assistance to refugees, and help to those kidnapped by the pro-Russian militias. Citizen journalists also used open-source tools and data to track the presence of Russian troops[52] and military equipment in Ukraine.[53] More recently, projects such as LetMyPeopleGo[54] have campaigned online for the release of Ukrainian citizens held captive illegally in Russia and annexed Crimea, while activists with a new online initiative Dostupno.UA[55] have used social media to break the pervasive stereotypes about people with disabilities and integrate them into society. Many officials in the new Ukrainian go ernment use Facebook and Twitter heavily to report on their actions and reforms, and regularly engage with comments and take into account public opinion in their work, helping to increase accountability.[56]

Social media has also been used to bring taboo topics into public discussion. After the coverage period, in July 2016, Anastasiya Melnychenko launched the hashtag, #яНебоюсьСказати (#IAmNotAfraidToSayIt), sharing stories of the pervasive sexual harassment and abuse she experienced throughout her life. The hashtag was widely shared across social media, with thousands of women from Ukraine and Russia mobilizing to share their own stories, with the aim of shifting cultural attitudes in their countries which often dismiss or blame women for inviting sexual violence.[57]

Violations of User Rights

Authorities have increasingly cracked down on social media in an attempt to curb anti-Ukrainian rhetoric online, imprisoning users for so-called "separatist" or "extremist" expression. While physical violence against online commentators has declined overall, a number of troubling instances of violence occurred, including the murder of a renowned independent journalist after the coverage period in July 2016. Furthermore, the security of thousands of journalists was compromised in a leak of a database containing the personal information of accredited journalists reporting in eastern Ukraine. Key infrastructure in Ukraine, including Kiev's international airport, has also been targeted by cyberattacks initiated by foreign agents.

Legal Environment

The right to free speech is granted to all citizens of Ukraine under Article 34 of the constitution, although the article also specifies that the sta e may restrict this right in the interest of national security or public order. Part 3 of Article 15 of the constitution forbids state censorship. In practice, however, these rights have been frequently violated. Especially grave violations were observed in occupied parts of eastern Ukraine, where journalists and regular internet users faced attacks, kidnappings and extralegal intimidation for their reporting or for demonstrating pro-Ukrainian views.

52 Tetyana Bohdanova, "Outing the Russian Military in Eastern Ukraine," *Global Voices*, March 19, 2015, http://bit.ly/1O5Tp0r.

53 Aric Toler, "Fact Checking the Conflict in Eas ern Ukraine," *Global Voices*, March 3, 2015, http://bit.ly/1YRnKVo.

54 LetMyPeopleGo, https://www.facebook.com/LetMyPeopleGoUkraine.en/. Accessed on August 1, 2016.

55 Dostupno.UA, https://www.facebook.com/ДоступноUA-1617803701799770/. Accessed on August 1, 2016.

56 "Каких украинских министров можно читать в Facebook," [Which Ukrainian Ministers You Can Follow on Facebook] *AIN*, March 17, 2014, http://bit.ly/1OaG20h.

57 Anastasiya Melnychenko, "The woman who wasn't afraid to say it," *Meduza,* July 8, 2016, https://meduza.io/en/feature/2016/07/08/the-woman-who-wasn-t-afraid-to-say-it.

There is no specific law mandating criminal penalties or civil liability for ICT activities, but other laws, such as those penalizing extremist activity, terrorism or calls to separatism, apply to online activity. Article 109(2)-(3) of the Ukraine Criminal Code outlines jail terms of three to fi e years for threats to the territorial integrity and sovereignty of Ukraine.[58]

In October 2015, Ukrainian authorities announced the creation of a cyberpolice unit within the Ministry of Interior as part of a broader police reform.[59] The new unit has been tasked with neutralizing threats in the field f information and communication technologies and battling internet crime, including international money laundering schemes and digital piracy.

Prosecutions and Detentions for Online Activities

In 2015-2016, multiple internet users in Ukraine have been detained,[60] fine [61] and even imprisoned for up to fi e years for creating, running and moderating social media pages and accounts that the Ukrainian authorities found contained "calls to extremism or separatism" or otherwise threatened the territorial integrity of Ukraine. For example, a Ukrainian user in Chernihiv was sentenced in March 2016 to fi e years in prison for disseminating "materials calling for change of Ukrainian territory or state borders" online.[62]

In May 2016, journalist Ruslan Kotsaba was convicted of obstructing the activities of Ukraine's armed forces and sentenced to 3 years and 6 months in prison.[63] He had been arrested in February 2015 by Ukraine's Security Service on charges of treason (which were eventually changed) after he posted a YouTube video calling viewers to boycott the military mobilization in Ukraine.[64] Kostaba's arrest sparked heated debates about the balance between information security and freedom of speech online during an armed conflict. otsaba was released from prison on July 14, 2016, when his conviction was overturned in court,[65] after 18 months in detention.

Surveillance, Privacy, and Anonymity

The pervasiveness and legality of surveillance is unclear as very little information on this is openly available, and there is generally a lack of comprehensive legislative regulation of communication interception and surveillance. The Security Service of Ukraine can initiate criminal investigations and use wiretapping devices on communications, but existing legislation (for example, the Law on

58 Criminal Code of Ukraine (2001, Amended 2016), http://bit.ly/2fzpeqb.

59 Tetyana Lokot, "Watch Out, Internet! Ukraine Is Getting Its Own Cyberpolice," Global Voices, October 12, 2015. https://globalvoices.org/2015/10/12/watch-out-internet-ukraine-is-getting-its-own-cyberpolice/

60 "В Днепропетровске задержали администратора антиукраинских групп в соцсетях" [In Dnepropetrovsk, administrator of anti-Ukrainian social media groups detained], *Donbass News*, January 25, 2016, http://novosti.dn.ua/details/268168/.

61 "За пост в соцсети могут привлечь к уголовной ответственности" [A social network post could lead to criminal responsibility], *Jurliga*, February 23, 2016, http://jurliga.ligazakon.ua/news/2016/2/23/141787.htm.

62 "Мешканця Чернігова, який в інтернеті вів антиукраїнську пропаганду, посадили на 5 років" [Chernihiv resident who conducted anti-Ukrainian propaganda online jailed for fi e years], Institute of Mass Information, March 3, 2016, http://imi.org.ua/news/52544-meshkantsya-chernigova-yakiy-v-interneti-viv-antiukrajinsku-propagandu-posadila-na-5-rokiv.html.

63 "Коцабу не визнали зрадником, але дали 3,5 року в'язниці" [Kotsaba not pronounced a traitor, but gets 3.5 years in jail], *Ukrainska Pravda*, May 12, 2016, http://www.pravda.com.ua/news/2016/05/12/7108218/.

64 Aric Toler, "Ukraine Arrests Journalist on Treason Charges for Calls to Boycott Mobilization," *Global Voices*, February 9, 2015, http://bit.ly/1VqhlRL.

65 Halyna Coynash, "Controversial Ukrainian blogger / journalist Kotsaba freed after 18 months in prison," *Human Rights in Ukraine*, July 15, 2016, http://www.khpg.org/en/index.php?id=1468506145.

Operative Investigative Activity[66]) does not specify the circumstances that justify interception of information from communication channels nor the time limits of any such interception.

A proposal announced in April 2015 by the State Service on Special Communications and Information Security mandates that all mobile phone users, including those using prepaid packages, would have to register and disclose their personal data (such as their passport number) to mobile providers.[67] The committee that is working on the legal framework for the proposal claims it has received pressure from law enforcement to institute the measure, given the terrorist and security threats Ukraine currently faces. So far, only a draft of the proposal has been published on the government website,[68] though it has already caused widespread criticism from the industry and free speech advocates. There is currently no obligatory registration for either internet users or prepaid mobile phone subscribers, and users can purchase prepaid SIM-cards anonymously, as well as comment anonymously on websites where the website owner does not require registration.

From 2002 to 2006, mechanisms for internet monitoring were in place under the State Committee on Communications' Order No. 122, which required ISPs to install so-called "black-box" monitoring systems that would provide access to state institutions. This was ostensibly done to monitor the unsanctioned transmission of state secrets. Caving to pressure from public protests and complaints raised by the Internet Association of Ukraine and the Ukrainian Helsinki Human Rights Union, the Ministry of Justice abolished this order in August 2006. Since the revocation of Order No. 122, the service has acted within the limits prescribed by the Law on Operative Investigative Activity.

In December 2013 the NCCIR released a new edition of "Rules for Activities in the Sphere of Telecommunications," which included a problematic paragraph about ISPs and telecom providers having to "install at their own cost in their telecommunications networks all technical means necessary for performing operative and investigative activities by institutions with powers to do so."[69] Some human rights groups and internet associations were concerned that this step will aid the Security Services and the government in restricting internet freedoms by creating additional means of pressure that the government can exert over ISPs, however there is no information available on the extent to which these provisions have been implemented.[70]

Intimidation and Violence

The simmering conflict in eas ern Ukraine continues to be a source of pressure and threats against online activists and journalists, with a number of troubling instances of violence occurring during the coverage period, and the murder of a renowned independent journalist in July 2016 shocking the media community. Activists, bloggers, and regular internet users are still targeted for their work or pro-Ukrainian views by Russian-backed militants. Ukrainian and international journalists reporting on the conflict ha e also faced intimidation from Ukrainian nationalist partisan forces.

66 Law of Ukraine on Operative Investigative Activity, http://zakon5.rada.gov.ua/laws/show/2135-12. Accessed on August 1, 2016.

67 Stas Yurasov, "Мобільний зв'язок буде за паспортами," [Mobile communications to require passports] *Ekonomichna Pravda*, April 9, 2015, http://bit.ly/1FKSa5b.

68 State Service of Special Communications and Information Security of Ukraine, Проект постанови «Про внесення змін до Правил надання та отримання телекомунікаційних послуг [Draft decree "On introducing changes to Rules of providing and accepting telecommunications services"] accessed on May 1, 2015, http://bit.ly/1LmytDr.

69 NCCI, Rules for Activities in the Sphere of Telecommunications.

70 Oleg Shynkarenko, Зашморг на інтернет [A Noose on the Internet], *INSIDER*, January 8, 2014, http://www.theinsider.ua/business/52bac42dd8f4d/.

- Luhansk online journalist and activist Maria Varfolomeeva, who was being held by separatists since January 2015, was released in a prisoner swap with the Ukrainian authorities in March 2016.[71]

- In January 2016, the car of online investigative reporter Svetlana Kryukova (of Strana.ua website) was smashed and its tires cut in a parking lot near her office [72] Kryukova connected the attack to her investigative work on Ukrainian politician Gennady Korban.

- In May 2016, Ukrainian nationalist activist website "Mirotvorets" (Peacemaker) published a leaked list of names and contact details of thousands of journalists who have received accreditation to report in the self-proclaimed "Donetsk People's Republic," branding them "accomplices of terrorists."[73] The doxing caused widespread consternation among the international media community,[74] but was met with little criticism among Ukrainian officials, some of whom, including Minister of Internal Affairs Arsen Avakov, applauded the partisan move. Several of the journalists from the list have received threats[75] and noted that the leak obstructed their efforts to report objectively on the conflict in eas ern Ukraine. Kyiv Prosecutor's Office in Ukraine has opened a criminal in estigation into the website's actions.

- In May 2016, Anatoliy Ostapenko, a journalist affilia ed with independent online TV outlet Hromadske Zaporizhzhya, was assaulted in the eastern city of Zaporizhzhya. Ostapenko had reportedly been working on investigations linking local authorities to corruption.[76]

- On July 20, 2016, Pavel Sheremet, a veteran Belarusian journalist working for Ukraine's *Ukrainska Pravda* website, was killed in a car bomb explosion[77] in the Ukrainian capital Kyiv. Sheremet, who had worked in Belarus, Russia and Ukraine, had previously endured state pressure and jail time for his reporting, which was often critical of political leaders. Although the investigation into his death is still ongoing, Sheremet's colleagues at *Ukrainska Pravda* believe his murder was retribution for his professional activity.[78]

Technical Attacks

A new wave of cyberattacks in Ukraine signifies the continued attle between pro-Russian and Ukrainian nationalist partisans. Hacker collectives like the pro-Russian "Cyber-Berkut," and the

71 "Мария Варфоломеева на свободе (стрим)" [Maria Varfolomeeva is free (stream)], *Kharkiv Crisis Infocenter*, March 3, 2016, http://civilforum.com.ua/infotsentr/5632-mariya-varfolomeeva-na-svobode-strim.html.

72 "Журналистка Крюкова заявила, что неизвестные разбили ее автомобиль" [Journalist Kryukova says unknown persons have smashed her car], *Ukrainska Pravda*, January 11, 2016, http://www.pravda.com.ua/rus/news/2016/01/11/7095063/.

73 Aric Toler, Tetyana Lokot, "Ukrainian Activists Leak Personal Information of Thousands of War Reporters in the Donbas," *Global Voices*, May 11, 2016, https://globalvoices.org/2016/05/11/ukrainian-activists-leak-personal-information-of-thousands-of-war-reporters-in-the-donbas/.

74 "Journalists fight ack against Ukrainian activists who doxed thousands of war correspondents in the Donbas," *Meduza*, May 11, 2016, https://meduza.io/en/news/2016/05/11/open-letter-demands-ukrainian-action-over-publication-of-undercover-journalists-information.

75 Halya Coynash, "Ukrainian journalist who twice confronted Putin targeted by Myrotvorets Centre vigilantes," *Human Rights in Ukraine*, May 25, 2016, http://www.khpg.org/en/index.php?id=1464127138.

76 Freedom House press release, "Ukrainian journalist from independent outlet attacked," May 24, 2016, http://bit.ly/2eEg3Qa.

77 Christopher Miller, "Prominent Belarusian-Born Journalist Pavel Sheremet Killed In Kyiv Car Blast," *Radio Liberty*, July 20, 2016, http://www.rferl.org/a/ukraine-journalist-pavel-sheremet-killed-car-bomb/27868777.html.

78 Alec Luhn, "Car bomb kills pioneering journalist Pavel Sheremet in Kiev," *The Guardian*, July 20, 2016, https://www.theguardian.com/world/2016/jul/20/ukraine-journalist-pavel-sheremet-killed-kiev-car-bombing.

nationalist "Ukrainian Cyber Forces" continued to deface websites and leak information belonging to their perceived foes.

There were also several hacking attacks on Ukrainian infrastructure, targeting power systems and transportation systems in the country. In December 2015, an attack on a powerplant owned by the electric company Prykarpattyaoblenergo in Ukraine's western Ivano-Frankivsk region led to a power blackout affecting about 80,000 citizens.[79] Both Ukraine's state security service and independent Western researchers have blamed Russian hackers for the attack, although it was not clear if the hackers were working at the behest of the Russian government. A January 2016 malware attack targeting the air traffic cont ol system of Kyiv's main Boryspil airport was also said to have originated from a server within Russia, with connections to the same hacker group. [80]

In March 2016, President Petro Poroshenko established a National Cybersecurity Coordination Centre within the National Security and Defense Council[81] as part of the country's new cybersecurity strategy shaped by external threats, many of them coming from Russia.

79 Tetyana Lokot, "Russian Hackers Behind Attack on Ukraine's Power Grid, Researchers Claim," *Global Voices*, January 8, 2016, https://globalvoices.org/2016/01/08/russian-hackers-behind-attack-on-ukraines-power-grid-researchers-claim/.

80 Pavel Polityuk, Alessanda Prentice, "Ukraine says to review cyber defenses after airport targeted from Russia," *Reuters*, January 18, 2016, http://www.reuters.com/article/us-ukraine-cybersecurity-malware-idUSKCN0UW0R0.

81 Maya Yarovaya, "Порошенко утвердил стратегию кибербезопасности Украины и создание координационного центра кибербезопасности при СНБО" [Poroshenko finalizes Ukraine s cybersecurity strategy and creation of coordination center for cybersecurity within NSDC], *AIN*, March 17, 2016, http://ain.ua/2016/03/17/638654.

Freedom House

United Kingdom

	2015	2016
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	2	2
Limits on Content (0-35)	6	5
Violations of User Rights (0-40)	16	16
TOTAL* (0-100)	**24**	**23**

* 0=most free, 100=least free

Population:	**65.1 million**
Internet Penetration 2015 (ITU):	**92 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2016 Status:	**Free**

Key Developments: June 2015 – May 2016

- The Investigatory Powers Bill was introduced in March 2016 to consolidate and reform government surveillance laws, but critics said it lacked adequate privacy safeguards; it was still being debated in parliament in mid-2016 (see **Surveillance, Privacy, and Anonymity**).
- In March 2016, the Crown Prosecution Service in England and Wales issued guidelines for offenses related to social media, particularly online harassment (see **Legal Environment**).
- On February 16, 2016, Police Scotland arrested a man who made controversial Facebook posts about Syrian refugees (see **Prosecutions and Detentions for Online Activities**).

Editor's Note

On June 23, 2016, outside the coverage period of this report, citizens of the United Kingdom voted to leave the European Union in a closely contested popular referendum. Prime Minister David Cameron resigned as leader of the ruling Conservative Party. He was replaced by Teresa May, who was previously the home secretary, in July.

Introduction

Internet freedom improved slightly, with few reports of political and social websites blocked by mistake, though transparency about content controls remains lacking. Online harassment, extremist speech, and privacy remained priority issues in the United Kingdom's internet policy in 2015 and 2016.

The UK has consistently been an early adopter of new information and communication technologies (ICTs). Internet access is rapidly approaching universal, with competitive prices and generally fast speeds. Mobile devices, especially smartphones, have become the most prevalent means of internet access.

Strategies to combat extremist as well as offensive speech online periodically threaten to curb legitimate expression. At least two people were briefly detained following de ogatory—though nonviolent—social media posts during the coverage period of this report. In February 2016, police were called to a school in Southampton by staff who reported a 15-year-old pupil for accessing the website of the populist right-wing United Kingdom Independence Party, concerned about the site's views on immigration and other matters.

The past year saw fie ce debate regarding surveillance powers. In June 2015, the Investigatory Powers Tribunal identified ir egularities in the Government Communications Headquarters (GCHQ) intelligence agency's handling of communications data intercepted from two civil society groups, Amnesty International and the South Africa-based Legal Resources Center. The tribunal ruled that those irregularities violated human rights standards, though the interception itself was lawful. In February 2016, in a separate case, the tribunal ruled that GCHQ computer network exploitation or hacking activities were also lawful.

However, an independent report commissioned by the government and released in June 2015 called the existing legislative framework on surveillance "undemocratic, unnecessary and—in the long run—intolerable." On March 1, 2016, the government introduced the Investigatory Powers Bill to consolidate and reform surveillance laws. The polarizing piece of legislation was criticized for authorizing overreaching surveillance and undermining privacy. In mid-2016, it was still being debated in parliament.

Obstacles to Access

Access to the internet is considered to be a key element determining societal and democratic participa-

tion in the UK.[1] ICT infrastructure is generally strong, allowing high levels of access. The overwhelming majority of UK citizens use the internet frequently on a widening variety of devices, particularly smartphones.[2] In recent years, substantial investments led by the government have led to better levels of service for many citizens and businesses. For financial and literacy reasons, those over the age of 75 and people in the lowest socioeconomic groups still lack access.[3] Policies and regulation in the country tend to favor access, although continuing revelations regarding extensive government surveillance practices may impact how citizens choose to access the internet.

Availability and Ease of Access

Internet penetration was reported at 87 percent, with the share of homes with fi ed and mobile broadband at 80 percent.[4] At the beginning of 2016, there were 24.4 million fi ed broadband connections, representing a 4 percent increase over the previous year.[5] The average broadband speed in 2014 was 22.8 Megabits per second (Mbps) according to an August 2015 report,[6] continuing a trend of rising speeds and growing satisfaction among consumers served by faster fibe -optic based services. Nearly 100 percent of all households are within range of ADSL connections.

While broadband access is effectively ubiquitous, steady progress continues towards the expansion of "superfast" broadband that has an advertised speed of at least 30 Mbps.[7] In 2015, 30 percent of all broadband connections were superfast, compared to 0.2 percent in 2009.[8] Funding for a government superfast broadband program, which is aimed at improving broadband speed and access, expanded to GBP 1.7 billion (US$ 2.62 billion).[9] In early 2015, an additional 2,411,395 premises had access to superfast broadband through the scheme, meaning a total of 80 percent of all UK premises had superfast broadband access availability, in line with a target of 95 percent by 2017.[10] A voucher scheme covering up to GBP 3,000 (US$ 4,440) of installation costs for small and medium enterprises has been in place in 50 British cities since April 2015.[11]

Mobile telephone penetration is extensive, with a reported penetration rate of 125 percent at the

1 Ofcom, *Internet Citizens 2014* (London: Ofcom), November 27, 2014, http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/Internet_Citizens_Report_14.pdf, p 1.

2 Ofcom, *The Communications Market Report*, August 6, 2015, http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr15/CMR_UK_2015.pdf, p.1

3 Ofcom, *Internet Citizens 2014*, p.11.

4 Ofcom, *Adults' media usage and attitudes*, April 2016, http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/adults-literacy-2016/2016-Adults-media-use-and-attitudes.pdf. The International Telecommunication Union reported penetration at 92 percent of the population aged 16 to 74 in 2015. See, International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1cblxxY.

5 Ofcom, "Telecommunications market data tables Q3 2015," January 26, 2016, http://stakeholders.ofcom.org.uk/binaries/research/cmr/telecoms/Q3-2015.pdf p.2.

6 Ofcom, *The Communications Market Report* 2015, p.15. Akamai reported average connection speeds of 14.9 Mbps in 2016. See, "'First Quarter, 2016 State Of The Internet Report," June 29, 2016, https://www.akamai.com/us/en/about/news/press/2016-press/akamai-fi st-quarter-2016-state-of-the-internet-connectivity-report.jsp.

7 For local area progress in broadband provision, see DCMS, *Table of local broadband projects*, October 2014, https://docs.google.com/spreadsheet/ccc?key=0Ah3sVRjT82kKdEltX0lJNjNVWWhNbjBnNGwxeHhqMHc#gid=0.

8 Ofcom, *The Communications Market Report* 2015, p3.

9 Department for Culture, Media and Sport (DCMS), *2010 to 2015 government policy: broadband investment*, updated May 8, 2015, https://www.gov.uk/government/publications/2010-to-2015-government-policy-broadband-investment, Appendix 2.

10 DCMS, *2.5 million more UK homes and businesses can now go superfast*, https://www.gov.uk/government/news/25-million-more-uk-homes-and-businesses-can-now-go-superfast .

11 DCMS, *2.5 million more UK homes and businesses can now go superfast* note 12.

end of 2015.[12] The introduction of faster fourth-generation (4G) services in 2012 encouraged video streaming and access to other data services. All national mobile network operators offered 4G mobile communication technology, with outdoor 4G coverage from at least one network accessible in over 89 percent of UK premises.[13] In 2016, 66 percent of adults reported a smartphone was their primary device for accessing the internet,[14] and reported valuing their smartphone over any other communication or media device;[15] indeed the smartphone was identified as the prima y device for access in fi e out of nine online activities.[16]

The UK provides a competitive market for internet access, and prices for communications services compare favorably with those in other countries, with the scope of services increasing while prices continue to fall and remain competitive.[17] The average British household spent GBP 81.30 (US$ 125) per month on telecommunication services in 2014, a decrease of 0.1 percent from 2013.[18] The difference between superfast and standard services in 2014 was between GBP 5 (US$ 7.66) and GBP 10 (US$ 15.31) per month.[19] While 4G services were initially more expensive than non-4G services, the difference is shrinking, and in some cases disappearing. The price basket of mobile services fell by 0.4 percent in 2014.[20]

People in the lowest income groups are significantly less li ely to have home internet subscriptions, with the gap between socioeconomic groups remaining the same for the past few years. In 2014, only 63 percent of individuals over the age of 65 used the internet, and among those in the lowest socioeconomic group, including unskilled laborers and long-term state dependents, only 64 percent self-describe as internet users.[21] However, in 2016, it was found that use in the 65 to 74 age group has increased by nearly 70 percent since 2011.[22] Of the 15 percent of adults without household internet access, 12 percent reported having no intention to get connected.[23] There is a no general gender gap in internet use though two-thirds of women over 75 have never used the internet.[24]

Restrictions on Connectivity

The government does not place limits on the amount of bandwidth ISPs can supply, and the use of internet infrastructure is not subject to direct government control. ISPs regularly engage in traffic shaping or slowdowns of certain services (such as peer-to-peer file sharing and elevision streaming).

12 International Telecommunication Union, *Mobile-cellular subscriptions 2000-2015*, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

13 Ofcom, *The Communications Market Report* 2015, p.1.

14 Ofcom, *Adults' media usage and attitudes*, April 2016 http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/adults-literacy-2016/2016-Adults-media-use-and-attitudes.pdf.

15 Ofcom, *Adults' media usage and attitudes*, April 2016 http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/adults-literacy-2016/2016-Adults-media-use-and-attitudes.pdf.

16 Ofcom, *Adults' media usage and attitudes*, April 2016 http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/adults-literacy-2016/2016-Adults-media-use-and-attitudes.pdf.

17 Ofcom, *The Consumer Experience of 2015: Research Report*.

18 Ofcom, *The Communications Market Report 2015*, p. 304.

19 Ofcom, *The Communications Market Report 2015*, p. 303.

20 Ofcom, *The Communications Market Report* 2015, p.317.

21 Ofcom, *Internet Citizens 2014*.

22 Office for National tatistics, "Internet users in the UK 2016," May 20, 2016, https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2016.

23 Ofcom, *The Communications Market Report* 2015, p.352.

24 Office for National tatistics, "Internet users in the UK 2016," p. 2.

Mobile providers have cut back on previously unlimited access packages for smartphones, reportedly because of concerns about network congestion.

ICT Market

The fi e major internet service providers (ISPs) are British Telecom (BT) with a 32 percent market share, Sky (22 percent), Virgin Media (20 percent), TalkTalk (14 percent), and EE (4 percent).[25] Through local loop unbundling—where communications providers offer services to households using infrastructure provided mainly by BT and Virgin—a wider number of companies provide internet access. Unbundled fi ed-lines reached 9.6 million homes in 2015, a 0.2 percent increase since the previous year.[26] At the time of this report, 95 percent of homes are able to receive unbundled telecommunications services.[27]

ISPs are not subject to licensing but must comply with general conditions set by the communications regulator, Ofcom, such as having a recognized code of practice and being a member of a recognized alternative dispute-resolution scheme.[28]

The telecommunications provider EE leads the mobile operator market, with some 33 percent of market, followed by O2 (21 percent), Vodafone (18 percent), Three (10 percent), and Tesco (8.5 percent) according to information from Statista as of June 2015.[29] Mobile Virtual Network Operators, including Tesco, provide service using the infrastructure of one of the other four.

Regulatory Bodies

Ofcom is the primary regulator, by virtue of the broad definitions f responsibility for "citizens," "consumers," and "communications matters" granted to it under the Communications Act 2003.[30]

In 2012, major ISPs published a "Voluntary Code of Practice in Support of the Open Internet".[31] The code commits ISPs to transparency and confi ms that traffic management practices will not be used to target and degrade the services of a competitor. The code was amended in 2013 to clarify that signatories could deploy content fil ering or provide such tools where appropriate for public Wi-Fi access.[32]

In 2013, the domain registrar Nominet reviewed the extent to which the ".uk" domain registration policy should restrict offensive or otherwise inappropriate words or expressions in domain name

25 Ofcom, *The Communications Market Report* 2015, p.292.

26 Ofcom, *The Communications Market Report 2015*, p. 283.

27 Ofcom, *The Communications Market Report 2015*, p. 282.

28 Ofcom, *Consolidated Version of General Conditions of Entitlement* (London: Ofcom), December 16, 2013, http://stakeholders.ofcom.org.uk/binaries/telecoms/ga/GENERAL_CONDITIONS_AS_AT_26_DECEMBER_2013.pdf.

29 "Market share held by mobile operators in the United Kingdom (UK) as of June 2015," Statista, http://www.statista.com/statistics/375986/market-share-held-by-mobile-phone-operators-united-kingdom-uk/.

30 Communications Act 2003, Part 1, Section 3, http://www.legislation.gov.uk/ukpga/2003/21/contents.

31 Broadband Stakeholder Group, "ISPs launch Open Internet Code of Practice," July 25, 2012, http://www.broadbanduk.org/2012/07/25/isps-launch-open-internet-code-of-practice/.

32 Broadband Stakeholder Group, "ISPs launch Open Internet Code of Practice," May 2013, http://www.broadbanduk.org/wp-content/uploads/2013/06/BSG-Open-Internet-Code-of-Practice-amended-May-2013.pdf.

registrations.[33] The Nominet Board agreed to all the recommended changes,[34] which included a post-registration domain name screening to suspend or remove domain names that encourage serious sexual offenses.[35]

Other groups regulate content through voluntary ethical codes and co-regulatory rules under independent oversight. The Internet Watch Foundation (IWF), an independent self-regulatory body funded by the European Union (EU) and industry bodies manages criminal online content (see Blocking and Filtering).[36] The Video On Demand Association, a private self-regulatory body, had previously regulated video content in keeping with the EU AudioVisual Media Services Directive. This function has been taken over by Ofcom.[37] The Advertising Standards Authority and the Independent Press Standards Organization regulate newspaper websites. With the exception of child abuse content, these bodies eschew pre-publication censorship and operate post-publication notice and takedown procedures within the E-Commerce Directive liability framework (see Content Removal).

Limits on Content

Various categories of criminal content such as depictions of child sexual abuse, promotion of extremism and terrorism, and copyright infringing materials are blocked by UK ISPs. Parental controls over content considered unsuitable for children are enabled by default on mobile networks, requiring adults to opt out to access adult material. These measures can result in overblocking, and a lack of transparency persists regarding the processes involved and the kind of content affected.

Blocking and Filtering

Service providers block and fil er some illegal and some legal content in the UK, with varying degrees of transparency. Illegal content falls into three categories. First, ISPs block potentially illegal content depicting child sexual abuse. Second, overseas-based URLs hosting content police report for violating the Terrorism Act 2006 by glorifying or promoting terrorism are included in the child fil ers supplied by many ISPs, and inaccessible in schools, libraries, and other facilities considered part of the "public estate." The list of sites in these two categories is kept from the public to prevent access to unlawful materials. Finally, ISPs are also required to block domains and URLs found to be hosting material that infringes copyright when ordered by the High Court. Those orders are not kept from the public, but can be hard to obtain.[38]

Separately, all mobile service providers and some ISPs providing home service fil er legal content considered unsuitable for children. Mobile service providers enable these fil ers by default, requiring customers to prove they are over 18 to access the unfil ered internet. In 2013, the four largest ISPs agreed with the government to present all customers with an "unavoidable choice" about whether

33 Nominet is the domain registrar in the United Kingdom, and manages access to the .uk, .wales, and .cymru domains.

34 Lord Macdonald QC, *Review of .uk Registration Policy*, December 2013, http://www.nominet.org.uk/sites/default/files Lord%20Macdonald%20Report%20final.pd .

35 Nominet, "Nominet to update registration policy in light of Lord Macdonald review," 15 January 2014, http://www.nominet.org.uk/news/latest/nominet-update-registration-policy-light-lord-macdonald-review.

36 The Internet Watch Foundation, https://www.iwf.org.uk/.

37 DigitalTV Europe, "Ofcom to take over VoD regulation from ATVOD" 14 October 2015, http://www.digitaltveurope.net/443191/ofcom-to-take-over-vod-regulation-from-atvod/.

38 451 Unavailable, "UK Blocking Orders," https://www.451unavailable.org/uk-blocking-orders/.

to enable parentally controlled fil ers.[39] Civil society groups say those fil ers lack transparency and affect too much legitimate content, making it hard for consumers to make informed choices, and for content owners to appeal.

ISPs block URLs using content fil ering technology known as Cleanfeed, which was developed by BT in 2004.[40] In 2011, a judge described Cleanfeed as "a hybrid system of IP address blocking and DPI-based URL blocking which operates as a two-stage mechanism to fil er specific in ernet traffic" While the process involves deep packet inspection (DPI), a granular method of monitoring traffic that enables ISPs to block individual URLs rather than entire domains, it does not enable "detailed, invasive analysis of the contents of a data packet," according to the judge's description. Other, similar systems adopted by ISPs besides BT are also "frequently referred to as Cleanfeed," the judge wrote.[41]

ISPs are notified about ebsites hosting content that has been determined to break, or potentially break UK law under different procedures:

- The Internet Watch Foundation (IWF) compiles a list of specific URLs containing pho o-graphic or computer-generated depictions of child sexual abuse or criminally obscene adult content to distribute to ISPs and other industry stakeholders who support the foundation through membership fees.[42] ISPs block those URLs in accordance with a voluntary code of practice set forth by the Internet Services Providers' Association (see Regulatory Bodies). IWF analysts evaluate sites hosting material that potentially violate a range of UK laws,[43] in accordance with a Sexual Offences Definiti e Guideline published by the Sentencing Council under the Ministry of Justice.[44] The IWF recommends that ISPs notify customers why the site is inaccessible,[45] but some have returned error messages instead.[46] The IWF website allows site owners to appeal their inclusion on the list. Citizens can also report criminal content via a hotline. In 2008, the IWF blacklisted a Wikipedia page displaying an album cover depict-ing a naked girl based on a complaint submitted by a reader. Other Wikipedia users report-ed that the block affected their ability to edit the site's user-generated content,[47] and the IWF subsequently removed the page from the list.[48] An independent judicial review of the human rights implications of IWF's operations conducted in 2014 said the body's work was consistent with human rights law.[49] The review recommended some improvements, such as restricting its remit to child sexual abuse, and appointing a human rights expert.

39 Ofcom, "Ofcom report on internet safety measures," December 16, 2015, http://stakeholders.ofcom.org.uk/binaries/internet/fourth_internet_safety_report.pdf

40 Martin Bright, "BT puts block on child porn sites," *The Guardian*, June 6, 2004, https://www.theguardian.com/technology/2004/jun/06/childrensservices.childprotection; "TCP Reset is sent back to the customer instead of content," *The Guardian,* December 8, 2008, https://www.theguardian.com/technology/blog/2008/dec/08/internet-censorship-wikipedia-diagram; Open Rights Group Wiki, "Cleanfeed," https://wiki.openrightsgroup.org/wiki/Cleanfeed.

41 [2011] EWHC 1981 (Ch), accessible: http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/28_07_11_bt_newzbin_ruling.pdf.

42 Internet Watch Foundation, "URL List Policy," https://www.iwf.org.uk/members/member-policies/url-list.

43 Internet Watch Foundation, "Laws Relating to the IWF's Remit," https://www.iwf.org.uk/hotline/the-laws.

44 Sentencing Council, Sexual Offences Definiti e Guideline, https://www.sentencingcouncil.org.uk/wp-content/uploads/Final_Sexual_Offences_Definiti_e_Guideline_content_web1.pdf.

45 Internet Watch Foundation, "Blocking: Good Practice," https://www.iwf.org.uk/members/member-policies/url-list/blocking-good-practice.

46 Open Rights Group Wiki, "Cleanfeed," https://wiki.openrightsgroup.org/wiki/Cleanfeed.

47 BBC News, "Wikipedia child image censored," December 8, 2008, http://news.bbc.co.uk/2/hi/uk_news/7770456.stm.

48 ISP Review, "Internet Watch Foundation U-Turns on Wikipedia Block," December 10, 2008, http://www.ispreview.co.uk/news/EkklIAlVuVbKzPsVgN.html.

49 "IWF audited on human right," January 27, 2014, https://www.iwf.org.uk/about-iwf/news/post/380-iwf-audited-on-human-rights.

- The police Counter Terrorism Internet Referral Unit compiles a list of URLs hosted overseas containing material considered to glorify or incite terrorism under the Terrorism Act 2006,[50] which are fil ered on networks of the public estate, such as schools and libraries; they can still be accessed on private computers.[51] In 2014, the four largest ISPs, BT, Virgin, Sky, and TalkTalk, said they would also fil er this content from children and young internet users.[52]

- The UK High Court can order ISPs to block websites found to be infringing copyright under the Copyright, Designs, and Patents Act 1988. The High Court has held that publishing a link to copyright infringing material, rather than actually hosting it, does not amount to an infringement;[53] this approach was confi med by the Court of Justice of the European Union.[54] In October 2014, a new intellectual property framework included exceptions for making personal copies of protected work for private use, as well as for "parody, caricature and pastiche."[55] Sections 17 and 18 of the Digital Economy Act (DEA) of 2010 separately allowed for the courts to order websites containing "substantial" violations of copyright to be blocked. In August 2011, the government announced that the DEA's blocking provisions would be dropped, in part because it was already authorized under another law.[56] Copyright-related blocking has been criticized for its inefficiency and lack f transparency. In May 2010, an Ofcom review determined that the practice is unlikely to be effective unless used in conjunction with other measures.[57] During the coverage period, the High Court ordered six ISPs to ban dozens of sites that copied or mirrored the content available on sites that had been blocked in the past.[58] After lobbying from the London-based Open Rights Group, in December 2014 BT, Sky, and Virgin Media began informing visitors to sites blocked by court order that the order can be appealed with the High Court.[59]

Mobile service providers also block URLs identified by the IWF as containing po entially illegal content. However, Mobile UK (formerly the Mobile Broadband Group), an industry group which consists of Vodafone, Three, EE, and O2,[60] introduced additional fil ering of content considered unsuitable for children in a code of practice published in 2004 and last updated in July 2013.[61] These child fil ers are enabled by default in mobile internet browsers, though users can disable them by verifying they

50 Open Net Initiative, "United Kingdom," December 18, 2010, https://opennet.net/research/profiles/uni ed-kingdom#footnote47_syc8fbo; Terrorism Act 2006, http://www.legislation.gov.uk/ukpga/2006/11/pdfs/ukpga_20060011_en.pdf.

51 What do they Know, attachment to the Freedom of Information request "Current status of terrorist internet fil ering," June 28, 2013, https://www.whatdotheyknow.com/request/160774/response/404100/attach/html/3/attachment.pdf.html

52 Patrick Wintour, "UK ISPs to introduce jihadi and terror content reporting button," *The Guardian,* November 13, 2014, https://www.theguardian.com/technology/2014/nov/14/uk-isps-to-introduce-jihadi-and-terror-content-reporting-button

53 *Paramount Home Entertainment International Ltd v British Sky* Broadcasting Ltd [2013] EWHC 3479 (Ch). For instances where the individual is merely browsing the content, the Supreme Court has held that this does not amount to an infringement. *PRCA v The Newspaper Licensing Agency Limited* [2013] UKSC 18.

54 Case C-466/12 *Svensson and others v Retreiver Sverige,* full judgement at: http://curia.europa.eu/juris/document/document.jsf?docid=147847&doclang=EN

55 "Major reform of intellectual property comes into force," UK Department for Business, Innovation and Skills, September 30, 2014, https://www.gov.uk/government/news/major-reform-of-intellectual-property-comes-into-force.

56 BBC News, "Government drops website blocking," August 3, 2011, http://www.bbc.com/news/technology-14372698.

57 Ofcom, "Site blocking" to reduce online copyright infringement," May 27, 2010 http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf.

58 "UK ISPs Unleash 85+ New Blocks on 'Pirate' Domains" *Torrent Freak,* December 14, 2015, https://torrentfreak.com/uk-isps-unleash-85-new-blocks-on-pirate-domains-151214/.

59 Jim Killock, "Website blocking orders made more transparent," Open Rights Group, December 5, 2014, https://www.openrightsgroup.org/blog/2014/website-blocking-orders-made-more-transparent.

60 Mobile UK, "Who we are," http://www.mobilebroadbandgroup.com/about-mobile-uk.html

61 Mobile Broadband Group, "UK Code of practice for the self-regulation of content on mobiles," version 3, July 1, 2013, http://www.mobilebroadbandgroup.com/documents/UKCodeofpractice_mobile_160515.pdf

are over 18. Mobile Virtual Network Operators are believed to "inherit the parent service's fil ering infrastructure, though they can choose whether to make this available to their customers."[62] Transparency about what content is affected depends on the provider. O2 allows its users to check how a particular site has been classified [63]

The fil ering is based on a classification frame ork for mobile content published by the British Board of Film Classification (BBFC) [64] Definitions f content the BBFC considers suitable for adults only include "the promotion, glamorization or encouragement of the misuse of illegal drugs;" "sex education and advice which is aimed at adults;" and "discriminatory language or behavior which is frequent and/or aggressive, and/or accompanied by violence and not condemned," among others. The BBFC adjudicates appeals from content owners about overblocking and publishes the results quarterly.[65]

The four largest ISPs, BT, Sky, Virgin Media and TalkTalk, offer all customers the choice to activate similar fil ers to protect children under categories that vary by provider, but can include social networking, games, and sexual education.[66] Website owners can check whether their site is fil ered under one or more category, or report overblocking, by emailing the industry-backed nonprofit g oup Internet Matters,[67] though the process and timeframe for correcting mistakes varies by provider.

These optional fil ers can affect a range of legitimate content including public health, homosexuality, drug awareness, and pages run by civil society groups and political parties. In 2012, O2 customers were temporarily unable to access the website of the right-wing nationalist British National Party.[68] Civil society groups also have criticized the subjectivity of the content selected for fil ering. A 2014 magazine article noted that all the ISPs had blocked dating sites with the exception of Virgin Media, which operates one.[69] During the coverage period of this report, an Ofcom report said that the ISPs include "proxy sites, whose primary purpose is to bypass fil ers or increase user anonymity, as part of their standard blocking lists."[70] Transparency about the process remains lacking. In August 2015, when a watchmaking business complained to BT that their company website was blocked by its Parental Control software, the provider responded that the process had been outsourced to "an expert third party," and that BT was "not involved."[71]

Blocked!, a site operated by the Open Rights Group, allows users to test the accessibility of websites and report overblocking of content by both home broadband and mobile internet providers.[72] In mid-2016, the website listed 11,715 sites blocked by default fil ers, meaning a user would have

62 Blocked! "Frequently Asked Questions," https://www.blocked.org.uk/faq.

63 O2, "Site Checker," http://urlchecker18plus.o2.co.uk/.

64 BBFC, "Mobile Content: Framework," http://www.bbfc.co.uk/what-classification/mobile-con ent/framework. In 2013, the British Board of Film Classification ook over this function from the Independent Mobile Classification Bod . See, BBFC, "BBFC replaces the Independent Mobile Classification B ard (IMCB) as the regulation framework provider for mobile internet content," July 1, 2013, http://www.bbfc.co.uk/about-bbfc/media-centre/bbfc-replaces-independent-mobile-classification-b ard-imcb-regulation.

65 BBFC, "Quarterly Report," http://www.bbfc.co.uk/what-classification/mobile-con ent/quarterly-report.

66 Ofcom, "Ofcom report on internet safety measures."

67 https://www.internetmatters.org/parental-controls/info-site-owners/

68 Thomas Brewster, O2 blocks BNP website as 'hate site', *Tech Week Europe,* May 18, 2012, http://www.techweekeurope.co.uk/workspace/o2-blocks-bnp-website-as-hate-site-78653.

69 Steven Mackenzie, "Internet Access: Are You Being Subjected To 'Private Sector Censorship?'" *The Big Issue,* September 10, 2014, http://www.bigissue.com/features/4323/internet-access-are-you-being-subjected-to-private-sector-censorship.

70 Ofcom, "Ofcom report on internet safety measures."

71 Blocked! "The personal cost of fil ers," https://www.blocked.org.uk/personal-stories.

72 Blocked! "Are you being blocked?" https://www.blocked.org.uk/.

to proactively disable the fil er in order to view the content affected. A further 21,239 sites were blocked by fil ers which users enable by choice.

Content Removal

Material blacklisted by the IWF because it constitutes a criminal offense (see Blocking and Filtering) can also be subject to removal. When the content in question is hosted on servers in the UK, the IWF coordinates with police and local hosting companies to have it taken down. For content that is hosted on servers overseas, the IWF coordinates with international hotlines and police authorities to get the offending content taken down in the host country. Similar processes are in place for the investigation of online materials inciting hatred under the oversight of TrueVision, a site that is managed by the police.[73]

The Terrorism Act calls for the removal of online material hosted in the UK if it "glorifies or praises" terrorism, could be useful to conducting terrorism, or incites people to carry out or support terrorism. A Counter Terrorism Internet Referral Unit (CTIRU) was set up in 2010 to investigate internet materials and take down instances of "jihadist propaganda."[74] The CTIRU compiles lists of URLs hosting such material outside its jurisdictions, which are then passed on to service providers for voluntary fil ering (see Blocking and Filtering). In June 2015, Home Secretary Theresa May said the unit was taking down "about 1,000 pieces of terrorist-related material per week."[75]

According to EU Directive 2000/31/EC (the E-Commerce Directive), website owners and companies who knowingly host illicit material and fail to remove it may held liable, even if the content was created by users.[76] While that directive applies to libelous content, updates to the Defamation Act effective since January 1, 2014 provide greater protections for companies by limiting their liability for user-generated content that is considered defamatory.

However, the Defamation Act offers protection to website operators from private libel suits based on third-party postings only if the victim alleging defamation can find the user esponsible.[77] While the act does not specify what sort of information the website operator must provide to plaintiffs, unauthenticated identity information may be falsified by use s and prevent the operator from benefiting f om the act's liability protections, thus placing website operators in the position of requiring authenticated identity information or risk civil liability.[78]

In May 2014, European Court of Justice gave search engines the task of removing links from their

73 True Vision, "Internet Hate Crime," http://www.report-it.org.uk/reporting_internet_hate_crime.

74 "2010 to 2015 government policy: counter-terrorism," Gov.UK, May 8, 2015, https://www.gov.uk/government/publications/2010-to-2015-government-policy-counter-terrorism/2010-to-2015-government-policy-counter-terrorism; National Police Chiefs Council, "The Counter Terrorism Internet Referral Unit," http://www.npcc.police.uk/NPCCBusinessAreas/PREVENT/TheCounterTerrorismInternetReferralUnit.aspx.

75 They Work For You, House of Commons Debate, June 11, 2015, c1367, https://www.theyworkforyou.com/debates/?id=2015-06-11c.1353.0#g1367.1.

76 Legislation at: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32000L0031.

77 Mike Masnick, "Did UK Gov't Already effectively Outlaw Anonymity Online With Its New Defamation Law?," *TechDirt*, August 11, 2014, https://www.techdirt.com/articles/20140807/17234928145/did-uk-govt-already-effectively-outlaw-anonymity-online-with-its-new-defamation-law.shtml.

78 Eric Goldman, "UK's New Defamation Law May Accelerate The Death of Anonymous User-Generated Content Internationally," Forbes, Sept. 9, 2014, http://www.forbes.com/sites/ericgoldman/2013/05/09/uks-new-defamation-law-may-accelerate-the-death-of-anonymous-user-generated-content-internationally/; Mike Masnick, "Did UK Gov't Already effectively Outlaw Anonymity Online With Its New Defamation Law?," TechDirt, Aug. 11, 2014, https://www.techdirt.com/articles/20140807/17234928145/did-uk-govt-already-effectively-outlaw-anonymity-online-with-its-new-defamation-law.shtml.

search results at the request of individuals if the stories in question were deemed to be inadequate or irrelevant. The so-called "right to be forgotten" ruling has had an impact on the way content is handled in the UK. Google reported receiving 93,968 requests involving the UK, requesting the removal of 215,066 URLs from its search results by July 2016, and complied in 39 percent of cases.[79] The BBC publishes a regular list of its news stories which have been delisted by search engines.[80] In May 2015, news reports said that the UK's data protection authority, the Information Commissioner's Office, was in talks with Google o er 48 cases that it believed the search engine had not resolved effectively.[81]

In 2016, Google announced that beginning mid-February, it would expand the right to be forgotten by removing links from all versions of its search engine.[82] It had previously removed them only on the local version in the country where the request originated, such as Google.co.uk, leaving them accessible to UK-based users searching international versions like Google.com. The change applies only to users with IP addresses indicating they are located within the jurisdiction of the removal request. The links remain available in searches conducted outside that jurisdiction.

Media, Diversity, and Content Manipulation

Self-censorship is difficult o measure in the United Kingdom, but not a grave concern. After the January 2015 attack on the French publication *Charlie Hebdo* some news outlets refrained from publishing the magazine's controversial cartoons of the prophet Muhammad,[83] but the decision was not government influenced or manda ed.

Due to the UK's extensive surveillance practices (see Surveillance, Privacy and Anonymity), it is possible that certain online groups self-censor to avoid potential government interference. Media and civil society groups filed legal challenges a ter Edward Snowden made GCHQ surveillance practices public, indicating heightened concern about the privacy of their communications. In September 2014, the London-based Bureau for Investigative Journalism filed an application with the Eu opean Court of Human Rights to rule on whether UK legislation properly protects journalists' sources and communications from government scrutiny and mass surveillance.[84] In January 2015, the European Court of Human Rights prioritized the case,[85] but in mid-2016 it remained pending.

There is no evidence documenting government manipulation of online content. Online media outlets face economic constraints that negatively impact their financial sustainabilit , but these are due to

79 Google Transparency Report, "European privacy requests for search removals," https://www.google.com/transparencyreport/removals/europeprivacy/.

80 Neil MacIntosh, "List of BBC web pages which have been removed from Google's search results," BBC Internet Blog, June 25 2015 http://www.bbc.co.uk/blogs/internet/entries/1d765aa8-600b-4f32-b110-d02fbf7fd379; and "May 2016: List of BBC web pages which have been removed from Google's search results," http://www.bbc.co.uk/blogs/internet/entries/b5963593-e7ca-4605-98fe-31f171874743

81 Kevin Rawlinson, Google in 'right to be forgotten talks with regulator', *BBC News*, 13 May 2015 http://www.bbc.co.uk/news/technology-32720944.

82 'Google takes wider action on 'right to be forgotten' BBC News, February 11 2016, http://www.bbc.co.uk/news/technology-35548532.

83 "News orgs censor Charlie Hebdo cartoons after attack," *Politico,* January 7, 2015, http://www.politico.com/blogs/media/2015/01/news-orgs-censor-charlie-hebdo-cartoons-after-attack-200709.html#.VK18tMDFVi5.twitter.

84 A summary of the Bureau's application to the European Court of Human Rights: https://www.thebureauinvestigates.com/2014/09/14/a-summary-of-the-bureaus-application-to-the-european-court-of-human-rights/.

85 Melanie Newman, "Surveillance state Boost for press freedom campaign as European court prioritises Bureau's legal challenge to UK snooping laws," *Bureau of Investigative Journalism* website, January 20, 2015, https://www.thebureauinvestigates.com/2015/01/20/boost-press-freedom-european-court-bureau-case-snooping-laws/.

market forces, not political intervention. Publications have struggled to find a p ofitable sys em for their online news platforms.

The UK lacks explicit protections for net neutrality, the principle that ISPs should not throttle, block or otherwise discriminate against internet traffic ased on content. Ofcom called for a self-regulatory approach to the issue in 2011,[86] describing the blocking of services and sites by ISPs as "highly undesirable" but subject to self-correction based on market forces.[87] Developments at EU level could have an impact on net neutrality provisions in the UK, after agreement has been reached to ban paid prioritization—content owners being able to pay to ISPs to push their content fi st—across the EU as part of the Digital Single Market policy package, which seeks to strengthen the digital economy through increased support and access.[88]

There are a wide variety of digital news platforms available, with 60 percent of people reporting that they consume news online, and 44 percent reporting that they consume news through apps. Blogs and social media also act as sources of news. Diverse views are present online, but may not be widely read, as 59 percent of people said they obtain news from the BBC website or app, 18 percent through Google, and 17 percent on Facebook.[89]

Digital Activism

Online political mobilization continues to grow both in terms of numbers of participants and numbers of campaigns, though the efficacy f online mobilization remains subject to debate and it is impossible to explain success with reference to online campaigns alone. Petition and advocacy platforms such as 38 Degrees and AVAAZ continued to grow, with AVAAZ claiming around 1.6 million users registered in the UK in 2015. All civil society organizations, charities and political parties now view online communication as an indispensable part of a wider campaign strategy.

In the lead up to the June 2016 referendum on the UK's membership of the European Union, the political discourse was largely conducted online, in keeping with other elections. Analysis of varying social media sites had found that, quantitatively, posts sympathetic to the leave campaign had more posts.[90] This was also found in independent research on Instagram users.[91]

Privacy advocates have also used digital tools to promote transparency about surveillance. In February 2015, the Investigatory Powers Tribunal said that aspects of the way UK and U.S. intelligence agencies shared information intercepted from internet communications between 2007 and 2014 breached human rights law (see Surveillance, Privacy and Anonymity).[92] The tribunal is obligated to

86 Ofcom, *Ofcom's approach to net neutrality*, November 11, 2011, http://stakeholders.ofcom.org.uk/consultations/net-neutrality/statement/.

87 European Commission, 'Digital Single Market', http://ec.europa.eu/digital-agenda/en/eu-actions; Andrus Ansip, "Making the EU work for people: roaming and the open internet," blog, European Commission, July 8, 2015, https://ec.europa.eu/commission/2014-2019/ansip/blog/making-eu-work-people-roaming-and-open-internet_en.

88 European Commission, 'Digital Single Market', http://ec.europa.eu/priorities/digital-single-market_en

89 Ofcom, "News Consumption in the UK," June 2014, http://stakeholders.ofcom.org.uk/binaries/research/tv-research/news/2014/News_Report_2014.pdf.

90 John Hermann, "'Brexit' Talk on Social Media Favored the 'Leave' Side," *New York Times*, June 24, 2016, http://www.nytimes.com/2016/06/25/business/brexit-talk-on-social-media-heavily-favored-the-leave-side.html?_r=0

91 Vyacheslav Polonski, "Social media voices in the UK's EU referendum," *Mashable,* May 15, 2016 https://medium.com/@slavacm/social-media-voices-in-the-uks-eu-referendum-brexit-or-bremain-what-does-the-internet-say-about-ebbd7b27cf0f#.usbbg521g.

92 Owen Bowcott, "UK-US surveillance regime was unlawful 'for seven years'," February 6, 2015, http://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa.

respond to any individual complaints and reveal if an individual was illegally monitored during that period. If so, the individual can ask that the data be deleted. To facilitate such complaints, Privacy International provided a form on its website which it submits to the Tribunal on behalf of individuals. More than 6,000 people signed up in the first 24 hours after the form was launched in early 2015.[93]

Violations of User Rights

The government has placed significant emphasis on stopping the dissemination of terrorist and hate speech online and on protecting individuals from targeted harassment on social media. User rights are undermined by extensive surveillance measures used by the government to monitor the flow of information for law enforcement and foreign intelligence purposes. There were several notable legal changes over the past year in these areas.

Legal Environment

The UK does not have a written constitution or other omnibus legislation detailing the scope of governmental power and individual rights. Instead, these constitutional powers and individual rights are encapsulated in various statutes and common law. The provisions of the European Convention on Human Rights (ECHR) were adopted into law via the Human Rights Act 1998. In 2014, Conservative Party officials, including the prime minister, announced their intentions to repeal the Human Rights Act in favor of a UK Bill of Rights in order to give British courts more control over application of human rights principles.[94] No such bill had been introduced to Parliament in mid-2016.[95]

Prosecutions for statements and messages posted online fall under various laws, including Section 5 of the Public Order Act 1986, which penalizes "threatening, abusive or insulting words or behavior." In 2013, it was amended to remove insults.[96] Section 127 of the Communications Act 2003 punishes "grossly offensive" communications sent through the internet.[97]

In February 2015, the Criminal Justice and Courts Act 2015 amended Section 1 of the Malicious Communications Act 1988.[98] The act already criminalized targeting individuals with abusive and offensive content online "with the purpose of causing distress or anxiety." The amendment additionally criminalized 'revenge porn,' the unwanted sharing of an individual's own private, sexual media for the purposes of embarrassment and humiliation,[99] and increased the maximum penalty from six months to two years in prison. These offenses were previously confined to the magistrates' courts,

93 Nicole Kobie, "From GCHQ to tech giants: why the fight for our personal data matters," *The Guardian,* March 3, 2015, http://www.theguardian.com/technology/2015/mar/03/gchq-tech-giants-fight-for-personal-data.

94 Oliver Wright, "David Cameron to 'scrap' Human Rights Act for new 'British Bill of Rights,'" The Independent, Oct. 1, 2014, http://www.independent.co.uk/news/uk/politics/conservative-party-conference-cameron-announces-plans-to-scrap-human-rights-act-9767435.html.

95 Owen Bowcott, "Plans to scrap the Human Rights Act delayed again", *The Guardian*, December 2, 2015 http://www.theguardian.com/law/2015/dec/02/plan-to-scrap-human-rights-act-delayed-again.

96 Adam Wagner, "Public insults to be legalised but grossly offensive messages still criminal", *The UK Human Rights Blog*, https://ukhumanrightsblog.com/2013/01/15/public-insults-to-be-legalised-but-grossly-offensive-messages-still-criminal/; See also CPS guidance on the offence: http://www.cps.gov.uk/legal/p_to_r/public_order_offences/#Section_5.

97 Claire Overman and Andrew Wheelhouse, "Papa Don't Preach (You May be Found Guilty of Hate Speech)," Oxford Human Rights Hub, March 22, 2016, http://ohrh.law.ox.ac.uk/papa-dont-preach-you-may-be-found-guilty-of-hate-speech/.

98 Ministry of Justice and The Rt Hon Chris Grayling MP, "Internet trolls to face 2 years in prison," Gov.uk, Press Release, Oct. 20, 2014, https://www.gov.uk/government/news/internet-trolls-to-face-2-years-in-prison.

99 "'Revenge porn' illegal under new law in England and Wales," BBC, February 12, 2015, http://www.bbc.co.uk/news/uk-31429026.

but the new law, effective in England and Wales as of April 13, 2015, allows the crown court to hear the more serious offenses, since it can issue higher prison sentences.[100] The changes also extended the time limit to bring charges for these offenses to three years from the date of the offense.[101]

The Crown Prosecution Service (CPS) publishes specific guidelines for the p osecution of crimes "committed by the sending of a communication via social media."[102] Updates in 2014 put digital harassment offenses committed with the intent to coerce the victims into sexual activity under the Sexual Offences Act 2003, which carries a maximum of 14 years in prison.[103] Revised guidelines were issued in March 2016.[104] The guidelines identify four categories of communications subject to possible prosecution under UK law: Credible threats; communications targeting specific individuals; b each of court orders; and grossly offensive, false, obscene, or indecent communications. They also advise prosecutors to consider the age and maturity of the poster before pursuing charges. Some observers said this could criminalize the creation of pseudonymous accounts, although only in conjunction with activity considered abusive.[105]

Some changes to the legal framework were debated during the coverage period. The Copyright, Designs, and Patents Act 1988 carries a maximum two year prison sentence for offenses committed online. In July 2015, the government held a public consultation regarding a proposal to increase the sentence to 10 years. Of the 1,011 responses, only 21 supported the proposal,[106] but in April 2016, a government consultation paper announced plans to submit an amendment to include the 10-year maximum sentence to parliament "at the earliest available legislative opportunity."[107]

In September 2015, the home secretary outlined a proposal for "extremism disruption orders."[108] The orders would allow judicial review of individuals and groups who "spread hate but do not break laws," disallowing them from posting messages to social media without fi st gaining government approval.[109] That proposal, supported by the prime minister, also included plans to grant Ofcom powers to prevent broadcast of "extremist messages," requiring pre-transmission monitoring of content.[110] However, the proposal met vocal opposition even from within the Conservative Party.[111]

100 "Internet trolls face up to two years in jail under new laws," BBC, October 19, 2014, http://bbc.in/ZAY5p9

101 Ministry of Justice and The Rt Hon Chris Grayling MP, "Internet trolls to face 2 years in prison," Gov.uk, Press Release, October 20, 2014, https://www.gov.uk/government/news/internet-trolls-to-face-2-years-in-prison.

102 CPS, "Guidelines on prosecuting cases involving communications sent via social media," http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/.

103 "Guidelines on prosecuting cases involving communications sent via social media," Crown Prosecution Service, amended October 2014, www.parliament.uk/documents/lords-committees/communications/socialmediaoffences/DPPLetter171014.pdf; Owen Bowcott, "Revenge porn could lead to 14-year-sentence, new guidelines clarify," *The Guardian*, October 7, 2014, www.theguardian.com/law/2014/oct/07/revenge-porn-14-year-sentence-cps-guidelines.

104 CPS, "New guidelines published on the prosecution of those who abuse victims online," March 3, 2016, http://www.cps.gov.uk/news/latest_news/new_guidelines_published_on_the_prosecution_of_those_who_abuse_victims_online/.

105 David Barrett, "Faking social media accounts could lead to criminal charges" *The Telegraph*, March 3, 2016 http://www.telegraph.co.uk/news/uknews/crime/12180782/Faking-social-media-accounts-could-lead-to-criminal-charges.html.

106 Intellectual Property Office, "Summa y of responses: Consultation on changes to the penalties…," http://bit.ly/2fzuCGw.

107 Intellectual Property Office, "Criminal Sanctions for Online Copyright Infringement: Go ernment Consultation Response," http://bit.ly/1putial.

108 Alan Travis, "What are Theresa May's new 'extremism disruption orders,'" *The Guardian*, September 2014, http://www.theguardian.com/politics/2014/sep/30/theresa-may-extremism-disruption-orders.

109 John Bingham, "Sharia law or gay marriage critics would be branded 'extremists' under Tory plans, atheists and Christians warn," *The Telegraph*, October 31, 2014, http://www.telegraph.co.uk/news/politics/11202290/Sharia-law-or-gay-marriage-critics-would-be-branded-extremists-under-Tory-plans-atheists-and-Christians-warn.html.

110 Rowena Mason and Alan Travis, "David Cameron backs proposal to block extremist messages on TV," The Guardian, May 22, 2015, http://bit.ly/2fFTGLY

111 Alan Travis, "It wasn't just Lib Dems who opposed Theresa May's counter-extremism plans," *The Guardian*, May 13, 2015, http://www.theguardian.com/world/2015/may/13/theresa-mays-counter-extremism-proposals-are-fraught-with-difficultie .

In 2014, a House of Lords committee recommended that websites allowing individuals to post content anonymously or under a pseudonym should be required to establish their actual identity.[112] Critics argue that such a measure would chill speech by removing the protections of anonymity from those afraid of repercussions.[113] In mid-2016, no action had been taken on the report's recommendation had been taken.

Libel laws that tended to favor the plaintiff had previously led to a large number of libel suits with only tenuous connection to the UK being brought in its courts, a phenomenon known as "libel tourism." This has had a chilling effect on free speech in the UK, which the Defamation Act 2013 intended to reduce. Sections which became active in January 2014 require claimants to prove that England and Wales is the most appropriate forum for the action, set a serious harm threshold for claims, and codify certain defenses such as truth and honest opinion. The overall number of defamation cases in the UK had fallen by 40 percent in the 2016 reporting period.[114]

Prosecutions and Detentions for Online Activities

Prosecutions involving interactions on social media increased in recent years, although jail sentences for political, social, or religious speech protected under human rights norms remain rare. According to a Freedom of Information request in October 2014,[115] about 12,000 people were prosecuted for offensive speech made via social media between 2008 and 2013.

Prosecutors have targeted Islamic extremism online. In April 2016, a court in London jailed Mohammed Moshin Ameen for fi e years for posting 8,000 Islamic State propaganda messages aimed at young men in the UK via 42 Twitter accounts.[116] He pleaded guilty to fi e counts of encouraging terrorist acts on social media, disseminating a terrorist video, and inviting support for a proscribed organization.

Other detentions involved comments about Muslims, though no prosecutions were subsequently reported. On February 16, 2016, Police Scotland arrested a man for posting a series of offensive messages on Facebook about the resettlement of Syrian refugees on the Isle of Bute, approximately 45 miles east of Glasgow.[117] Police Scotland said that they would not "tolerate any form of activity which could incite hatred and provoke offensive comments on social media."[118] In a separate, widely publicized case, police in south London arrested a man on March 23, 2016 for a Twitter post in which he described "confronting" a Muslim woman and asking her to "explain" a series of bombings

112 Communications Committee – First Report: Social media and criminal Offences, House of Lords, July 22, 2014, ¶54, http://www.publications.parliament.uk/pa/ld201415/ldselect/ldcomuni/37/3704.htm#a14.

113 Danny O'Brien, "UK's Lords and EU Take Aim at Online Anonymity," Electronic Frontier Foundation, August 5, 2014, https://www.eff.org/deeplinks/2014/08/uks-lords-and-eu-take-aim-online-anonymity.

114 Judicial Statistics, 2015: Issued defamation claims down by 40%, the second lowest number since 1992, http://bit.ly/2emOcbg

115 What Do They Know, "Social Media Abuse," https://www.whatdotheyknow.com/request/social_media_abuse#incoming-579232.

116 "Security guard jailed for fi e years over tweets glorifying Isis," *The Guardian*, April 28, 2016, http://www.theguardian.com/uk-news/2016/apr/28/security-guard-mohammed-moshin-ameen-jailed-for-fi e-years-over-tweets-glorifying-isis

117 Libby Brooks, "Man arrested for Facebook posts about Syrian refugees in Scotland", *The Guardian*, February 16, 2016, http://www.theguardian.com/uk-news/2016/feb/16/man-arrested-facebook-posts-syrian-refugees-scotland.

118 Libby Brooks, "Man arrested for Facebook posts."

carried out by Islamic State in Brussels on March 22.[119] A charge against him under the Public Order Act was dropped on March 25.

Some critics fear the drive against online extremism may affect individuals expressing or accessing political opinion. In February 2016, staff at a school in Southampton reported a 15-year-old pupil to police for accessing the United Kingdom Independence Party website in class, citing concern about the right-wing site's "extremist views."[120] The pupil said he was conducting research, and police took no further action.[121]

Changes in the law provided a means for redress for those affected by revenge porn (see Legal Environment). At least 175 cases were reported to police between April and October 2015, according to the *Guardian*.[122] That figu e, obtained from a freedom of information request, covered "just over a third of police forces in England and Wales."

Some of these cases were prosecuted during the reporting period. On September 1, 2015, Paige Mitchell pleaded guilty to assault and posting four sexually explicit pictures of her girlfriend on Facebook after an argument.[123] A court in Stevenage, Hertfordshire, sentenced her to six weeks in prison, suspended for 18 months, and mandatory counselling. In a separate case in October 2015, a court in Newport, Wales, sentenced Jesse Hawthorne to 16 weeks in prison, suspended for 12 months, for posting an explicit image of his ex-girlfriend on Facebook. He was barred from communicating with his ex-girlfriend for two years, including on social media.[124]

Surveillance, Privacy, and Anonymity

Surveillance became a major point of contention in the UK following the revelations by former National Security Agency (NSA) contractor Edward Snowden on the activities of GCHQ and its international counterparts, published by the *Guardian* since June 2013. One of the priorities of the current government is the overhaul of investigatory powers of its law enforcement and intelligence agencies. Over the past two years, investigatory powers have been subject to independent reviews. In these reviews, it has been consistently found that surveillance regulation is in need of reform, particularly in relation to specification f scope, establishing credible oversight, and appropriate safeguards for individual liberty. On March 1, 2016, the government introduced the Investigatory Powers Bill to consolidate and reform surveillance laws.[125] Critics say it lacks adequate safeguards and would

119 Alexandra Sims "Brussels attacks: Croydon man charged after tweet 'confronting Muslim woman over Brussels attacks'", The Independent, 25 March 2016, http://www.independent.co.uk/news/uk/crime/brussels-attacks-croydon-man-matthew-doyle-charged-tweet-confronting-muslim-woman-brussels-attacks-a6951711.html.

120 Siobhan Fenton "School calls police because pupil visited UKIP website on class computer" The Independent, 27 February 2016, http://www.independent.co.uk/news/uk/home-news/school-called-police-because-boy-visited-ukip-website-on-class-computer-a6899641.html

121 "Hedge End school defends UKIP call" The Breeze, 29 February 2016, http://www.thebreeze.com/southampton/news/local-news/hedge-end-school-defends-police-ukip-call/

122 Josh Halliday, "Revenge porn: 175 cases reported to police in six months," *The Guardian,* October 11, 2015, http://www.theguardian.com/uk-news/2015/oct/11/revenge-porn-175-cases-reported-to-police-in-six-months

123 CPS, "Female sentenced for revenge porn, believed to be fi st female prosecuted under the new law." http://www.cps.gov.uk/news/latest_news/female_sentenced_for_revenge_porn/ ; Ben Farmer, "Revenge porn: First woman sentenced for offence is spared jail," *The Telegraph,* September 1, 2015, http://www.telegraph.co.uk/news/uknews/law-and-order/11836591/Revenge-porn-First-woman-sentenced-for-offence-is-spared-jail.html

124 "Jesse Hawthorne gets suspended jail term for 'revenge porn'", BBC News, 7 October 2015, http://www.bbc.co.uk/news/uk-wales-south-east-wales-34468647.

125 UK Home Office, "In estigatory Powers Bill," March 1, 2016, https://www.gov.uk/government/collections/investigatory-powers-bill.

oblige the technology industry to provide backdoors to government agencies. In mid-2016, it was still being debated in parliament.

There are a number of legislative measures authorizing surveillance,[126] including the Regulation of Investigatory Powers Act 2000 (RIPA).[127] RIPA includes provisions related to the interception of communications, the acquisition of communications data, intrusive surveillance, secret surveillance in the course of specific operations, and access o encrypted data. Under current rules, RIPA allows national agencies and over 400 local bodies to access communication records for a variety of reasons, ranging from national security to tax collection. RIPA established the Investigatory Powers Tribunal to adjudicate issues regarding government surveillance, including by Britain's three intelligence agencies—GCHQ, MI5, and MI6. The 2012 Protection of Freedoms Act required local authorities to obtain the approval of a magistrate to access communications data.[128]

A clause within Part I of RIPA allows the foreign or home secretary to sign off on bulk surveillance if communications data is arriving from or departing to foreign soil.[129] This clause provided the legal basis for Tempora, a secret surveillance project documented in material leaked by Edward Snowden. Since the UK's fibe -optic network often routes domestic traffic th ough international cables, this provision legitimized widespread surveillance over most, if not all UK citizens.[130] Working with telecom companies, GCHQ installed intercept probes at the British landing points of undersea fiber-optic cables, giving the agency access to some 200 cables by 2012, each carrying up to 10 Gbps of data. Intelligence agents can process data collected by the probes, including phone calls, emails, social networking posts, private messages, and more. Content collected is stored for three days, and metadata (information such as mobile phone locations and email logs) for thirty days.[131] The arrangement allowed GCHQ to pass on information to its US counterparts in the NSA regarding U.S. citizens, thereby bypassing American restrictions on domestic surveillance. In 2013, documents revealed that the U.S. government had provided at least GBP 100 million (US$ 155 million) in funding to GCHQ since 2010, leading observers to argue that the U.S. government was paying to use information obtained by the UK government.[132]

Ten civil society organizations separately filed suit against GCHQ with the In estigatory Powers Tribunal in 2013, on grounds that surveillance impeded their work and contravened international human rights law. These were consolidated into a single case, *Liberty vs GCHQ*. In June 2015, the tribunal found that interception of two groups' communications had violated human rights standards, but made no determination in the other eight, (see Surveillance, Privacy and Anonymity).

126 For a general overview of surveillance and the diverse parties involved in the UK, see "Surveillance Road Map: A Shared Approach to the Regulation of Surveillance in the United Kingdom," *ICO*, February 14, 2014, http://ico.org.uk/~/media/documents/library/Corporate/Practical_application/surveillance-road-mapV2.pdf.

127 RIPA, http://www.legislation.gov.uk/ukpga/2000/23/contents; "Explanatory Notes" to RIPA, http://www.legislation.gov.uk/ukpga/2000/23/notes/contents.

128 Protection of Freedoms Act 2012, http://www.legislation.gov.uk/ukpga/2012/9/enacted.

129 Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies & James Ball, "GCHQ taps fib e-optic cables for secret access to world's communications," *The Guardian*, June 21, 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

130 Nick Hopkins, "NSA and GCHQ spy programmes face legal challenge," *The Guardian*, July 8, 2013, http://www.theguardian.com/uk-news/2013/jul/08/nsa-gchq-spy-programmes-legal-challenge.

131 Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, "GCHQ taps fib e-optic cables for secret access to world's communications," *The Guardian,* June 21, 2013, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

132 Nick Hopkins & Luke Harding, "GCHQ accused of selling its services after revelations of funding by NSA," *The Guardian*, August 2, 2013, http://www.theguardian.com/uk-news/2013/aug/02/gchq-accused-selling-services-nsa.

Civil society groups challenged the legitimacy of these practices with the Investigatory Powers Tribunal in *Liberty vs GCHQ*. The tribunal issued judgements in December 2014, and February 2015, and a related decision in June.[133] The 2014 judgement said that sharing of information intercepted from internet communications between GCHQ and the NSA was lawful now that some of the procedures had been publicly disclosed. The February 2015 judgment said that prior to that public disclosure, between 2007 and 2014, the activity violated European human rights standards.[134] That decision marked the first time the tribunal has ruled against any of the intelligence agencies that it is entrusted to oversee.[135] The June 2015 decision found procedural irregularities in the retention of communications intercepted from Amnesty International and the South Africa-based Legal Resources Center, though it found that the interception itself was lawful.[136] The tribunal made "no determination" on the claims brought by other NGOs, meaning either that no surveillance took place, or that it was considered lawful.

Three independent reviews of mass surveillance and the underlying legal framework have called more clearly for reform:

- In December 2014, a parliamentary Home Affairs Committee inquiry concluded that RIPA was not fit for purpose and that the legislation governing communications data is in need of complete overhaul.[137]
- In March 2015, the parliamentary Intelligence and Security Committee published the results of an inquiry into the extent and scale of mass surveillance.[138] The report found that bulk interception does not equate to blanket or indiscriminate surveillance, and that the country's intelligence agencies do not seek to circumvent the law. However, a new, single act of parliament should be introduced to address the complicated nature of the legal framework and the lack of transparency surrounding it, the report said.
- In June 2015 David Anderson, an independent person appointed by the home secretary to evaluate the operation of current counter-terrorism law, called for a clean slate for government surveillance activities, lamenting the fragmentation and obscurity of current laws. A new law should be both comprehensive in scope and comprehensible in nature, the report said.[139]

Other laws besides RIPA have been subject to criticism, particularly in respect to the length of time companies are obliged to store data about their users' activities. Regulations to implement the 2006

133 "GCHQ spied on Amnesty International - UK's surveillance tribunal," RT, July 2, 2015, https://www.rt.com/uk/271111-gchq-amnesty-international-spy/; Global Freedom of Expression, Columbia University, "Liberty vs GCHQ," https://globalfreedomofexpression.columbia.edu/cases/liberty-v-gchq/.

134 Owen Boycott, "UK-US surveillance regime was unlawful 'for seven years,'" *The Guardian,* February 6, 2015, http://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa.

135 "GCHQ-NSA intelligence sharing unlawful, says UK surveillance tribunal," Privacy International, February 2, 2015, https://privacyinternational.org/?q=node/482.

136 Investigatory Powers Tribunal, "IPT to Liberty and Others," July 1, 2015, http://www.ipt-uk.com/docs/IPT_to_Liberty_Others.pdf; Owen Bowcott, "GCHQ's surveillance of two human rights groups ruled illegal by tribunal," *The Guardian,* June 22, 2015, http://www.theguardian.com/uk-news/2015/jun/22/gchq-surveillance-two-human-rights-groups-illegal-tribunal.

137 Parliament.uk Commons Select Committee, "RIPA not fit for purpose say MPs" December 6, 2014, http://www.parliament.uk/business/committees/committees-a-z/commons-select/home-affairs-committee/news/141206-ripa-rpt-pubn/.

138 Rowena Mason, "Top web firms urge more transparency over UK requests for user data," *The Guardian*, October 18, 2013, http://www.theguardian.com/uk-news/2013/oct/17/uk-gchq-nsa-surveillance-inquiry-snowden.

139 David Anderson, "A Question of Trust," June 11, 2015, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf.

EU Data Retention Directive were adopted in the UK in 2009,[140] requiring providers to retain user metadata for 18 months, though not the content of their communications.[141] In April 2014, the Court of Justice of the European Union (CJEU) struck down the EU directive as a breach of fundamental privacy rights,[142] sparking fears that companies would begin to delete data on UK users and undermine counterterrorism investigations. The government passed the temporary UK Data Retention and Investigatory Powers Act (DRIPA) in July 2014, requiring telecommunication companies to retain users' metadata for up to 12 months.[143] It will expire at the end of 2016.

During the coverage period of this report, the legitimacy of DRIPA was debated in the courts. Academics, journalists, and privacy advocates criticized the legislation for reintroducing data retention requirements that were struck down by the European court.[144] Two members of parliament represented by human rights group Liberty challenged the Act in court on grounds that it is incompatible with the UK Human Rights Act, and the EU Charter of Fundamental Rights.[145] In July 2015, the High Court found in their favor, stating that sections 1 and 2 of the Act are unlawful, as they fail to provide clear and concise rules for ensuring that data is accessed for the purpose of serious offenses, and that access is not authorized by a court or other independent body.[146]

The government appealed the ruling, and on November 20, the Court of Appeal referred to the CJEU for clarification [147] The High Court's DRIPA judgement relied on an earlier CJEU's judgment which declared the EU Data Retention Directive invalid.[148] The Court of Appeal asked the CJEU whether it had intended that judgement to serve as a mandatory requirement for EU member states to follow in national legislation, and whether the judgement expanded the interpretation of certain articles of the EU Charter of Fundamental Rights. The CJEU expedited the case in February 2016,[149] but had not issued a response in mid-2016. In July, outside the coverage period of this report, the court's preliminary ruling said data retention was only legitimate during the investigation of serious crimes.[150]

With a final judgement on DRI A still pending, the government introduced the Investigatory Powers Bill (IP Bill) on March 1 2016.[151] Besides replacing DRIPA, the bill is meant to consolidate and reform disparate legal provisions into a single, accessible piece of legislation, replacing the current regime, including large parts of RIPA. (Other relevant legislation includes the Wireless Telegraphy Act 2006, the Telecommunications Act 1984, the Police Act 1997, the Intelligence Services Act 1994, and the Human Rights Act 1999.) However, critics said the bill lacked appropriate safeguards. A draft Code of

140 The Data Retention (EC Directive) Regulations 2009 (SI 2009 No. 859), April 2, 2009, http://www.legislation.gov.uk/ukdsi/2009/9780111473894.

141 The Retention of Communications Data (Code of Practice) Order 2003: http://www.legislation.gov.uk/uksi/2003/3175/made.

142 C−293/12, *Digital Rights Ireland v Minister for Communications*.

143 Andrew Grice, "Emergency data law: David Cameron plots to bring back snoopers' charter," *The Independent*, July 11, 2014, http://www.independent.co.uk/news/uk/politics/emergency-data-law-government-railroading-through-legislation-on-internet-and-phone-records-9596695.html.

144 Kadhim Shubber, "Everything you need to know about surveillance law DRIP," *Wired UK*, July 16, 2014, http://www.wired.co.uk/news/archive/2014-07/16/everything-you-need-to-know-about-drip; Alan Travis, "Snooper's charter or justified safeguard? The security bill explained," *The Guardian*, July 10, 2014, http://www.theguardian.com/politics/2014/jul/10/snoopers-charter-security-bill-explained.

145 Liberty, Campaigning for No Snoopers' Charter, https://www.liberty-human-rights.org.uk/campaigning/no-snoopers-charter.

146 [2015] EWHC 2092 (Admin)

147 *Secretary of State v Davis & Watson* [2015] EWCA Civ 1185

148 C−293/12, *Digital Rights Ireland v Minister for Communications*

149 ECLI:EU:C:2016:70, Order of the President of the Court, 1 February 2016, Accessed at: http://bit.ly/1WZEjhG

150 "Bulk data collection only lawful in serious crime cases, ECJ indicates," *The Guardian,* July 19, 2016, https://www.theguardian.com/world/2016/jul/19/bulk-data-collection-can-only-be-used-to-figh -serious.

151 UK Home Office, "In estigatory Powers Bill."

Practice published at the same time of the IP Bill included a requirement for communications service providers to "provide a technical capability to give effect to interception, equipment interference, bulk acquisition warrants or communications data acquisition authorizations."[152]

Requirements for technology companies to provide "backdoors" to government agencies—mechanisms to enter into a program or service without the user's permission—drew particular scrutiny in the context of the government's attitude towards encryption. Prime Minister David Cameron called for a ban on encryption in messaging apps in January 2015,[153] and reaffi med his commitment to making sure that terrorists were not able to communicate safely via new digital technologies in June.[154] There are no legal restrictions on the use of encryption technologies in the UK, though under Part 3 of RIPA it is a crime not to disclose an encryption key upon an order from a senior policeman or a High Court judge.[155] In 2008, the Court of Appeal held that such disclosure would not necessarily violate the privilege against self-incrimination.[156] The provision has been used to obtain court orders to force disclosure of keys.

Major technology companies such as Apple submitted statements to the IP Bill committee, which collects and analyzes evidence from stakeholders during the drafting of legislation, criticizing the requirement to maintain backdoors. In December 2015, Apple argued that weakening encryption or the use of backdoors would weaken individual security.[157] Robert Hannigan, the director of GCHQ, defended the bill in March 2016, arguing that neither GCHQ or the IP Bill advocate weakening encryption, but rather work to make security stronger and make the law clearer.[158] However, more than 200 lawyers called the bill "not fit for purpose" in a let er to the *Guardian* published the same month.[159] On March 8, the United Nations' Special Rapporteur for Privacy, Joseph Cannataci, highlighted the bill in his fi st report, which recommended that "disproportionate, privacy-intrusive measures such as bulk surveillance and bulk hacking as contemplated in the Investigatory Powers Bill be outlawed."[160] In mid-2016, the bill was in the committee stage of the legislative process.[161]

Earlier attempts to change the legal framework supporting surveillance were similarly criticized for expanding access for intelligence agencies without suitable strengthening of privacy protections. In 2012, the government introduced the Communications Data Bill to replace elements of RIPA. The

152 Natasha Lomas, "UK surveillance powers bill could force startups to bake in backdoors," *Tech Crunch,* March 10, 2016, https://techcrunch.com/2016/03/10/uk-surveillance-powers-bill-could-force-startups-to-bake-in-backdoors/.

153 Cory Doctorow, "What David Cameron just proposed would endanger every Briton and destroy the IT industry," *Boingboing*, January 13 2015, http://boingboing.net/2015/01/13/what-david-cameron-just-propos.html; James Ball, "Cameron wants to ban encryption – he can say goodbye to Digital Britain," *Guardian*, January 13 2015 http://www.theguardian.com/commentisfree/2015/jan/13/cameron-ban-encryption-digital-britain-online-shopping-banking-messaging-terror.

154 Adam Bienkov, "David Cameron: Twitter and Facebook privacy is unsustainable," *Politics,* June 30, 2015, http://www.politics.co.uk/news/2015/06/30/david-cameron-twitter-and-facebook-privacy-is-unsustainable.

155 2000, accessible: http://www.legislation.gov.uk/ukpga/2000/23/contents.

156 *R v S & Anor* [2008] EWCA Crim 2177 (October 09, 2008), http://www.bailii.org/ew/cases/EWCA/Crim/2008/2177.html.

157 Apple Inc and Apple Distribution International – Written Evidence (IPB0093) accessed at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26341.pdf.

158 Robert Hannigan, Speech to MIT "Front doors and strong locks: encryption, privacy and intelligence gathering in the digital era", March 8, 2016, https://www.gchq.gov.uk/speech/front-doors-and-strong-locks-encryption-privacy-and-intelligence-gathering-digital-era.

159 "Investigatory powers bill not up to the task", *The Guardian*, March 14, 2016, http://www.theguardian.com/law/2016/mar/14/investigatory-powers-bill-not-up-to-the-task; https://www.theguardian.com/world/2016/mar/14/investigatory-powers-bill-not-fi -for-purpose-say-200-senior-lawyers.

160 Joseph Cannataci, "Report of the Special Rapporteur on the right to privacy," OHCHR, March 8, 2016, http://www.ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc at para. 39.

161 Investigatory Powers Bill website, UK Parliament, http://services.parliament.uk/bills/2015-16/investigatorypowers.html.

media dubbed the bill 'the Snooper's Charter,' as it would have recorded details of messages sent over social media platforms, phone call records, and internet browsing activity including each website a user had visited (although not the pages within that site).[162] The Liberal Democrats, a coalition partner with the Conservatives, withdrew their support for the bill in 2013.[163]

According to the latest available data, 517,236 requests for communications data were submitted by public authorities in 2014, compared to 514,608 in 2013; 2,795 lawful intercept warrants were issued, a slight increase from 2,760 in 2013.[164]

Intimidation and Violence

There were no reported incidences of violence against users for their online activities over the coverage period, though cyberbullying, particularly targeting women, is widespread.[165] Some online abuse is subject to prosecution under UK law (see Legal Environment and Prosecutions and Detentions for Online Activities).

Technical Attacks

Nongovernmental organizations, media outlets, and activists are not generally targeted for technical attacks by government or nonstate actors, although the use of computer exploitation techniques have been avowed by the government and GCHQ. On February 12, 2016, the Investigatory Powers Tribunal ruled in *Privacy International v. Secretary of State for the Foreign and Commonwealth Office et al* that computer network exploitation carried out by GCHQ was in principle lawful.[166] The arguments provided in defense of these activities rested on the powers being within the limitations in the European Convention of Human Rights. The tribunal also noted that network exploitation is legal if the warrant is as specific and nar ow as possible. There are no figu es or further information on where such exploitation takes place and in which circumstances.

In wider cybercrime, financially-moti ated fraud and hacking continue to present a challenge to authorities and the private sector. Incidents of cyberattacks have increased in recent years. Observers also question the security of devices connected to the network though the Internet of Things.[167]

162 The term Snooper's Charter has also been applied to the current IP bill due to the broad similarities between the two pieces of proposed legislation.

163 Thomas Brewster "Nick Clegg 'kills off Snooper's Charter'", *Tech Week Europe*, April 25, 2013, http://www.techweekeurope.co.uk/workspace/nick-clegg-kills-off-snoopers-charter-114390.

164 Rt Hon Sir Anthony May, *2014 Annual Report of the Interception of Communications Commissioner* (London: House of Commons), March 201,5 http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20%28Web%29.pdf.

165 Sandra Laville, "Top tech fi ms urged to step up online abuse fight ack," *The Guardian,* April 11, 2016, https://www.theguardian.com/technology/2016/apr/11/facebook-twitter-google-urged-to-step-up-online-abuse-fight_ack.

166 [2016] UKIP Trib 14_85-CH *Privacy International v. Secretary of State for the Foreign and Commonwealth Office et al.*

167 Andrew Meola, "How the Internet of Things will affect security & privacy," *Business Insider,* August 24, 2016, http://www.businessinsider.com/internet-of-things-security-privacy-2016-8?r=UK&IR=T.

Freedom House

United States

	2015	2016
Internet Freedom Status	**Free**	**Free**
Obstacles to Access (0-25)	3	3
Limits on Content (0-35)	2	2
Violations of User Rights (0-40)	14	13
TOTAL* (0-100)	**19**	**18**

* 0=most free, 100=least free

Population:	**321.4 million**
Internet Penetration 2015 (ITU):	**75 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**No**
Press Freedom 2016 Status:	**Free**

Key Developments: June 2015 – May 2016

- The USA FREEDOM Act passed in June 2015 limited bulk collection of Americans' phone records and established other privacy protections. Nonetheless, mass surveillance targeting foreign citizens continues through programs authorized under Section 702 of the FISA Amendments Act and Executive Order 12333 (see **Surveillance, Privacy, and Anonymity**).
- Online media outlets and journalists face increased pressure, both financiall and politically, that may impact future news coverage (see **Media, Diversity, and Content Manipulation**).
- Following a terrorist attack in San Bernardino in December 2015, the FBI sought to compel Apple to bypass security protections on the locked iPhone of one of the perpetrators (see **Surveillance, Privacy, and Anonymity**).

Introduction

Internet freedom improved slightly as the United States took a significan step toward reining in mass surveillance by the National Security Agency (NSA) with the passage of the USA FREEDOM Act in June 2015.

The law ended the bulk collection of Americans' phone records under Section 215 of the PATRIOT Act, a program detailed in documents leaked by former NSA contractor Edward Snowden in 2013 and ruled illegal by the Second Circuit Court of Appeals in May 2015. Intelligence agencies must now make more specifi requests to telecommunications companies to retrieve records. Under the law, a privacy advocate will be included in proceedings in the closed-door FISA court, which approves surveillance requests.

Despite these improvements, privacy advocates continue to call for reforms of Section 702 of the FISA Amendments Act and Executive Order 12333, which have been used to authorize other mass surveillance programs that collect metadata and communications content targeting foreign civilians, and which sweep up and store Americans' information in the process.

The debate over encryption, fueled in part by the NSA revelations in 2013, continued throughout the past year and intensifie following a Federal Bureau of Investigation (FBI) investigation into a mass shooting in San Bernardino, California in December 2015. After recovering one of the assailant's passcode-protected iPhones, the FBI obtained a court order that would have compelled Apple to create a software update to disable the passcode and allow access to the phone's contents. Apple refused, and the U.S. Department of Justice dropped the case after the FBI said a third party was able to successfully hack into the phone.[1]

While freedom of expression is well protected and the online media environment generally represents a range of diverse viewpoints, a few cases of powerful individuals seeking to punish media outlets signaled a worrying trend. Donald Trump, the Republican nominee in the 2016 presidential race, repeatedly prevented journalists—including several from online outlets—from attending press briefing in retribution for their critical coverage of his campaign. In May 2016, news reports said billionaire tech entrepreneur Peter Thiel had finance a lawsuit against Gawker Media with the intention of bankrupting the company, apparently in retaliation for online news reports published by the group that he said invaded his privacy. This set a troubling precedent for targeted litigation as an intimidation tactic and a financia constraint on media freedom.

Following the release of the Open Internet Order that established net neutrality protections in 2015, the Federal Communications Commission (FCC) continued to advance broadband access and protect the open internet. As part of the authorization of Charter Communications' acquisition of Time Warner Cable in May 2016, the FCC required that the company establish new cable lines in areas without access, and provide affordable internet access to at least 525,000 low-income families. In December 2015, Chairman Tom Wheeler said the commission would examine the practice of zero-rating—programs offered by telecommunications companies which allow users unlimited access to content from select providers, while charging for others—to determine whether these programs are in line with the Open Internet Order's net neutrality provisions.

1 Julia Edwards, "FBI paid more than $1.3 million to break into San Bernardino iPhone," *Reuters*, April 22, 2016, http://www.reuters.com/article/us-apple-encryption-fbi-idUSKCN0XI2IB; Devlin Barrett, "Federal Prosecutors Drop Court Case to Force Apple to Unlock iPhone," *Wall Street Journal,* April 22, 2016, http://www.wsj.com/articles/federal-prosecutors-drop-court-case-to-force-apple-to-unlock-iphone-1461377642.

Obstacles to Access

Access to the internet in the United States is largely unregulated. It is provided and controlled in practice by a small group of private cable television and telephone companies that own and manage the network infrastructure. This model has been questioned by observers who warn that insufficient competition in the ISP market could increase the cost of access, adversely affecting the economy and individuals' participation in civic life, which increasingly occurs online.[2] In 2016, the FCC began buying TV airwaves to resell to mobile broadband providers in a spectrum auction designed to increase wireless broadband availability and improve data delivery services, as more users rely on mobile phones for internet access.

Availability and Ease of Access

Although the United States is one of the most connected countries in the world, the speed, affordability, and availability of its broadband networks has fallen behind several other developed countries. According to the International Telecommunication Union, internet penetration in the United States reached 74 percent by the end of 2015.[3] Broadband adoption rates are high, with approximately 80 percent of Americans subscribing to either a home-based or smartphone-based internet service as of 2015, though the percentage of those who only have smartphone-based access is increasing, while home-based access is decreasing.[4] While the broadband penetration rate is high by global standards, it lags significantl behind countries such as Switzerland, the Netherlands, Denmark, and South Korea.[5] Moreover, access, cost, and usability remain barriers for many Americans, particularly senior citizens, people who live in rural areas, and low-income households. However, internet access rates for those 65 years of age and older has steadily increased over the past decade, with more 58 percent of individuals in this age bracket using the internet as of 2015, according to recent data from the Pew Research.[6]

The FCC's annual progress report on broadband adoption issued in January 2016 found that a digital divide between Americans living in rural versus urban areas persists despite some improvements.[7] Lack of access in rural areas continues to be a barrier, where low population densities make it less appealing for private companies to make large investments in network infrastructure. As a result, 39 percent of rural residents lack access to broadband internet, compared with only 4 percent of urban residents.[8]

In January 2015, citing advances in technology, market offerings, and consumer demand, the Federal

2 Mark Cooper, "The Socio-Economics of Digital Exclusion in America, 2010," (paper presented at 2010 TPRC: 38th Research Conference on Communications, Information, and Internet Policy, Arlington, Virginia, October 1–3, 2010).

3 In 2016, the ITU revised its penetration data for the U.S. in 2014 from 87 percent to 73 percent. International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015,", http://bit.ly/1FDwW9w.

4 John B. Horrigan and Maeve Duggan, "Home Broadband 2015," Pew Research Center, December 21, 2015, http://www.pewinternet.org/2015/12/21/2015/Home-Broadband-2015/

5 OECD Broadband Statistics, "OECD Fixed (Wired) Broadband Subscriptions per 100 Inhabitants, by Technology, June 2014," December 2014, http://bit.ly/1cP4RGV; "OECD Terrestrial Mobile Wireless Broadband Subscriptions per 100 Inhabitants, by Technology, June 2014."

6 Andrew Perrin and Maeve Duggan, *Americans' Internet Access: 2000-2015*, Pew Research Center: Internet, Science & Tech, June 26, 2015, http://pewrsr.ch/1TRMM48.

7 Federal Communications Commission, "Broadband Progress Report: Significan Improvements but Digital Divide Persists," January 28, 2016, https://apps.fcc.gov/edocs_public/attachmatch/DOC-337471A1.pdf.

8 Federal Communications Commission, "2016 Broadband Progress Report," Federal Communications Commission, January 29, 2016, https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2016-broadband-progress-report.

Communications Commission (FCC) updated its benchmark speeds for broadband internet service to 25 Megabits per second (Mbps) download and 3 Mbps upload, up from the 2010 standard of 4 Mbps download and 1 Mbps upload. Under the new definition the FCC found that 10 percent of the population lacks access to broadband service in its January 2016 report, compared to 17 percent in 2015.[9]

The cost of broadband internet access in the United States continues to be higher than many countries in Europe with similar internet penetration rates. According to a 2014 report, the median cost of broadband access with speeds of 30 Mbps is US$55 in the United States, compared to US$43 in Europe.[10] For gigabit internet service (speeds of 1,000 Mbps or higher), prices in Tokyo, Seoul, and Hong Kong ranged from US$30-40 per month, compared to $70-110 in cities like Chattanooga and Lafayette, LA that have community broadband networks, and $70 in cities like Kansas City with Google Fiber.[11] Yet most cities in the United States do not have these options. Cities like Los Angeles, Washington DC, and New York, which had the next highest speeds of 500 Mbps offered through Verizon Fios, cost on average US$299 per month.[12]

Uptake rates for internet-enabled mobile devices have increased dramatically throughout the United States in recent years. In 2015, 92 percent of adults reported that they own a mobile phone, and 68 percent of adults own a smartphone.[13] A growing number of people use their cell phones to view streaming video services offered by companies such as Netfli or Hulu (33 percent of smartphone owners in 2015, compared to 15 percent in 2012).[14] Pew Research reported in early 2015 that young adults, minorities, and those with lower household incomes are more likely to be "smartphone-dependent," with limited options for internet access other than their phones.[15]

Restrictions on Connectivity

Internet users in the United States face few government-imposed restrictions on their ability to access content online. The backbone infrastructure is owned and maintained by private telecom companies, including AT&T and Verizon. In contrast to countries with only a few connections to the backbone internet infrastructure, the United States has numerous connection points, which would make it nearly impossible to disconnect the entire country from the internet.

At the same time, law enforcement agencies in the United States are known to have and occasionally wield the power to inhibit wireless internet connectivity in emergency situations. The federal government has a secret protocol for shutting down wireless internet connectivity in response to particular events, some details of which recently came to light following a lawsuit brought under

9 Federal Communications Commission, "2016 Broadband Progress Report," Federal Communications Commission, January 29, 2016, https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2016-broadband-progress-report.

10 "The Cost of Connectivity 2014," Open Technology Institute, October 30, 2014, https://www.newamerica.org/oti/policy-papers/the-cost-of-connectivity-2014/.

11 "The Cost of Connectivity 2014," Open Technology Institute, October 30, 2014, https://www.newamerica.org/oti/policy-papers/the-cost-of-connectivity-2014/.

12 "The Cost of Connectivity 2014," Open Technology Institute, October 30, 2014, https://www.newamerica.org/oti/policy-papers/the-cost-of-connectivity-2014/.

13 Monica Anderson. "Technology Device Ownership: 2015." Pew Research Center, October 2015, http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015.

14 Monica Anderson, "More Americans using smartphones for getting directions, streaming TV," Pew Research Center, January 29, 2016, http://www.pewresearch.org/fact-tank/2016/01/29/us-smartphone-use/.

15 Aaron Smith, *Smartphone Use in 2015*, Pew Research, http://pewrsr.ch/19JDwMd.

the Freedom of Information Act.[16] The protocol, known as Standard Operating Procedure (SOP) 303, established in 2006 on the heels of a 2005 cellular-activated subway bombing in London, codifie the "shutdown and restoration process for use by commercial and private wireless networks during national crisis." However, what constitutes a "national crisis," and what safeguards exist against abuse remain largely unknown, as the full SOP 303 documentation has never been released to the public.[17]

State and local law enforcement also have tools to jam wireless internet. In 2011, San Francisco public-transit provider Bay Area Rapid Transit (BART) interrupted wireless service on its platforms to disrupt protests sparked by the police shooting of a homeless man named Charles Hill.[18] In December 2014, the FCC issued an Enforcement Advisory clarifying that it is illegal to jam cell phone networks without a federal authorization, even for state and local law enforcement agencies.[19]

ICT Market

There are few obstacles that prevent the existence of diverse business entities providing access to digital technologies in the United States, which is home to a thriving startup community of innovators and entrepreneurs that has produced many low-cost, globally successful online platforms and tools.

While there are many broadband service providers operating in the United States, the industry has trended toward consolidation. As of 2015, fi e dominant providers — Comcast, AT&T, Time Warner Cable, Verizon, and CenturyLink — owned the majority of network cables and other infrastructure, serving a combined 65 million customers and controlling 70 percent of the market for 4 Mbps service.[20] For customers subscribing to service that meets the new 25 Mbps benchmark for broadband, the market is even less competitive, with a single provider — Comcast — controlling over 50 percent of the market.[21]

Further consolidation of the telecom sector threatens to limit consumer choice of ICT services. On May 6, 2016, the FCC announced that it had voted to approve Charter Communications Inc.'s acquisition of Time Warner Cable and Bright House Networks, which was subsequently approved by the California Public Utilities Commission.[22] The deal would result in two companies—Charter Communications and Comcast—controlling an estimated 70 percent of the market for broadband access, raising concerns about increased market consolidation.[23] At the same time, the FCC included provisions within the deal that require Charter Communications to expand broadband availability

16 The Electronic Privacy Information Center (EPIC) file suit against the Department of Homeland Security (DHS) in 2013 for information about the protocol. After winning an appeal in the DC Circuit, the DHS retained exemption from disclosing SOP 303, and in July of 2015 released a redacted version of the protocol. Electronic Privacy Information Center, *EPIC v. DHS – SOP 303,* http://bit.ly/1GscPWS; Electronic Privacy Information Center, *SOP 303 Updated Release*, http://bit.ly/1WI9hZV.

17 Electronic Privacy Information Center, *EPIC v. DHS – SOP 303*.

18 Melissa Bell, "BART San Francisco Cut Cell Services to Avert Protest," *The Washington Post*, August 12, 2011, http://wapo.st/1GscX8T

19 Federal Communications Commission, *WARNING: Jammer Use Is Prohibited*, December 8, 2014, http://fcc.us/1L1RV2O.

20 Leichtman Research Group, "3 Million Added Broadband From Top Providers in 2014," press release, March 5, 2015, http://bit.ly/1WIa1hL.

21 Jon Brodkin, "Comcast now has more than half of all US broadband customers" *Ars Technica*, January 30, 2015, http://bit.ly/1FPGOgI.

22 Meg Jones, "California regulators approve Charter's takeover of Time Warner Cable," *Los Angeles Times*, May 12, 2016, http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-charter-puc-20160512-snap-story.html.

23 Jon Brodkin, "Comcast and Charter may soon control 70% of 25Mbps Internet subscriptions," ArsTechnica, January 26, 2016, http://arstechnica.com/business/2016/01/comcast-and-charter-may-soon-control-70-of-25mbps-internet-subscriptions/.

in an effort to close the digital divide, including establishing new cable lines in areas of California without access, and providing affordable internet access to at least 525,000 low-income families.[24] Other conditions prohibit the companies from taking steps that would privilege cable services over online video competitors, such as imposing data caps on online content that would discourage subscribers from streaming video.[25] In 2015, regulators at the FCC and the Department of Justice blocked a proposed merger between Time Warner Cable and Comcast, citing concerns about Comcast's ability to interfere with over-the-top services (such as Netflix) as well as increased market concentration. [26]

In 2005, the FCC embraced an aggressive deregulation agenda that freed network owners from a longstanding obligation to lease their lines to competing providers. Deregulation proponents claimed that this step would give large cable and telephone companies incentive to expand and upgrade their networks, while opponents worried that the move would lead to higher prices, fewer options for consumers, and worse service. Although average broadband speeds have increased over the past decade, the majority of American households have access to only one broadband provider that offers download speeds of at least 25 Mbps.[27]

Americans increasingly access the internet via mobile technologies, as wireless carriers deploy advanced Long-Term Evolution (LTE) networks. Following a decade of consolidation, the U.S. wireless market is dominated by four national carriers — AT&T, Verizon, Sprint, and T-Mobile — which accounted for 98 percent of the market share by the end of 2014. The combined revenue of AT&T and Verizon Wireless alone accounted for 71 percent of the market.[28] The U.S. government has looked unfavorably on further consolidation of mobile networks. Regulators blocked AT&T's proposed merger with T-Mobile in 2011, and separately signaled that they would block a rumored merger between Sprint and T-Mobile in 2014.[29] Moreover, the government has promoted mobile broadband through a series of spectrum auctions. In March 2016, the FCC began the process of buying back airwaves set aside for TV broadcasters to increase the available spectrum for wireless broadband, as outlined in the government's 2012 National Broadband Plan, which set a goal of establishing universal broadband by 2020.[30]

In January 2015, President Barack Obama announced an initiative to encourage the development of community-based broadband services and asked the FCC to remove barriers to local investment.[31] One month later, the FCC "preempted," or overturned, state laws in Tennessee and North Carolina

24 Meg Jones, "California regulators approve Charter's takeover of Time Warner Cable," *Los Angeles Times*, May 12, 2016, http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-charter-puc-20160512-snap-story.html.

25 Jon Brodkin, "Comcast and Charter may soon control 70% of 25Mbps Internet subscriptions," ArsTechnica, January 26, 2016, http://arstechnica.com/business/2016/01/comcast-and-charter-may-soon-control-70-of-25mbps-internet-subscriptions/.

26 Federal Communications Commission, "Statement from FCC Chairman Tom Wheeler on the Comcast-Time Warner Cable Merger," news release, April 24, 2015, http://bit.ly/1OfzSug; U.S. Department of Justice, "Comcast Corporation Abandons Proposed Acquisition of Time Warner Cable After Justice Department and Federal Communications Commission Informed Parties of Concerns," press release, April 24, 2015, http://1.usa.gov/1Qrf57U.

27 Prepared Remarks of Federal Communications Commission Chairman (FCC) Tom Wheeler "The Facts and Future of Broadband Competition". September 4, 2014 https://apps.fcc.gov/edocs_public/attachmatch/DOC-329161A1.pdf .

28 Federal Communications Commission, *Annual Report Of Competitive Market Conditions For Commercial Mobile Wireless*, December 23, 2015, https://apps.fcc.gov/edocs_public/attachmatch/DA-15-1487A1.pdf.

29 Michael J. De La Merced, "Sprint and Softbank End Their Pursuit of a T-Mobile Merger," *DealB%*k (blog), *New York Times*, August 5, 2014, http://nyti.ms/1KW0LBh.

30 Colin Lecher, "How the FCC's massive airways auction will change America—and your phone service," *The Verge*, April 21, 2016, http://www.theverge.com/2016/4/21/11481454/fcc-broadcast-incentive-auction-explained.

31 The White House, Offic of the Press Secretary, "FACT SHEET: Broadband That Works: Promoting Competition & Local Choice In Next-Generation Connectivity," press release, January 13, 2015, http://1.usa.gov/1GUJIQ9.

that restrict local broadband services, arguing that such laws create barriers to broadband deployment.[32] In August 2016, a federal court ruled that the FCC does not have the authority to preempt these state laws,[33] which are also on the books in many other states. The ruling threatens to limit affordable broadband options for small remote communities.

Regulatory Bodies

No single agency governs the internet in the United States. The Federal Communications Commission (FCC), an independent agency, is charged with regulating radio and television broadcasting, interstate communications, and international telecommunications that originate or terminate in the United States. The FCC has jurisdiction over a number of internet-related issues, especially since February 2015, when it issued a decision to legally classify broadband as a telecommunications service under the Communications Act. Other government agencies, such as the Commerce Department's National Telecommunications and Information Administration (NTIA), also play advisory or executive roles with respect to telecommunications, economic and technological policies, and regulations. It is the role of Congress to create laws that govern the internet and delegate regulatory authority. Government agencies such as the FCC and the NTIA must act within the bounds of congressional legislation.

Limits on Content

Access to information on the internet is generally free from government interference in the United States. There is no government-run filtering mechanism affecting content passing over the internet or mobile phone networks. Users with opposing viewpoints engage in vibrant online political discourse and face almost no legal or technical restrictions on their expressive activities online. However, politicians and businessmen raised concerns about press freedom by openly articulating their intentions to silence media outlets they believed to be opposing them, including many that operate online. Additionally, revelations about the extent of government surveillance of online communications and aggressive investigations into journalists in whistleblower cases have led some to reports of increased self-censorship online.

Blocking and Filtering

In general, the U.S. government does not block or fil er online content. Some states require publicly funded schools to install fil ering software on their computers to block obscene, illegal, or harmful content.[34] The Children's Internet Protection Act of 2000 (CIPA) requires public libraries that receive certain federal government subsidies to install fil ering software that prevents users from accessing child pornography or visuals that are considered obscene or harmful to minors. Libraries that do not receive the specifie subsidies from the federal government are not obliged to comply with CIPA,

32 Federal Communications Commission, "FCC Grants Petitions to Preempt State Laws Restricting Community Broadband in North Carolina, Tennessee," news release, February 26, 2015, http://bit.ly/1Z3DrZO.

33 See *State of TN vs. FCC*, http://www.ca6.uscourts.gov/case_reports/rptPendingAgency.pdf; Brian Fung, "Cities looking to compete with large Internet providers just suffered a big defeat," *Washington Post,* August 1-, 2016, https://www.washingtonpost.com/news/the-switch/wp/2016/08/10/the-government-just-lost-a-big-court-battle-over-public-internet-service/.

34 National Conference of State Legislators, "Laws Relating to Filtering, Blocking, and Usage Policies in Schools and Libraries," June 12, 2015, http://bit.ly/1zvIfGT.

but more public libraries are seeking federal aid in order to mitigate budget shortfalls.[35] Under the U.S. Supreme Court's interpretation of the law, adult users can request that the fil ering be removed without having to provide a justification However, not all libraries allow this option, arguing that decisions about fil ering should be left to the discretion of individual libraries.[36]

The rise of the Islamic State has sparked intense debate about the appropriate role of social media companies in combating the use of mainstream social media as a tool used by terrorist organizations for recruitment and communication. Some government official have proclaimed that social media companies are being exploited by terror organizations, and that the companies have an active responsibility to block or remove terror-related content.[37] Various companies maintain internal trust and safety policies with regard to hate speech and extremist groups, and in July 2015, the Senate Intelligence Committee approved legislation in a closed hearing that would require "electronic communication service providers" to report suspected terrorist content to federal authorities.[38]

Limits on Content

The government does not censor any particular political or social viewpoints, although legal rules do restrict certain types of content on the internet. Illegal online content, including child pornography and content that infringes on copyright, is subject to removal through a court order or similar legal process if it is hosted within the United States. Aside from these examples, government pressure on ISPs or content hosts to remove content is not a widespread issue. Social media companies and other content providers may remove content that violates their terms and conditions.

Content removal by private companies was brought into the spotlight in August 2016 (outside the coverage period of this report) when Facebook complied with a request from Baltimore police to temporarily disable Facebook and Instagram accounts operated by 23-year-old Korryn Gaines. Gaines was using her Facebook account to broadcast live as she used a shotgun to resist police attempting to serve her with an arrest warrant stemming from traffi violations. Later during the same encounter she was shot and killed, and her fi e-year-old son wounded.[39] Facebook subsequently restored her account, but restricted two videos it said violated its terms of service. Critics of the measure said the videos could have revealed more information about the circumstances of Gaines' death.[40] Smartphone videos of law enforcement shootings of African American citizens have drawn national media attention to cases that might otherwise be underreported and can support criminal charges against police office s if they provide evidence of

35 American Library Association, "Public Library Funding Landscape," 2011-2012, accessed June 4, 2015, 15, http://bit.ly/1KW2uql.

36 *See, e.g.*, Bradburn v. North Central Regional Library District (Washington state Supreme Court) No. 82200-0 (May 6, 2010); Bradburn v. NCLR, No. CV-06-327-EFS (E.D. Wash. April 10, 2013).

37 Scott Higham and Ellen Nakashima, "Why the Islamic State leaves tech companies torn between free speech and security," *Washington Post,* July 16, 2015, http://wapo.st/1O9SVUQ.

38 Ellen Nakashima, "Lawmakers want Internet sites to fla 'terrorist activity' to law enforcement," *Washington Post*, July 4, 2015, http://wapo.st/1H9hEq9.

39 Baynard Woods, "Facebook deactivated Korryn Gaines' account during standoff, police say," *The Guardian,* August 3, 2016, https://www.theguardian.com/us-news/2016/aug/03/korryn-gaines-facebook-account-baltimore-police.

40 Justin Fenton, "Korryn Gaines case: Video posting by suspects poses new challenges for police," *Baltimore Sun,* August 3, 2016, http://www.baltimoresun.com/news/maryland/crime/bs-md-ci-facebook-police-deactivate-20160803-story.html.

misconduct.[41] Individuals who have filme shooting incidents routinely report harassment by police (see Prosecutions and Detentions for Online Activity and Intimidation and Violence).

One of the most important protections for online free expression in the United States is Section 230 of the Communications Decency Act of 1934 (CDA 230), amended by the Telecommunications Act of 1996, which generally shields online sites and services from legal liability for the activities of their users, allowing rich user-generated content to flouris on a variety of platforms.[42] However, public concern over intellectual property violations, child pornography, protection of minors from harmful or indecent content, harassing or defamatory comments, publication of commercial trade secrets, gambling, and financia crime have presented a strong impetus for aggressive legislative and executive action, and some have threatened to undermine the broad protections of CDA 230.

Congress has passed several laws designed to restrict adult pornography and shield children from harmful or indecent content online, such as the Child Online Protection Act of 1998 (COPA), but these laws have been overturned by courts due to their ambiguity and potential infringements on the First Amendment of the U.S. Constitution, which protects freedom of speech and the press. Advertisement, production, distribution, and possession of child pornography—on the internet and in all other media—is prohibited under federal law and can carry a sentence of up to 30 years in prison. According to the Child Protection and Obscenity Enforcement Act of 1988, producers of sexually explicit material must keep records proving that their models and actors are over 18 years old. In addition to prosecuting individual offenders, the Department of Justice, the Department of Homeland Security, and other law enforcement agencies have asserted their authority to seize the domain name of a website allegedly hosting child abuse images after obtaining a court order.[43]

In 2015, Congress introduced a law known as the SAVE Act, which would help protect against sex traffickin of children by making it a serious criminal offense to publish advertisements related to sex traffickin or to benefi from such advertising.[44] Civil society groups argued that the law's harsh penalties would chip away at CDA 230 protections, chill a robust advertising ecosystem that is generally content neutral, and encourage online websites and services to self-censor.[45] On May 29, 2015, the SAVE Act became law after it was added to S. 178 Justice for Victims of Traffickin Act of 2015.[46] The fina text of the legislation was changed to make it illegal to knowingly advertise content related to sex trafficking a higher requirement than an earlier draft that would have established liability for "knowledge of" or "active disregard for the likelihood of" hosting such content.[47] At the same time, the law still establishes federal criminal liability for third-party content, which could lead to companies choosing to over-censor rather than face criminal penalties, or to limit the practice of

41 David Uberti, "How smartphone video changes coverage of police abuse," *Columbia Journalism Review,* April 9, 2015, http://www.cjr.org/analysis/smartphone_video_changes_coverage.php.

42 47 U.S.C. §230 (1998), http://bit.ly/1hlnlbP; *see* Electronic Frontier Foundation, "Section 230 of the Communications Decency Act," http://bit.ly/1EYGbk1.

43 Treating domain names as property subject to criminal forfeiture, 18 U.S.C. §2253.

44 H.R. 285, https://www.congress.gov/114/bills/hr285/BILLS-114hr285rfs.pdf.

45 Center for Democracy & Technology, "Coalition Statement in Opposition to Federal Criminal Publishing Liability," January 29, 2015, http://bit.ly/1OSYquU.

46 The Justice for Victims of Traffickin Act of 2015, Pub. L 144-22, May 29, 2015, https://www.congress.gov/bill/114th-congress/senate-bill/178.

47 Sophia Cope and Adi Kamdar, "SAVE Act Passes in House, Comes One Step Closer to Unnecessarily Chilling Online Speech," Electronic Frontier Foundation, January 29, 2015, https://www.eff.org/deeplinks/2015/01/save-act-passes-house-coming-one-step-closer-chilling-online-speech.

monitoring content altogether so as to avoid "knowledge" of illegal content.[48]

The government has pursued alleged infringements of intellectual property rights on the internet more aggressively in recent years. Since 2010, the Immigration and Customs Enforcement (ICE) division of the Department of Homeland Security has engaged in several rounds of domain-name seizures, with targets including blogs and file-sharin sites that allegedly link to illegal copies of music and films as well as sites that sell counterfeit goods.[49] These seizures have been criticized as overly secretive and lacking in due process. Nevertheless, ICE continues to pursue the project, known as "Operation In Our Sights."[50] In November 2015, ICE partnered with law enforcement agencies from 27 countries to seize 37,479 websites selling counterfeit merchandise.[51]

In 2014, the International Trade Commission (ITC), a trade agency that can block the importation of goods that infringe intellectual property, declared that it had the authority to block the cross-border transmission of data violating a U.S. patent.[52] Civil society groups and academics urged the ITC to reconsider, cautioning that the "decision has enormous ramifications opening the door to internet content blocking efforts rejected by Congress and the public."[53] In a positive step, the Federal Circuit Court of Appeals issued a decision on November 10, 2015 stating that the ITC does not have jurisdiction over electronically imported data.[54]

For copyright infringement claims, the removal of online content is dictated by the safe harbor provisions created in Section 512 of the Digital Millennium Copyright Act (DMCA).[55] Operating through a "notice-and-takedown" mechanism, internet companies are shielded from liability if they remove infringing content upon receipt of a DMCA notice. However, because companies have the incentive to err on the side of caution and remove any hosted content subject to a DMCA notice, there have been occasions where overly broad or fraudulent DMCA claims have resulted in the removal of content that would otherwise be excused under free expression, fair-use, or educational provisions.[56] In some cases, the immediate removal of content through DMCA requests has been used to target political campaign advertisements, since they are unlikely to be challenged in court after the campaign ends and achieve the goal of making the content unavailable during the campaign season.[57]

Major internet companies, including Google, Twitter, Facebook, and Yahoo, publish information about removal requests from governments based on local laws. In its most recent report, Twitter reported receiving three court orders and ninety-eight U.S. government or law enforcement

48 "Coalition Statement in Opposition to Federal Criminal Publishing Liability," Center for Democracy and Technology, January 29, 2015, https://cdt.org/insight/coalition-statement-in-opposition-federal-criminal-publishing-liability/.

49 Agatha Cole, "ICE Domain Name Seizures Threaten Due Process and First Amendment Rights, " American Civil Liberties Union, June 20, 2012, http://bit.ly/1j9cXpl.

50 U.S. Immigration and Customs Enforcement "Operation In Our Sites," May 22, 2014, http://1.usa.gov/1WIeTn7.

51 "Illegal websites seized in global operations," U.S. Immigration and Customs Enforcement, November 30, 2015, https://www.ice.gov/news/releases/illegal-websites-seized-global-operation.

52 United States International Trade Commission, "Certain Digitals Models, Digital Data, and Treatment Plans for Use in Making Incremental Dental Positiong Adjustment Applicances, The Appliances Made Therefrom, and Methods of Making the Same," commission opinion, April 10, 2014, http://bit.ly/1Pf0nky.

53 "Letter to the International Trade Commission," Public Knowledge, April 10, 2015, http://bit.ly/1Z3Ih9u.

54 Aimee N. Soucie, "*ClearCorrect Operating, LLC v. ITC*," Kenyon IP Insight, November 11, 2015, http://www.kenyon.com/NewsEvents/News/2015/11-11-ClearCorrect-Operating-LLC-v-ITC.aspx.

55 17 U.S.C.§ 512, https://www.law.cornell.edu/uscode/text/17/512.

56 Electronic Frontier Foundation, "Lenz v. Universal," https://www.eff.org/cases/lenz-v-universal.

57 Electronic Frontier Foundation, "Once Again, DMCA Abused to Target Political Ads," November 17, 2015, https://www.eff.org/deeplinks/2015/11/once-again-dmca-abused-target-political-ads.

requests to remove or withhold content between July and December of 2015, but did not comply.[58] Yahoo reported receiving three U.S. government removal requests during the same period, and complied with one of them.[59] Google reported receiving 286 U.S. government requests to remove content from its platforms from January to July 2015, and complied fully or partially in 86 percent of instances.[60]

In February 2016, the United States signed the Trans-Pacifi Partnership (TPP) trade agreement with 11 other participating countries following years of secret negotiations that critics said lacked consultation from civil society and other stakeholders.[61] The agreement primarily governs free trade between nations. The text of the TPP agreement, made public in November 2015, included provisions that would extend portions of U.S. copyright terms internationally. Observers noted this would make it more difficul for legislators to reform those laws.[62]

Media, Diversity, and Content Manipulation

The online environment in the United States is vibrant, diverse, and generally free of economic or political constraints. Anyone can start a blog, forum, or social media site to discuss opinions and share news and information. The FCC's decision to protect net neutrality regulations prohibits ISPs from throttling, blocking, or otherwise discriminating against internet traffi based on its content. In addition, over the past year the FCC has questioned whether zero-rating practices by mobile providers violates these net neutrality protections.

At the same time, an increasingly partisan media environment has negatively impacted several online media outlets. Donald Trump, the Republican Party candidate in the 2016 presidential race, refused to issue press credentials for several media outlets whose coverage he deemed unfavorable in late 2015 and early 2016. Reporters from the online media outlets Buzzfeed, *Politico, Huffington Post*, and the *Daily Beast*, as well as from the broadcast and traditional media like the *Washington Post*, Univision, and the *Des Moines Register*, were periodically prevented from attending Trump campaign press events and rallies.[63] These restrictions—and the threat of being banned or blacklisted for unfavorable coverage—risked inhibiting objective reporting on his candidacy.[64]

Another case also indicated the potential for powerful individuals to use personal resources to punish adversarial reporting. In May 2016, news reports revealed that Silicon Valley entrepreneur and venture capitalist Peter Thiel was financin a lawsuit against Gawker Media with the intention of bankrupting the group. The suit involved its flagshi website *Gawker* publishing part of a sex tape

58 Twitter , "Removal Requests," *Transparency Report,* July-December, 2015, https://transparency.twitter.com/removal-requests/2015/jul-dec.

59 Yahoo, "Government Removal Requests," *Transparency Report*, https://transparency.yahoo.com/government-removal-requests/index.htm

60 Google, "Government Requests to Remove Content," https://www.google.com/transparencyreport/removals/government/.

61 TorrentFreak, TPP: U.S. May Not Force DMCA on Other Countries https://torrentfreak.com/tpp-u-s-may-accept-partners-own-isp-liability-frameworks-150707/.

62 Maira Sutton, "How the TPP Will Affect You and Your Digital Rights," Electronic Frontier Foundation, December 8, 2015, https://www.eff.org/deeplinks/2015/12/how-tpp-will-affect-you-and-your-digital-rights.

63 Tom Kludt and Brian Stelter, "'The Blacklist:' Here are the media outlets banned by Donald Trump," CNN, June 14, 2016, http://money.cnn.com/2016/06/14/media/donald-trump-media-blacklist/.

64 Kyle Blaine, "How Donald Trump Bent Television To His Will," Buzzfeed, March 18, 2016, https://www.buzzfeed.com/kyleblaine/how-donald-trump-bent-television-to-his-will?utm_term=.ioJba25Rz#.rmPn4K85k.

involving the retired wrestling celebrity Hulk Hogan (whose real name is Terry G. Bollea).[65] Bollea sued Gawker Media for invasion of privacy, and his lawsuit was backed by more than $10 million from Peter Thiel. Thiel contends that *Gawker* frequently published "damaging" content that targets individuals where "there was no connection with the public interest."[66] Thiel himself had been the subject of commentary by Gawker Media, including an article 2007 that outed Thiel as gay.[67] In June 2016, Gawker Media file for Chapter 11 bankruptcy protection after a Florida jury found the company liable for $140 million in damages.[68] While the group was known for publishing gossip and sensationalist reporting, it also published independent investigative reports, such as one into the online drug trade.[69] Some lawyers argued that the ability of a powerful businessman to fund a personal vendetta against an online media outlet could have worrying repercussions for press freedom, discouraging journalists from investigating individuals with wealth and connections. Thiel also supported Donald Trump, who has called for changing U.S. libel laws to make it easier to sue the media.[70]

Reports of self-censorship among journalists, lawyers, and everyday internet users persist, due to the extensive government surveillance of online communication and activities revealed over the past few years. Although the U.S. Constitution includes core protections for freedom of the press, the U.S. government does bring some enforcement actions against whistleblowers and journalists. The then-Attorney General said in 2013 that the government would not prosecute Glenn Greenwald, the journalist who first published documents leaked by Edward Snowden, or "any journalist who's engaged in true journalistic activities,"[71] but investigations and prosecutions of several other whistleblowers and journalists continue. In 2016, a grand jury investigation into whistleblower website Wikileaks was ongoing. In 2015, news reports said the government had issued warrants to Google to access at least three journalists' Google email accounts and metadata in 2012, and barred the company from notifying the targets.[72] Reporters from several major media outlets have had their communications collected in pursuit of other whistleblower investigations.

Journalists report that their ability to investigate and publish freely has been chilled in recent years due to government pressure and threats to the security of their digital communications. Several recent studies have concluded that the aggressiveness with which the Department of Justice investigates leaks — as well as pervasive government surveillance programs such as those disclosed by Edward Snowden — causes journalists and writers to self-censor and raises concerns about

65 Nick Madigan and Ravi Somaiya "Hulk Hogan Awarded $115 Million in Privacy Suit Against Gawker," *New York Times,* March 18, 2016, http://www.nytimes.com/2016/03/19/business/media/gawker-hulk-hogan-verdict.html.

66 Andrew Ross Sorkin, "Peter Thiel, Tech Billionaire, Reveals Secret War with Gawker," *New York Times*, May 25, 2016, http://www.nytimes.com/2016/05/26/business/dealbook/peter-thiel-tech-billionaire-reveals-secret-war-with-gawker.html.

67 David Streitfeld and Katie Benner, "In Silicon Valley, Gossip, Anger and Revenge," *New York Times,* May 25, 2016, http://www.nytimes.com/2016/05/26/technology/gossip-in-silicon-valley-and-the-digital-age.html.

68 Paul Farhi, "Gawker file for Chapter 11 bankruptcy protection," *Washington Post,* June 10, 2016, https://www.washingtonpost.com/lifestyle/style/gawker-files-fo -chapter-11-bankruptcy-protection/2016/06/10/45ef7420-2f2e-11e6-9b37-42985f6a265c_story.html.

69 Adrian Chen, "The Underground Website Where You Can Buy Any Drug Imaginable," *Gawker,* June 1, 2011, http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160.

70 Katie Rogers and John Herrman, "Thiel-Gawker Fight Raises Concerns About Press Freedom," *New York Times*, May 26, 2016, http://www.nytimes.com/2016/05/27/business/media/thiel-gawker-figh -raises-concerns-about-press-freedom.html?_r=0.

71 Sari Horowitz, "Justice is reviewing criminal cases that used surveillance evidence gathered under FISA," *Washington Post*, November 15, 2013, http://wapo.st/1jKgo5Z.

72 Nick Cumming-Bruce, "WikiLeaks Assails Google and the U.S.," *New York Times*, January 26, 2015, http://nyti.ms/1MUi0n9.

whether they are able to protect the confidentialit of their sources.[73]

Writers responding to a survey by the free expression and literature advocacy group PEN America reported increased self-censorship following the NSA surveillance revelations, according to results published in January 2015. Of 520 respondents, 42 percent reported having altered or avoided social media activities, 31 percent reported deliberately avoiding certain topics in phone or email conversations, and 34 percent reported avoiding writing or speaking about a particular topic.[74] Separately, Human Rights Watch and the American Civil Liberties Union surveyed journalists and lawyers in 2014 about the impact of the revelations on their ability to communicate with sources and clients confidentiall . Journalists reported that government official are significantl less likely to accept interviews due to concerns about anonymity and the ability of the intelligence agencies to access their communications information. Lawyers also reported facing increasing pressure to conceal or secure their communications with clients, particularly in cases with foreign governments or prosecutions that might spark an intelligence inquiry.[75]

Ordinary American citizens have also changed their behavior in response to extensive government surveillance. A study published in *Journalism & Mass Communication Quarterly* in February 2016 found that priming participants with subtle reminders about mass surveillance had a chilling effect on individuals' willingness to publicly express minority opinions online.[76] A March 2015 study by the Pew Research Center on Americans' privacy strategies post-Snowden noted that 30 percent of people surveyed had altered their behavior, including changing privacy settings, being more selective about applications they use, or communicating in person instead of online or over the phone.[77]

Diversity of content online is ensured in part through the protection of network neutrality — a foundational principle of the internet that prohibits network operators from giving preferential treatment to favored content or from blocking disfavored content. In February 2015, the FCC approved a new Open Internet Order that many legal experts believe is based on stronger legal authority than an earlier version of the order issued in 2010,[78] which was later vacated by the

73 Human Rights Watch and American Civil Liberties Union, *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy,* 2014, http://bit.ly/1uz3CL1; PEN America, *Global Chilling: The Impact of Mass Surveillance on International Writers*, January 5, 2015, http://bit.ly/1VBgCYT; see also PEN America, *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*, November 2013, http://bit.ly/1rZ3LXt; and Jesse Holcomb, Amy Mitchell, and Kristen Purcell, *Investigative Journalists and Digital Security: Perceptions of Vulnerability and Changes in Behavior*, Pew Research Center, February 5, 2015, http://pewrsr.ch/1xqJh6i.

74 PEN America, *Global Chilling: The Impact of Mass Surveillance on International Writers.*

75 Human Rights Watch and American Civil Liberties Union, *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy.*

76 Elizabeth Stoycheff, "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring," *Journalism & Mass Communication Quarterly,* 2016, http://m.jmq.sagepub.com/content/early/2016/02/25/1077699016630255.full.pdf; Karen Turner, "Mass surveillance silences minority opinions, according to study," *Washington Post*, March 28, 2016, https://www.washingtonpost.com/news/the-switch/wp/2016/03/28/mass-surveillance-silences-minority-opinions-according-to-study/.

77 Lee Rainieand and Mary Madden, *Americans' Privacy Strategies Post-Snowden*, Pew Research Center, March 16, 2015, http://pewrsr.ch/1MIHWjv.

78 Leticia Miranda, "Verizon, the FCC and What You Need to Know About Net Neutrality," *The Nation,* December 6, 2013, https://www.thenation.com/article/verizon-fcc-and-what-you-need-know-about-net-neutrality/; Federal Communications Commission, "Report and Order: In the Matter of Protecting and Promoting the Open Internet," December 21, 2010, **https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-201A1_Rcd.pdf.**

courts.[79] The order prohibits blocking and unreasonable discrimination on both fi ed and wireless networks, reflectin the growing importance of mobile broadband in the United States. As with the 2010 order, several broadband companies and their trade associations file a lawsuit against the FCC to overturn the rules.[80] On June 14, 2016, the federal appeals court in Washington DC upheld the FCC's authority to issue the Open Internet Order, further solidifying the principle of net neutrality.[81]

In December 2015, the FCC sent letters to Comcast, AT&T, and T-Mobile requesting information about their zero-rating services, which allow unlimited streaming of video content from some services but not from others.[82] FCC Chairman Tom Wheeler stated that the letters were not part of an officia investigation, instead emphasizing that he wanted to make sure these practices are compatible with the goal of maintaining a free and open internet. More than 50 advocacy groups signed a letter to Chairman Wheeler arguing that zero-rating practices violate net neutrality and the spirit of the Open Internet Order, though it does not explicitly prohibit them.[83] As of June 2016, the FCC had not taken any further steps toward formally investigating the zero-rating services.

Digital Activism

Political activity in the United States is increasingly moving online. According to a 2014 survey by the Pew Research Center, between the 2010 and 2014 midterm elections, the proportion of Americans using social media to follow politicians more than doubled, from 6 percent to 16 percent.[84] In 2013, another Pew survey found that 34 percent of American adults used online methods to contact a government officia or to speak out in a public forum; 39 percent had participated in political activity using a social networking site like Facebook or Twitter in the prior year; and 21 percent of email users reported regularly receiving calls to action on social or political issues by email.[85] In addition, political candidates and elected official increasingly use email, mobile apps, and online content to garner support and keep their constituents engaged. Researchers have come to a general consensus that internet use is now deeply linked to political participation and citizenship.[86]

An unprecedented number of Americans used online tools to mobilize in support of the open to advance the FCC's passage of a historic network neutrality order in February 2015. Nearly 4 million Americans contacted the FCC about its proposed net neutrality rules — a record-breaking number that far exceeded the number of comments the agency had received on any topic in its history.[87]

79 Federal Communications Commission, "Report and Order on Remand, Declaratory Ruling, and Order: In the Matter of Protecting and Promoting the Open Internet," GN Docket No. 14-28, February 26, 2015, http://bit.ly/1NOC8bv; Shuli Wang, "The FCC's Net Neutrality Rules on Protecting and Promoting Open Internet," ed. Yaping Zhang, *JOLT Digest*, *Harvard Journal of Law and Technology,* March 23, 2015, http://bit.ly/1Le1RtH.

80 Jim Puzzanghera, "Opponents of FCC's net neutrality rules ask court for partial stay," *LA Times*, May 13, 2015, http://lat.ms/1KW5gvC.

81 Alina Selyukh, "U.S. Appeals Court Upholds Net Neutrality Rules in Full," NPR, June 14, 2016, http://www.npr.org/sections/thetwo-way/2016/06/14/471286113/u-s-appeals-court-holds-up-net-neutrality-rules-in-full.

82 Cecilia Kang, "F.C.C. Asks Comcast, AT&T and T-Mobile About 'Zero-Rating' Services," *The New York Times*, December 17, 2015, http://bits.blogs.nytimes.com/2015/12/17/f-c-c-asks-comcast-att-and-t-mobile-about-zero-rating-services/.

83 Zero rating letter to FCC, March 28, 2016, https://www.eff.org/files/2016/04/07/finalz oratingsign-onletter.fa929bef59a5423089a496b4f909fb97.pdf.

84 Aaron Smith, *Cell Phones, Social Media, and Campaign 2014*, November 3, 2014, http://pewrsr.ch/1rTCqj1.

85 Aaron Smith, *Civic Engagement in the Digital Age*, Pew Research Center, April 25, 2013, http://pewrsr.ch/1nighxK.

86 Karen Mossberger et al., "Digital Citizenship: Broadband, Mobile Use, and Activities Online," (paper presented at International Political Science Association conference, Montreal, Canada, July 2014), http://paperroom.ipsa.org/papers/paper_36182.pdf.

87 Chris Welch, "FCC net neutrality debate passes Janet Jackson's nip slip in total comments," *The Verge*, September 10, 2014, http://bit.ly/1JOEbqg.

The FCC's website crashed several times as a result of the influ of public comments, notably after comedian John Oliver urged Americans to contact the agency in a televised rant that went viral on social media.[88] A broad coalition of grassroots organizations, advocacy groups, and technology companies used online tools to mobilize supporters and pressure the FCC and elected officials In September 2014, members of this coalition staged an "Internet Slowdown Day" in which dozens of high-profil websites displayed a spinning wheel to indicate what the internet could look like in a world without net neutrality protections.[89] When the FCC approved the strongest network neutrality rules in its history in February 2015, policymakers credited the millions of Americans who spoke out in online forums.[90]

Violations of User Rights

The United States has a robust legal framework that supports freedom of expression both online and offline, and the government does not typically prosecute individuals for online speech or activities unless a crime is committed. The broader picture of user rights in America, however, has become increasingly complex as a series of U.S. government practices, policies, and laws touch on, and in some cases appear to violate, the rights of individuals both inside the United States and abroad. Government surveillance is a major concern, especially following revelations about NSA practices, although several of these programs were reformed following the passage of the USA FREEDOM Act in June 2015. Aggressive prosecution under the Computer Fraud and Abuse Act (CFAA) has also been criticized. In addition, the privacy of NGOs, companies, government agencies and individual users is threatened by a growing number of cyberattacks initiated by both domestic and international actors.

Legal Environment

The First Amendment of the U.S. Constitution includes protections for free speech and freedom of the press, and in 1997 the US Supreme Court reaffi med that online speech has the highest level of constitutional protection.[91] Lower courts have consistently struck down attempts to regulate online content.

Nonetheless, aggressive prosecution under the Computer Fraud and Abuse Act (CFAA) has fueled growing criticism of the law's scope and application. Under CFAA, it is illegal to access a computer without authorization, but the law fails to defin the term "without authorization," leaving the provision open to interpretation in the courts.[92] In one prominent case from 2011, programmer and internet activist Aaron Swartz secretly used Massachusetts Institute of Technology servers to download millions of file from JSTOR, a service providing academic articles. Prosecutors sought harsh penalties for Swartz under CFAA, which could have resulted in up to 35 years imprisonment.[93] Swartz committed suicide in 2013 before he could be tried. After his death, a bipartisan group of

88 Soraya Nadia MacDonald, "John Oliver's net neutrality rant may have caused the FCC website to crash," *Washington Post*, June 4, 2014, http://wapo.st/1mzTd8j.

89 Barbara van Schewick, "Is the Internet about to get sloooooow?" *CNN*, September 10, 2014, http://cnn.it/1hlqw37.

90 Craig Aaron, "How We Won Net Neutrality," *The Blog, Huffington Post*, February 26, 2015, http://huff.to/18pvCYE.

91 Reno, Attorney General of the United States, et al. vs. American Civil Liberties Union et al, 521 U.S. 844 (1997), http://bit.ly/1OT33VQ.

92 Electronic Frontier Foundation, "Computer Fraud and Abuse Act Reform," accessed May 14, 2014, https://www.eff.org/issues/cfaa.

93 "Deadly Silence: Aaron Swartz and MIT," *The Economist*, August 3, 2013, http://econ.st/1L21COJ.

lawmakers introduced "Aaron's Law," draft legislation that would prevent the government from using CFAA to prosecute terms of service violations and stop prosecutors from bringing multiple redundant charges for a single crime.[94] The bill was reintroduced in 2015,[95] but in mid-2016 had not garnered enough support to move forward.

Companies are shielded from liability for the activities of their users by Section 230 of the Communications Decency Act (see Content Removal). The Digital Millennium Copyright Act (DMCA) of 1998 provides a safe harbor to intermediaries that take down allegedly infringing material after notice from the copyright owner.[96] A number of U.S. laws also protect speech from harmful corporate actions, including corporate surveillance that may lead users to self-censor, and failure of private actors to sufficientl protect internet users' personal information from unauthorized access (see Surveillance, Privacy, and Anonymity).

There are no legal restrictions on user anonymity on the internet, and constitutional precedents protect the right to anonymous speech in many contexts. There are also state laws that stipulate journalists' right to withhold the identities of anonymous sources, and at least one such law has been found to apply to bloggers.[97] The legal framework for government surveillance, however, has been open to abuse. In June 2015, President Obama signed the USA FREEDOM Act into law in June 2015, introducing some restrictions on the way the NSA can access information about American citizens from their phone records. Other laws used to authorize surveillance have yet to be reformed (see Surveillance, Privacy, and Anonymity).

During the coverage period of this report, the Senate passed a version of the Cybersecurity Information Sharing Act (CISA) bill to promote information sharing about security threats between private companies and federal agencies (see Technical Attacks).[98]

Prosecutions and Detentions for Online Activities

Prosecutions or detentions for online activities, particularly for online speech, are relatively infrequent given broad protections under the First Amendment. However, there have been prosecutions related to threats posted on social media, arrests related to filmin police interactions, and problematic prosecutions under the Computer Fraud and Abuse Act.

On June 1, 2015, the Supreme Court overturned the conviction of a man who posted violent threats on Facebook, marking its fi st ruling on a free speech case involving social media.[99] Anthony Elonis had been sentenced for threatening another person over state lines based on Facebook posts directed at his estranged wife. The Supreme Court ruled that prosecutors had not done enough to

94 Representative Zoe Lofgren, officia website, "Rep Zoe Lofgren Introduces Bipartisan Aaron's Law," press release, June 20, 2013, http://1.usa.gov/1QUsnbx.

95 Kaveh Waddell, "'Aaron's Law' Reintroduced as Lawmakers Wrestle Over Hacking Penalties," *National Journal*, April 21, 2015, http://bit.ly/1Pf4m0u.

96 Center for Democracy and Technology, "Intermediary Liability: Protecting Internet Platforms for Expression and Innovation," April 2010, http://bit.ly/1hlr3Cj.

97 "Apple v. Does," Electronic Frontier Foundation, accessed August 1, 2012, http://www.eff.org/cases/apple-v-does.

98 Consolidated Appropriations Act, 2016, Pub. L. 114-113, December 18, 2015, https://www.congress.gov/bill/114th-congress/house-bill/2029/text.

99 Ariane de Vogue, "SCOTUS rules in favor of man convicted of posting threatening messages on Facebook," CNN, June 1, 2015, http://www.cnn.com/2015/06/01/politics/supreme-court-elonis-facebook-ruling/.

prove that his intent at the time he made the statements was to issue a threat.[100] Analysts said the court's decision gave little guidance to judges and lawyers in future cases and did not weigh in on the First Amendment implications of the case, deciding instead only on the criminal law principle of intent.[101]

Police periodically detain individuals who upload images or broadcast live video of police activity with their phones, posing a threat to First Amendment protections.[102] Most of the arrests have been made on unrelated charges, such as obstruction or resisting arrest, since openly filmin police activity is a protected right. Several citizen journalists were arrested or reported police intimidation while attempting to record police activity with smartphones in 2014 and 2015 during protests in the aftermath of the police killings of Eric Garner, Freddie Gray, and Michael Brown in New York, Baltimore, and Ferguson, Missouri respectively. During protests in Ferguson, at least 21 journalists were arrested, including reporters for the *Huffington Post* and the *Washington Post*;[103] and Antonio French, a city alderman in St. Louis, was detained by the police while covering police activity on Twitter, Vine, and Instagram. In July 2016, outside the coverage period of this report, police briefl detained or harassed individuals who shared footage online of the fatal shootings by police of Alton Sterling in Baton Rouge, Louisiana and Philando Castile in St. Anthony, Minnesota (see Intimidation and Violence).[104]

During the reporting period, the government used the Computer Fraud and Abuse Act to prosecute Matthew Keys, a former Tribune Company journalist and social media editor who had given log-in credentials to the hacking group Anonymous. The hackers used the information to change the headline of a story on the *Los Angeles Times* website. Charged with a felony and facing a maximum penalty of 25 years in prison, Keys was convicted in October 2015 and sentenced to two years' imprisonment on April 13, 2016.[105] Some critics of CFAA argued that Keys' sentencing was overly harsh, and that many of his crimes could be charged as misdemeanors.[106]

Many states also have their own laws related to computer hacking or unauthorized access. Several smaller cases in the past few years highlight the shortcomings and lack of proportionality of these laws. In December 2014, 21-year-old Georgia Institute of Technology student Ryan Gregory Pickren was arrested on felony computer trespass charges after hacking into the rival University of Georgia's online calendar as part of a prank leading up to a football game between the two schools. According to Georgia state law, a person convicted for computer trespass—define as "alter[ing], damag[ing] or in any way caus[ing] the malfunction of a computer, computer network, or computer program regardless of how long it occurs"—faces a maximum penalty of 15 years in prison and a $50,000

100 Adam Liptak, "Supreme Court Overturns Conviction in Online Threats Case, Citing Intent," *New York Times*, June 1, 2015, http://www.nytimes.com/2015/06/02/us/supreme-court-rules-in-anthony-elonis-online-threats-case.html?_r=0.

101 Adam Liptak, "Supreme Court Overturns Conviction in Online Threats Case, Citing Intent," *New York Times*, June 1, 2015, http://www.nytimes.com/2015/06/02/us/supreme-court-rules-in-anthony-elonis-online-threats-case.html?_r=0.

102 Frank Eltman, "Citizens filmin police often fin themselves arrested," *Albuquerque Journal*, August 30, 2015, http://www.abqjournal.com/636460/citizens-filming-police- ften-find-themsel es-arrested.html.

103 PEN America, *Press Freedom Under Fire in Ferguson*, October 27, 2014, http://bit.ly/1zDIsOl.

104 PEN America, "Retaliation For Documenting Police," petition, September 12, 2016, https://pen.org/blog/retaliation-documenting-police.

105 Christopher Mele, "Matthew Keys Gets 2 Years in Prison in Los Angeles Times Hacking Case," *New York Times*, April 13, 2016, http://www.nytimes.com/2016/04/14/business/media/matthew-keys-gets-2-years-in-prison-in-los-angeles-times-hacking-case.html.

106 Kim Zetter, "Matthew Keys Sentenced to Two Years for Aiding Anonymous," *Wired*, April 13, 2016, https://www.wired.com/2016/04/journalist-matthew-keys-sentenced-two-years-aiding-anonymous/.

fine [107] Pickren was ultimately accepted into a pretrial intervention program in lieu of prosecution. In a separate case in early 2015, Florida authorities arrested 14-year-old Domanik Green on felony cybercrime charges after the boy used a teacher's administrative password to log onto a school computer and change its desktop background.[108]

Surveillance, Privacy, and Anonymity

The passage of the Uniting and Strengthening America by Fulfillin Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act) in June 2015 marked the most significan reform to U.S. surveillance practices in recent decades. Despite this reform, however, a number of problematic provisions within U.S. law revealed during the 2013 NSA leaks remain in effect.

Under a set of complex statutes, U.S. law enforcement and intelligence agencies can monitor communications content and communications records, or metadata, under varying degrees of oversight as part of criminal or national security investigations. (Metadata can reveal where and when communications took place, among other details.) The government may request companies store such data for up to 180 days under the Stored Communications Act, but how they otherwise collect and store communications content and records varies by company.[109]

Law enforcement access to metadata generally requires a subpoena issued by a prosecutor or investigator without judicial approval;[110] a warrant is only required in California under the California Electronic Communications Privacy Act, which went into effect on January 1, 2016.[111] In criminal probes, law enforcement authorities can monitor the content of internet communications in real time only if they have obtained an order issued by a judge, under a standard that is actually a little higher than the one established by the constitution for searches of physical places. The order must reflec a findin that there is probable cause to believe that a crime has been, is being, or is about to be committed.

The status of stored communications is more uncertain. One federal appeals court has ruled that the Constitution applies to stored communications, so that a judicial warrant is required for government access.[112] However, the 1986 Electronic Communications Privacy Act (ECPA) states that the government can obtain access to email or other documents stored in the cloud with a subpoena.[113] Bills to update ECPA have had significan support, including from the White House. In April 2016, the House of Representatives passed the Email Privacy Act, which would require the government

107 Joe Johnson, "Georgia Tech student who hacked into UGA computer network gets pretrial diversion," *Athens Banner-Herald*, February 26, 2015, http://bit.ly/1FSEllk.

108 Josh Solomon, "Middle school student charged with cybercrime in Holiday," *Tampa Bay Times*, April 9, 2015, http://bit.ly/1ybpTBg.

109 Electronic Frontier Foundation, "Mandatory Data Retention: United States," https://www.eff.org/issues/mandatory-data-retention/us.

110 Electronic Frontier Foundation, "Mandatory Data Retention: United States;" Center for Constitutional Rights, "Surveillance After the USA Freedom Act: How Much Has Changed?," *Huffington Post*, December 17, 2015, http://www.huffing onpost.com/the-center-for-constitutional-rights/surveillance-after-the-us_b_8827952.html.

111 American Civil Liberties Union, "California Electronic Communications Privacy Act (CalECPA) - SB 178," https://www.aclunc.org/our-work/legislation/calecpa.

112 United States v. Warshak, 09-3176, United States Court of Appeals for the Sixth Circuit.

113 Ibid.

to obtain a probable cause warrant before accessing email or other private communications stored with cloud service providers.[114] As of May 2016, it was awaiting review in the Senate.[115]

The USA PATRIOT Act, passed following the terrorist attacks of September 11, 2001, expanded government surveillance and investigative powers in terrorism and criminal investigations, permitting intelligence agencies secret access to a wide range of private business records "relevant" to terrorism investigations under Section 215 with authorization from the Foreign Intelligence Surveillance Court (FISA Court), a closed court established under the FISA Act in 1978 to approve government surveillance requests. Other provisions of the PATRIOT Act granted broad authority to conduct roving wiretaps of unidentifie or "John Doe" targets, and to wiretap "lone wolf" suspects who have no known connections to terrorist networks. These expiring provisions were renewed for four years in May 2011.[116]

In June 2013, news outlets revealed a series of secret documents leaked by former NSA contractor Edward Snowden which provided new information about government surveillance activities,[117] including bulk collection of phone records based on the PATRIOT Act. According to the documents, the FISA court had interpreted Section 215 as grounds to order telecommunications companies to provide the NSA with records of all phone calls made to, from, and within the country on an ongoing basis.[118] NSA analysts conducted broad queries on this data without oversight.[119] In May 2015, the Second Circuit Court of Appeals ruled that the NSA's bulk collection program under PATRIOT ACT Section 215 was illegal. The court did not comment on the constitutional questions raised by bulk collection.[120]

On June 2, 2015, President Obama signed the USA FREEDOM Act into law. The Act extended the expiring provisions of the PATRIOT Act, including the roving wiretaps of John Doe targets and lone wolf surveillance authority, but significantl reformed Section 215.[121] The law replaced the bulk collection program with a system that allows the NSA to access records held by phone companies with an order from the FISA court.[122] Requests for that access require the use of a "specifi selection term" (SST) representing an "individual, account, or personal device,"[123] which is intended to prohibit broad applications for records based on zip code or other indicators, and can only be extended or

114 Sophia Cope, "House Advances Email Privacy Act, Setting the Stage for Vital Privacy Reform," Electronic Frontier Foundation, April 27, 2016, https://www.eff.org/deeplinks/2016/04/house-advances-email-privacy-act-setting-stage-vital-privacy-reform.

115 H.R. 699 Email Privacy Act, https://www.congress.gov/bill/114th-congress/house-bill/699/text.

116 "Patriot Act Excesses," New York Times, October 7, 2009, http://www.nytimes.com/2009/10/08/opinion/08thu1.html.

117 E.g. Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," The Guardian, June 5, 2013, http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order.

118 Aubra Anthony, "When Metadata Becomes Megadata: What Government Can Learn," Center for Democracy and Technology PolicyBeta Blog, June 17, 2013, https://www.cdt.org/blogs/1706when-metadata-becomes-megadata-what-government-can-learn-metadata.

119 "Comparing Two Secret Surveillance Programs," The New York Times, June 7, 2013, http://www.nytimes.com/interactive/2013/06/07/us/comparing-two-secret-surveillance-programs.html.

120 Marty Lederman, "BREAKING: Second Circuit rules that Section 215 does not authorize telephony bulk collection program," Just Security, May 7, 2015, http://bit.ly/1j9kTqO.

121 "USA Freedom Act: What's in, what's out," *Washington Post,* June 2, 2015, https://www.washingtonpost.com/graphics/politics/usa-freedom-act/.

122 Aarti Shahani, "Phone Carriers Are Tight-Lipped On How They Will Comply With New Surveillance Law," NPR, June 4, 2015, http://www.npr.org/sections/alltechconsidered/2015/06/04/411870819/phone-carriers-are-tight-lipped-over-law-that-overhauls-nsa-surveillance.

123 Rainey Reitman, "The New USA Freedom Act: A Step in the Right Direction, but More Must Be Done," Electronic Frontier Foundation, April 30, 2015, https://www.eff.org/deeplinks/2015/04/new-usa-freedom-act-step-right-direction-more-must-be-done.

renewed in certain circumstances.[124] The SST provision also applies when intelligence agents use FISA pen registers and trap and trace devices, instruments that will capture a phone's outgoing or incoming records, and to national security letters, secret subpoenas to request call records issued by the FBI.[125]

The USA FREEDOM Act also required that the FISA court appoint an *amicus curiae*, an individual (or several) qualifie to provide legal arguments that "advance the protection of individual privacy and civil liberties."[126] During the coverage period of this report, the court designated six individuals eligible to serve as an amicus curiae, fi e in November 2015, and a sixth on March 31, 2016.[127] Despite these significan improvements, several privacy protections that had been included in previous versions of the bill were removed from the fina text, such as revisions to Section 702 of the FISA Act (see below) that aimed to limit incidental collection or "reverse targeting" of U.S. citizens' data.[128]

Other surveillance programs revealed by the NSA leaks were authorized under laws which, though partially reformed since they were exposed in 2013, still contain scope for surveillance that lacks oversight, specificit , and transparency.

- *Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008*: Section 702 was used to authorize PRISM and "Upstream" collection, the controversial programs under which the NSA reportedly collects users' communications data—including the content—directly from U.S. tech companies and through the physical infrastructure of undersea cables.[129] Section 702 only authorizes the collection of information about foreign citizens, yet the content of Americans' communications is also collected and stored in a searchable database.[130] The USA FREEDOM Act made no changes to this practice or to the NSA's access to the communications content collected. It limits the use of information about U.S. citizens in court or in other government proceedings if the NSA did not follow existing procedures to minimize the likelihood of collecting that information. The FISA court will determine whether or not those procedures were followed.[131] The FISA Amendments Act is set to expire in December 2017, offering an opportunity for reform.[132]

- *Executive Order 12333*: Originally issued in 1981, Executive Order 12333 outlines how and when the NSA or other agencies may conduct surveillance on U.S. citizens and other

124 "USA Freedom Act of 2015," Council on Foreign Relations, June 2, 2015, http://www.cfr.org/intelligence/usa-freedom-act-2015/p36594.

125 Uniting and Strengthening America by Fulfillin Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act), Pub. L. 114-23, June 1, 2015, https://www.congress.gov/bill/114th-congress/house-bill/2048/text.

126 USA FREEDOM Act of 2015, Sec. 401.

127 United States Foreign Intelligence Surveillance Court, "Amici Curiae," http://www.fisc.uscou ts.gov/amici-curiae.

128 See text of House version of USA FREEDOM ACT (2014): H.R. 3361, https://www.congress.gov/113/bills/hr3361/BILLS-113hr3361rh.pdf.

129 Brett Max Kaufman, "A Guide to What We Know About the NSA's Dragnet Searches of Your Communications," ACLU, August 9, 2013, https://www.aclu.org/blog/guide-what-we-now-know-about-nsas-dragnet-searches-your-communications.

130 Dia Kayyali, "The Way the NSA Uses Section 702 is Deeply Troubling. Here's Why." Electronic Frontier Foundation, May 7, 2014, https://www.eff.org/deeplinks/2014/05/way-nsa-uses-section-702-deeply-troubling-heres-why.

131 See USA FREEDOM Act of 2015, Sec. 301, and 50 U.S.C. 1881a(i)(3), available at: https://www.gpo.gov/fdsys/pkg/USCODE-2011-title50/pdf/USCODE-2011-title50-chap36-subchapVI-sec1881a.pdf.

132 Cindy Cohn and Rainey Reitman, "USA Freedom Act Passes: What We Celebrate, What We Mourn, and Where We Go From Here," Electronic Frontier Foundation, June 2, 2015, https://www.eff.org/deeplinks/2015/05/usa-freedom-act-passes-what-we-celebrate-what-we-mourn-and-where-we-go-here.

individuals within the United States,[133] authorizing the collection of U.S. citizens' metadata and the content of communications if that data is collected "incidentally."[134] The extent of current NSA practices authorized under EO12333 is unclear, but documents from the NSA leaks suggest that EO12333 was used to authorize the so-called "MYSTIC" program, which was reportedly used to capture all of the incoming and outgoing phone calls of one or more target countries on a rolling basis. *The Intercept* identifie the Bahamas, Mexico, Kenya, and the Philippines as targets in 2014.[135] In December 2014, Congress passed a law that included a requirement that the NSA develop "procedures for the retention of incidentally acquired communications" collected pursuant to Executive Order 12333, and that such communications may not be retained for more than fi e years except when subject to certain broad exceptions.[136] In January 2015, the president updated a 2014 policy directive that put in place important new restrictions relevant to EO12333 on the use of information collected in bulk for foreign intelligence purposes.[137] Civil society groups continue to campaign for its complete reform.[138]

The USA FREEDOM Act also changed the way private companies publicly report on government requests they receive for user information. The U.S. Department of Justice (DOJ) limits the disclosure of information about national security letters, including in the transparency reports voluntarily published by some internet companies and service providers.[139] In 2014, the DOJ reached a settlement with Facebook, Google, LinkedIn, Microsoft, and Yahoo that would permit the companies to disclose the number of government requests they receive, but only in aggregated bands of 0-249 or 0-999.[140] Twitter, not a party to the settlement, file suit against the DOJ in October 2014 on grounds that the rules amount to an unconstitutional prior restraint that violates the company's First Amendment rights.[141] In May 2016, a judge partially dismissed Twitter's case but gave them the opportunity to refile [142] The USA FREEDOM Act allows companies the option of more granular reporting, though reports containing more detail are still subject to time delays and their frequency is limited.[143]

User data is otherwise protected under Section 5 of the Federal Trade Commission Act (FTCA),

133 Executive Order 12333—United States Intelligence Activities. Federal Register, National Archives. http://www.archives.gov/federal-register/codification/e ecutive-order/12333.html.

134 "Executive Order 12333," Electronic Privacy Information Center, https://epic.org/privacy/surveillance/12333/.

135 Barton Gellman and Ashkan Soltani, "NSA surveillance program reaches 'into the past' to retrieve, replay phone calls," *Washington Post*, March 18, 2014, https://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html; Ryan Devereaux, Glenn Greenwald, Laura Poitras, "Data Pirates of the Caribbean," *The Intercept*, May 19, 2014, https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/.

136 H.R. 4681, Intelligence Authorization Act for Fiscal Year 2015 Sec. 309, 113th Cong. (2014).

137 Presidential Policy Directive – Signals Intelligence Activities PPD-28, January 17, 2014, http://1.usa.gov/1MUm5Yz.

138 Human Rights Watch, "Strengthen the USA Freedom Act," May 19, 2015, https://www.hrw.org/news/2015/05/19/strengthen-usa-freedom-act.

139 Craig Timberg & Adam Goldman, "U.S. to Allow Companies to Disclose More Details on Government Requests for Data," *Washington Post,* January 27, 2014, http://wapo.st/LhuLxw.

140 Offic of the Deputy Attorney General, email correspondence fto Facebook, Google, LinkedIn, Microsoft, and Yahoo general counsels, January 27, 2014, http://1.usa.gov/1IuJYqL.

141 Ben Lee, "Taking the figh for #transparency to court," *Twitter Blog*, October 7, 2014, http://bit.ly/Zc3Mtm; Alexei Oreskovic, "Twitter Sues U.S. Justice Department for Right to Reveal Surveillance Requests," *Reuters,* October 7, 2014, http://reut.rs/1yLKbRe.

142 "Twitter lawsuit partly dismissed over U.S. information requests," Reuters, May 2, 2016, http://www.reuters.com/article/us-twitter-government-ruling-idUSKCN0XT1RK

143 For additional information on reporting standards, please reference: USA Freedom Act, H.R. 2048 (2015), http://1.usa.gov/1jKsHzc.

which has been interpreted to prohibit entities operating over the internet from deceiving users about what personal information is being collected and how it is being used, as well as from using personal information in ways that harm users without offering countervailing benefits In addition, the FTCA has been interpreted to require entities that collect users' personal information to adopt reasonable security measures to safeguard it from unauthorized access. State-level laws in 47 U.S. states and the District of Columbia also require entities that collect personal information to notify consumers—and, usually, consumer protection agencies—when they suffer a security breach leading to unauthorized access of personal information. Section 222 of the Telecommunications Act prohibits telecommunications carriers from sharing or using information about their customers' use of the service for other purposes without customer consent. This provision has historically only applied to phone companies' records about phone customers, but following the FCC's net neutrality order, it now also applies to ISPs' records about broadband customers.[144]

While there are no legal restrictions on anonymous communication online, some social media platforms require users to register using their real names through Terms of Service or other contracts.[145] Online anonymity has been challenged in cases involving hate speech, defamation or libel. In one recent example, a Virginia court tried to compel the crowdsourced review platform Yelp to reveal the identities of anonymous users, before the Supreme Court of Virginia ruled that they did not have the authority.[146]

The 2011 National Strategy for Trusted Identities in Cyberspace (NSTIC) specificall endorsed anonymous online speech.[147] It supported the creation of an "identity ecosystem" in which internet users and organizations can more completely trust one another's identities and systems when carrying out online transactions.[148]

By contrast, other government agencies may have acted to undermine user anonymity. Documents leaked by Edward Snowden suggest that the NSA may have engaged in cyberattacks, including a project to develop malware targeting users of Tor, a tool that enables people to communicate anonymously online,[149] as well as efforts to undermine international technical standards for encryption.[150] Law enforcement officials technology experts, and privacy advocates continue to debate whether companies should be allowed to market products with strong encryption that neither they nor the government can decrypt.

Following a terrorist attack in San Bernardino in December 2015, the U.S. government sought to compel Apple to unlock a passcode-protected iPhone belonging to one of the perpetrators. Because some iPhones are programmed to permanently block access to all of the phone's encrypted data once an incorrect passcode is entered too many times, the government issued a court order that

144 Alex Bradshaw, Stan Adams, "FCC Should Act to Protect Broadband Customers' Data," CDT, January 20, 2016, https://cdt.org/blog/fcc-should-act-to-protect-broadband-customers-data/.

145 Erica Newland, et. al., *Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users*, Global Network Initiative, September 2011, http://cyber.law.harvard.edu/node/7080.

146 Justin Jouvenal, "Yelp won't have to turn over names of anonymous users after court ruling" *Washington Post,* 16 April 2015, http://wapo.st/1MbcE48.

147 Jay Stanley, "Don't Put Your Trust in 'Trusted Identities,'" American Civil Liberties Union, January 7, 2011, http://bit.ly/1M7hILh; See also, Jim Dempsey, "New Urban Myth: The Internet ID Scare," *Policy Beta* (blog), Center for Democracy and Technology, January 11, 2011, http://bit.ly/1Oi3I2U.

148 National Strategy for Trusted Identities in Cyberspace, "About NISTIC," accessed May, 14, 2014, http://1.usa.gov/1hluGbe.

149 "Costs to Cybersecurity" in Danielle Kehl et al., "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom, and Cybersecurity," New America's Open Technology Institute, July 2014, http://bit.ly/1GsrIbD.

150 James Ball, Julian Borger and Glenn Greenwald, "Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security," *The Guardian,* September 6, 2013, http://gu.com/p/3thvv/stw.

would compel Apple to create new software enabling the FBI to access the phone.[151] This and similar cases raised the question of the degree to which the courts can force technology companies to comply with court orders, particularly those that would require the companies to alter their products. Security experts argued that requiring companies to create "backdoors" for law enforcement to access encrypted data would undermine security and public trust.[152]

Conversely, there have been efforts to codify rules that would bar the government from requiring surveillance backdoors. In 2014, the U.S. House of Representatives approved an amendment to a bill governing appropriations which would ban spending on government-mandated backdoors with overwhelming bipartisan support, although later negotiations prevented it from being adopted into the fina bill.[153] The House approved two similar amendments in 2015.[154] Building on that support, the Secure Data Act was introduced in Congress in December 2014, which would similarly prohibit the government from requiring that companies weaken the security of their products or insert backdoors to facilitate access.[155] As of mid-2016, no further action had been taken.

Despite vigorous debate, there have been no legislative changes regarding the use of encryption, nor is there any indication that the government is currently planning to move forward with the technical solutions it has proposed.[156] While the Communications Assistance for Law Enforcement Act (CALEA) currently requires telephone companies, broadband carriers, and interconnected Voice over Internet Protocol (VoIP) providers to design their systems so that communications can be easily intercepted when government agencies have the legal authority to do so, it does not cover online communications tools such as Gmail, Skype, and Facebook.[157] Calls to update CALEA to cover online applications and communications have not been successful. In 2013, 20 technical experts published a paper explaining why such a proposal (known as "CALEA II") would create significan internet security risks.[158]

Other legal implications of law enforcement access to devices have been debated in the courts. In 2014, a judge ruled that police could compel someone to unlock their smartphone using a fingerprin scanner, reasoning that this would be similar to requiring a DNA swab or handwriting sample.[159] In September 2015, in a separate case involving a passcode-protected phone, a federal judge in Pennsylvania ruled that law enforcement could not compel someone to produce their

151 Julia Angwin, "What's Really At Stake in the Apple Encryption Debate," ProPublica, February 24, 2016, https://www.propublica.org/article/whats-really-at-stake-in-the-apple-encryption-debate.

152 Press Release, "Open Technology Institute Opposes Government Attempt to Mandate Backdoor into Apple iPhone," Open Technology Institute, February 17, 2016, https://www.newamerica.org/oti/press-releases/open-technology-institute-opposes-government-attempt-to-mandate-backdoor-into-apple-iphone/.

153 See Amendment to H.R. 4870, the Department of Defense Appropriations Act, offered by Representative Massie of Connecticut. The Amendment "prohibits funds for the government to request that products or services support lawful electronic surveillance": The FY 2015 Department of Defense Appropriations Bill: House Adopted Amendments, H.R. 4870 (2014), http://1.usa.gov/1jDUJpd.

154 Robyn Greene, "Representatives Should Vote "Yes" on Three Amendments to Prohibit Bulk Collection and to Protect Encryption," New America Open Technology Institute, June 2, 2015 [updated June 3, 2015], http://bit.ly/1M7pLHQ.

155 Secure Data Act of 2014, S.2981, 113th Cong. (2014), http://1.usa.gov/1Lc1Eme.

156 Cory Bennett, "Lawmakers skeptical of FBI's encryption warnings," *The Hill*, April 29, 2015, http://bit.ly/1bGPbwO.

157 Charlie Savage, "U.S. Tries to Make it Easier to Wiretap the Internet." *New York Times*, September 27, 2010, http://nyti.ms/1WIzNlX; See also Declan McCullagh, "FBI: We Need Wiretap-Ready Websites – Now," *CNET*, May 4, 2012, http://cnet.co/1iRh6vA.

158 Ben Adida et al, *CALEA II: Risks of Wiretap Modifications to Endpoints*, Center for Democracy & Technology, May 17, 2013, http://bit.ly/1Gsv12v.

159 Lily Hay Newman, "Law Enforcement Can Make You Unlock Devices with Your Fingerprint in Virginia," *Slate*, October 31, 2014, http://www.slate.com/blogs/future_tense/2014/10/31/virginia_police_can_make_you_unlike_your_smartphone_with_your_fingerprint.htm .

passcode as this would involve the individual's personal thoughts or knowledge, which are protected by the Fifth Amendment right against self-incrimination.[160]

In March 2016, a Maryland state appellate court issued a ruling stating that law enforcement must obtain a warrant before using "covert cell phone tracking devices" known by the product name Stingray.[161] Stingray devices act like cell phone towers, causing nearby cell phones to send it identifying information and thus allowing law enforcement to track targeted phones or determine the phone numbers of people in a nearby area. In its decision, the court rejected the argument that individuals are effectively "volunteering" their private information when they choose to turn on their phones, since doing so allows third parties (the phone company's cell towers) to send and receive signals from the phone.[162] This was the fi st court decision addressing whether a warrant is required in the use of Stringray devices[163]

In addition to monitoring private communications, law enforcement agencies have also used open, public websites, and social media platforms to monitor different groups for suspected criminal activity. The New York Police Department (NYPD) is one such agency, with the Associated Press reporting that, from 2006 onward, the NYPD Cyber Intelligence unit monitored blogs, websites, and online forums of Muslim student groups and produced a series of secret "Muslim Student Association" reports describing group activities, religious instruction, and the frequency of prayer by the groups.[164] In April 2014, the NYPD closed down one unit that monitored locations associated with the Muslim community, including mosques and businesses.[165] Civil liberties advocates welcomed this step but warned that other NYPD units may still be using discriminatory practices.

Federal intelligence agencies closely monitor social media as part of their terrorism investigations.[166] This monitoring has led to the identificatio of specifi targets, like an Ohio man arrested in 2014 for planning to attack the Capitol who drew the attention of the FBI through Twitter.[167] Since monitoring is not limited to the targets of investigations, it encompasses innocent individuals' online activities and may chill online speech.

Intimidation and Violence

Bloggers and other ICT users generally are not subject to extralegal intimidation or violence from state actors. However, police have used intimidation and threats to discourage bystanders from

160 Lily Hay Newman, "Federal Judge Says Law Enforcement Can't Make You Hand Over Your Smartphone Passcode," *Slate*, September 25, 2015, http://www.slate.com/blogs/future_tense/2015/09/25/court_rules_that_defendants_don_t_have_to_provide_smartphone_passcodes.html.

161 Spencer S. Hsu, "A Maryland court is the fi st to require a warrant for covert cellphone tracking," *Washington Post,* March 31, 2016, https://www.washingtonpost.com/world/national-security/a-maryland-court-is-the-fi st-to-require-a-warrant-for-covert-cellphone-tracking/2016/03/31/472d9b0a-f74d-11e5-8b23-538270a1ca31_story.html.

162 Joshua Kopstein, "Maryland Attorney General: If You Don't Want To Be Tracked, Turn Off Your Phone," *Motherboard,* February 4, 2016, https://motherboard.vice.com/read/maryland-attorney-general-if-you-dont-want-to-be-tracked-turn-off-your-phone.

163 Alex Emmons, "Maryland Appellate Court Rebukes Police for Concealing Use of Stingrays," *The Intercept,* March 31, 2016, https://theintercept.com/2016/03/31/maryland-appellate-court-rebukes-police-for-concealing-use-of-stingrays/;

164 Associated Press,"AP's Probe Into NYPD Intelligence Operations," accessed May 5, 2015 http://bit.ly/L3pdWB.

165 Matt Appuzzo and Joseph Goldstein, "NY Drops Unit that Spied on Muslims," *New York Times*, Apr. 15, 2014, http://nyti.ms/1evekec.

166 Kevin Sullivan, "Three American teens, recruited online, are caught trying to join the Islamic State," *Washington Post*, December 8, 2014, http://wapo.st/1L2hEIz.

167 Sari Horwitz, "Ohio man arrested in alleged plot to attack Capitol," *Washington Post*, January 14, 2015, http://wapo.st/1Rr8cml.

filmin or from uploading footage, particularly surrounding protests related to police violence against African Americans. Citizens have a legal right to fil police interactions openly if they are not interfering with police activities. Covert filmin may fall under illegal wiretapping regulations.[168]

In April 2015, Baltimore police arrested Kevin Moore after he filme them arresting Freddie Gray and shared the footage on YouTube. Gray died from injuries sustained in police custody, prompting widespread protests against police abuse. Moore was released without charge but subsequently reported being followed by the police along with other forms of intimidation.[169] A similar pattern of harassment was observed in July 2016, after the coverage period of this report, when police in Louisiana detained store owner Abdullah Muflah for six hours and confisca ed his cellphone after he filme the fatal shooting of Alton Sterling by police. Chris LeDay, a Georgia-based musician who shared another video of the same incident on Facebook, was arrested soon after for unpaid traffi fines [170]

Technical Attacks

Financial, commercial, and governmental entities in the United States are targets of significan cyberattacks. Government policies and laws are in place to prevent and protect against cyberattacks, though many question their impact, effectiveness, and respect for civil liberties.

In June 2015, government official reported two successive cyberattacks beginning in March 2014 which resulted in hackers breaching the Offic of Personal Management (OPM) and other executive agencies.[171] The social security numbers of over 21.5 million individuals, including former employees and their spouses or acquaintances, were stolen.[172] Some analysts linked the attack to a Chinese state-backed hacker known as "Deep Panda."[173] Some commentators said the Obama administration refrained from accusing China of involvement in the hack to avoid disclosing evidence that might reveal the United States' own cybersecurity capabilities.[174] The Chinese government denied involvement, and reported the arrest of several individuals they said carried out the hack prior to President Xi Jinping's visit to the U.S. in September.[175]

In response to these incidents and others, the U.S. has taken legal and policy measures to address growing cyber-threats. In December 2015, President Obama signed an omnibus bill that included

168 Dia Kayyali, "Want to Record the Cops? Know Your Rights," Electronic Frontier Foundation, April 16, 2015, https://www.eff.org/deeplinks/2015/04/want-record-cops-know-your-rights.

169 Mariah Stewart, "Man Who Filmed Freddie Gray Arrest Detained By Baltimore Police, Along With Ferguson Video Activists," *Huffington Post*, http://huff.to/1VBuAtR.

170 Amy Goodman & Denis Moynihan, "Videotaping a Crime Is Not a Crime," Democracy Now, July 14, 2016, http://www.democracynow.org/2016/7/14/videotaping_a_crime_is_not_a.

171 Lily Hay Newman, "Government Discovered Employee Data Breach While It Was Trying to Upgrade Security," *Slate,* June 5, 2015, http://www.slate.com/blogs/future_tense/2015/06/05/office_ f_personnel_management_discovered_hack_while_trying_to_upgrade_security.html.

172 Brian Naylor, "OPM: 21.5 Million Social Security Numbers Stolen From Government Computers," NPR, July 9, 2015, http://www.npr.org/sections/thetwo-way/2015/07/09/421502905/opm-21-5-million-social-security-numbers-stolen-from-government-computers.

173 David Perera, "Researchers: 'Deep Panda' Behind Hacking of Federal Data," *Politico*, June 4, 2015, http://politi.co/1OgcZad.

174 Ellen Nakashima, "U.S. decides against publicly blaming China for data hack," *Washington Post*, July 22, 2015, https://www.washingtonpost.com/world/national-security/us-avoids-blaming-china-in-data-theft-seen-as-fair-game-in-espionage/2015/07/21/03779096-2eee-11e5-8353-1215475949f4_story.html.

175 Ellen Nakashima, "Chinese government has arrested hackers it says breached OPM database," *Washington Post*, December 2, 2015, https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html.

a version of the Cybersecurity Information Sharing Act (CISA) already passed in the Senate. The Act intends to mitigate cybersecurity threats by requiring the Department of Homeland Security to share information about threats with private companies, and by allowing companies to voluntarily disclose information to federal agencies without fear of being sued for violating user privacy.[176]

Civil liberties advocates said that the fina text of the bill did not include strong enough privacy protections, and weakened requirements in earlier drafts to remove from disclosures any personal information not needed to identify cybersecurity threats. Critics also said that allowing companies to voluntarily disclose data to any federal agency—including the Department of Defense and the NSA—undermines civilian control of cybersecurity programs and would blur the line between the use of this data for cybersecurity versus law enforcement purposes.;[177] and that the text authorizes "defensive measures" even if these cause damage to others' networks or data, though it prohibits measures that provide unauthorized access to other systems.[178]

President Obama issued two Executive Orders to address cyberattacks in 2015. In January, in response to a high-profil attack on Sony Pictures Entertainment's internal networks apparently carried out to prevent it from releasing a controversial comedy about North Korea, Obama issued an order authorizing the Treasury Department to impose sanctions on individuals and entities associated with the North Korean government.[179] In April, the White House issued an Executive Order permitting the U.S. Department of the Treasury to levy sanctions against individuals or companies that conduct "significan malicious cyber-enabled activities."[180]

176 Consolidated Appropriations Act, 2016, Pub. L. 114-113, December 18, 2015, https://www.congress.gov/bill/114th-congress/house-bill/2029/text.

177 Jadzia Butler, Greg Nojeim, "Cybersecurity Information Sharing in the 'Ominous' Budget Bill: A Setback for Privacy," Center for Democracy and Technology, December 17, 2015, https://cdt.org/blog/cybersecurity-information-sharing-in-the-ominous-budget-bill-a-setback-for-privacy/.

178 Jadzia Butler, Greg Nojeim, "Cybersecurity Information Sharing in the 'Ominous' Budget Bill: A Setback for Privacy," Center for Democracy and Technology, December 17, 2015, https://cdt.org/blog/cybersecurity-information-sharing-in-the-ominous-budget-bill-a-setback-for-privacy/.

179 Zeke J. Miller, "U.S. Sanctions North Korea Over Sony Hack," *Time*, January 2, 2015, http://ti.me/1JP4EnL.

180 , The White House, Offic of the Press Secretary, "Executive Order: Blocking the Property of Certain Persons Engaging in Significan Malicious Cyber-Enabled Activities," April 1, 2015, http://1.usa.gov/1F2sjPD.

Freedom House

Uzbekistan

	2015	2016
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	19	20
Limits on Content (0-35)	28	28
Violations of User Rights (0-40)	31	31
TOTAL* (0-100)	**78**	**79**

* 0=most free, 100=least free

Population:	**31.2 million**
Internet Penetration 2015 (ITU):	**43 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- Voice over Internet Protocol services, including Skype, WhatsApp, and Viber, have been unavailable since July 2015 (see **Restrictions on Connectivity**).
- In April 2016, amendments to the criminal code increased penalties for poorly defined offences like threatening public order using mass media or telecommunications networks (see **Legal Environment**).
- Freelance online journalist and human rights activist Dmitry Tikhonov fled Uzbekistan a ter an intimidation campaign and threats of arrest (see **Intimidation and Violence**).

Introduction

Internet freedom declined in the coverage period, with Voice-over-Internet-Protocol (VoIP) services restricted for much of the year, though both the government and service providers denied responsibility.

Uzbekistan has one of the most tightly controlled online and media environments in the world, with restrictions on any content critical of the government, high levels of surveillance, and lengthy prison sentences for posting controversial content online. The websites of many international news outlets have been blocked for the past decade. In a move likely to further impede critical reporting online, authorities amended the criminal code in 2016 to strengthen penalties for vague crimes like threatening public order using mass media or telecommunications networks.

The sudden death of President Islam Karimov in September 2016 threw the country into uncertainty. Acting President Shavkat Mirziyoyev has pledged to continue Karimov's legacy, meaning internet freedom is unlikely to improve.

Obstacles to Access

Nearly half of the population had internet access in 2015, with growing mobile penetration playing a critical role in improving access. However, expensive service, low broadband speeds, and limits on data volume continue to curb internet use. The state controls the country's international internet gateways through the state-owned telecommunications operator Uztelecom. Since July 2015, Voice over IP (VoIP) services such as Skype, WhatsApp, and Viber have been inaccessible, though both the government and service providers denied blocking them. Competition among mobile cellular network operators looks set to decline with the withdrawal of one foreign provider, and the state assuming control of another in August 2016.

Availability and Ease of Access

According to the International Telecommunication Union (ITU), internet penetration increased to almost 43 percent in December 2015, compared to 36 percent in 2014, reaching about 12.7 million people.[1] The number of mobile internet users reached 11.2 million at the end of 2015,[2] nearly half of the 21.8 million mobile cellular phone subscriptions.[3] In February 2016, the Uzbek government set a target of increasing this number to 27 million by 2020.[4]

Fixed broadband was available to 1.5 million subscribers by December 2015.[5] Internet access is based primarily on ADSL technology, which the government estimates as being available to 67 percent of subscribers.[6] The remaining 32 percent use connections via fiber optic net orks (FTTx broad-

1 ITU ICT Statistics, "Time Series by Country (until 2015)," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
2 "On the state and prospects of the development of the ICT industry in Uzbekistan," *InfoCom*, September 29, 2015, http://infocom.uz/2015/09/29/o-sostoyanii-i-perspektivax-razvitiya-ikt-v-uzbekistane/.
3 ITU ICT Statistics, "Time Series by Country (until 2015)," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
4 Resolution of the Cabinet of Ministers RU, "On the Programme for the Development of Services for 2016 – 2020," No. 55, February 26, 2016, in *SZRU* (2016) No. 9 (717).
5 ITU ICT Statistics, "Time Series by Country (until 2015)," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
6 ITU ICT Statistics, "Time Series by Country (until 2015)," http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

band). Only 1 percent of subscribers use WiMAX broadband, initially introduced by the state-owned telecommunications operator Uztelecom in 2006.

Internet connection speeds remain relatively low. None of the ADSL/FTTB subscriptions from private ISPs enable internet download speeds faster than 8 Mbps. Subscribers experience poor connection quality, frequent disconnections and poor technical support. "Unlimited" ADSL/FTTB subscriptions, advertised by all ISPs, actually entail quotas on traffic. If the quota is e ceeded, the connection speed sharply decreases. Mobile providers continued to invest into 4G LTE broadband connectivity, with speeds of up to 70Mbps offered by provider UMS.[7] Internet access prices are still prohibitively expensive in comparison to the average household income in Uzbekistan.[8] Monthly subscriptions cost US$50 on average, offering free traffic up o 12 GB.[9]

Since September 2005, all public institutions such as educational and academic institutions, youth organizations, libraries, and museums, must connect to the wider internet exclusively via ZiyoNET,[10] a nationwide access and information network that enables the government to monitor all communications traffic. Since July 2013, the go ernment allowed the state-owned telecommunications operator Uztelecom to serve as the exclusive provider of access to ZiyoNet.[11] Fixed ZiyoNET broadband subscriptions start at US$6 per month for 700 MB of data.[12]

The use of mobile technology is limited in schools and universities.[13] In a May 21, 2012 resolution, the government completely banned the use of mobile phones in educational institutions except in "justified and u gent" cases.[14] The measure was justified as a means f preventing cheating, digital gaming, and the dissemination of materials that undermine morals and promote violence or "reactionary sectarian, pseudo-religious ideology."

In December 2015, the government announced it would allocate US$883 million to developing broadband infrastructure by 2019,[15] including the construction of over 6000 miles of fiber optic ne - works by 2020.[16] At the same time, the government said it would work to improve internet access, particularly in rural areas, where 49.4 percent of the population was based in December 2015.[17] The capital Tashkent has much higher rates of internet penetration and of fib e-to-the-building (FTTB)

7 "UMS launches LTE in Tashkent," *TeleGeography*, June 21, 2016, https://www.telegeography.com/products/commsupdate/articles/2016/06/21/ums-launches-lte-in-tashkent/.

8 As reported by ITU in 2012, internet access prices were prohibitively high in Uzbekistan and exceeded the monthly GNI per capita level at the rate of approximately 188 percent. See ITU, "Measuring the Information Society: 2012."

9 See subscription „Record-6," as of May 2016, at http://uzonline.uz/ru/services/internet/.

10 Resolution of the President RU "О создании общественной образовательной информационной сети Республики Узбекистан" [On the Establishment of the Public, Educational, and Information Network of the Republic of Uzbekistan], No. ПП-191, 28 September 2005, SZRU (No. 40), item. 305, at Art. 4.

11 Resolution of the Cabinet of Ministers RU "О мерах по дальнейшему развитию образовательной сети "ZiyoNET"" [On the Further Development of the Educational Network "ZiyoNET"], No. 198, July 10, 2013, *SZRU* (2013) No. 28 (580), item 362, at Art. 4.

12 Uztelecom, Uzonline internet tariffs per May 31 2016, at http://uzonline.uz/ru/services/internet.

13 "Is it allowed to use a mobile phone in college?" [in Russian] *Darakchi*, July 13, 2016, http://ru.darakchi.uz/article/867-mojno-li-polzovatsya-sotovim-v-kolledje.

14 Resolution of the Cabinet of Ministers RU, "О мерах по упорядочению пользования мобильными телефонами в образовательных учреждениях Республики Узбекистан" [On measures to streamline the use of mobile phones in educational institutions of the Republic of Uzbekistan], No. 139, May 21, 2012, *SZ RU* (2013 No. 21 (521), item. 229.

15 "Uzbekistan will allocate $883 million to increase access to the internet," *Sputnik*, December 1, 2015, http://ru.sputniknews-uz.com/society/20151201/1197905.html.

16 "Uzbekistan will allocate $883 million to increase access to the internet," *Sputnik*, December 1, 2015, http://ru.sputniknews-uz.com/society/20151201/1197905.html.

17 Resolution of the Cabinet of Ministers RU, „On the Adoption of the E-Commerce Concept in the Republic of Usbekistan for the period of 2016 to 2018," NO. 353 of December 4, 2015, *SZRU* (2015), NO. 49, item 612.

broadband connectivity than the country's 12 regions (*viloyati*) and the autonomous Republic of Karakalpakstan.[18] Uztelecom's FTTB broadband service reaches 3,287 buildings in Tashkent, and just four in Termez city in the geographically remote Surkhandariya region on the border to Afghanistan, home to 136,000 people.[19] ICT facilities also depend on a stable electricity supply to the telecommunications infrastructure, which has been less reliable in rural areas.[20]

Uztelecom and at least two private mobile operators offer public Wi-Fi hotspots in limited locations. In 2016, Uztelecom operated 67 hotpots across Samarkand, Bukharam, and four regions, including 14 in Tashkent.[21] In February 2016, the government set a goal of extending public Wi-Fi coverage to the remaining eight regions, and the Republic of Karakalpakstan. The private mobile operator Beeline launched its fi st public Wi-Fi network in August 2015 and currently operates 27 Wi-Fi hotspots in 6 cities.[22]

In February 2016 EVO, a private mobile broadband internet provider, launched free Wi-Fi services in public buses in Tashkent. However, the service was terminated a few days later, leading observers to question whether the authorities had intervened.[23]

Public access points such as internet cafes remain popular, particularly among young internet users. However, since December 2010, minors are officially p ohibited from visiting internet cafes unsupervised between 10:00 p.m. and 6:00 a.m.[24]

The state installs computers in every *mahallah* committee—traditional local community councils that the government has turned into an official sys em for public surveillance and control.[25] Civil servants' access to the internet and social media channels for personal use is largely restricted by technical tools as a result of information security concerns.[26]

Restrictions on Connectivity

The government exercises significant cont ol over the infrastructure and ordered internet shutdowns during the coverage period; Voice-over-Internet-Protocol (VoIP) services were also significantly di - rupted in the past year.

Internet access is routed via Uztelecom, a state-owned telecommunications and internet access provider, and a TAS-IX peering center and content delivery network. Uztelecom is an upstream ISP

18 Uztelecom, "Зона покрытия FTTB", (Coverage zone of FTTB) accessed July 2016, http://uzonline.uz/ru/services/fttb/.

19 Uztelecom, "Зона покрытия FTTB", (Coverage zone of FTTB) accessed July 2016, http://uzonline.uz/ru/services/fttb/.

20 International Telecommunication Union, "Sustainable supply of electricity to telecommunication facilities in rural and remote areas (Uzbekistan)," accessed February 10, 2014, http://bit.ly/1FV5uod.

21 Uztelecom, " "Uzbektelecom JSC continues development of Wi-Fi network project on the territory of historical and cultural heritage and tourist activity of Uzbekistan," September 26, 2015, http://www.uztelecom.uz/en/press/news/2015/1936/.

22 Beeline has Wi-Fi hotsports: 16 (Tashkent), 5 (Samarkand), 3 (Samarkand), 1 (Namangan), 1 (Fergana), and 2 (Djizak), https://www.beeline.uz/uz/Catalog/Services/Wi-Fi/p/wi-fi

23 "Free Wi-Fi in buses of Tashkent distributed and banned," [in Russian] *Digital.Report*, February 17, 2016, https://digital.report/besplatnyiy-wifi-v-av obusah-tashkenta-udivil-nablyudateley/.

24 "O poriadke predostavlenia dostupa k seti Internet v obschestvennikh punktakh pol'zovania" [On Adoption of the Terms of Provision of Access to the Internet Network in Public Points of Use], promulgated by Order of the Communications and Information Agency of Uzbekistan No. 216, July 23, 2004, *SZRU* (2004) No. 30, item 350, art. 17 (e).

25 See Resolution of the President RU No. ПП-1920.

26 «Чиновникам Узбекистана запретили интернет на рабочем месте» (Uzbek officials an internet in the workplace), *UzNews*, March 3, 2014, at http://www.uznews.net/ru/human-rights/25388-chinovnikam-uzbekistana-zapretili-internet-na-rabochem-meste.

and sells international internet traffic o domestic ISPs at a wholesale price. Uztelecom runs the International Centre for Packet Switching to aggregate international internet traffic at a single node within its infrastructure. Private ISPs are prohibited by law from bypassing Uztelecom's infrastructure to connect to the internet, and from installing and maintaining their own satellite stations in order to establish internet connectivity.

The TAS-IX peering center and content delivery network, established in February 2004, interconnects the networks of private ISPs to enable traffic con eyance and exchange at no mutual charge and without the need to establish international internet connections via Uztelecom.[27] Private ISPs provide no traffic limitations o websites hosted within the TAS-IX networks but fil er and block website to the same extent as Uztelecom.[28]

The authorities periodically impose temporary internet shutdowns, and even annually order mobile operators to shut down internet and text message services nationwide to avoid cheating during August university entrance exams.[29] Internet users in Tashkent reported connectivity was interrupted in January 2016, after Uztelecom warned of disruptions for maintenance purposes; observers speculated the disturbance was related to the installation of surveillance equipment (see Surveillance, Privacy, and Anonymity).[30]

Services offering Voice-over-Internet-Protocol (VoIP), including Skype, WhatsApp, and Viber, have been unavailable to users in Uzbekistan since at least July 2015, with some reports of disruptions from as early as October 2014; some users reported the apparent block was lifted briefly in Oc ober 2015. As of May 2016, the Skype website remained inaccessible from within Uzbekistan except via virtual private network (VPN). Experts linked the restrictions to the threat these free services pose to Uztelecom revenue from international calls.[31] Uztelecom and the Ministry for the Development of Information Technologies and Communications, which regulates ICTs, both denied responsibility for the block. Uztelecom said the inaccessibility was caused by "maintenance work on the network of its partners," from July 2015 until October 2015. In May 2016, in an official esponse to a user complaint posted on an e-government website, a director of Uztelecom's information security department said the company was "not responsible for the due or proper operability of third-party resources." The ministry said that that "servers of multimedia services like Skype, WhatsApp, Viber, and others are located in foreign states. National ISPs (operators and providers) in the Republic of Uzbekistan might be held responsible by the law for the functioning and accessibility of segments of the internet network, however, they cannot influence the quality f the aforesaid service."

ICT Market

There are numerous legal, regulatory, and economic obstacles to competitive business in the ICT sector.

27 TAS-IX, List of Members, http://tas-ix.uz/index.php?option=com_content&view=article&id=63:listofmembers.

28 TAX-IS participating ISP maintain a service to find out whether a ebsite is in the TAS-IX network. See, e.g., ISP TPS, http://www.tps.uz/tasix/.

29 "Отключение мобильного интернета скажется на работе терминалов," (Disconnection of mobile internet will affect terminals) *Gazeta*, July 31, 2016, https://www.gazeta.uz/ru/2016/07/31/uzcard.

30 "In Uzbekistan, complaints about the quality of internet connections," *Regnum*, January 16, 2016, https://regnum.ru/news/polit/2049248.html; "Uzbekistan: what to do with a problem called internet," *Eurasianet*, January 8, 2016, http://www.eurasianet.org/node/76741.

31 "Why doesn't Skype work?" *UzMetronom,* October 17, 2014, Uzmetronom.com, http://www.uzmetronom.com/2014/10/17/pochemu_so_skype_snjali_skalp.html.

As of May 2016, there were 854 companies classified as p oviding data or telecommunications services, including the internet, representing a decrease from 930 at the end of 2013.[32] This figu e includes internet cafes and does not indicate the number of private internet service providers (ISPs), though fewer than 40 connect with the TAS-IX peering center.

State control over the mobile telecommunications sector increased in 2016. Five mobile phone operators shared the market in Uzbekistan as of May 31, including Uzmobile, a brand of Uztelecom, and three privately owned operators: Perfectum Mobile (owned by the Uzbek company Rubicon Wireless Communication), Beeline (owned by the Amsterdam-based VimpelCom), and Ucell (under the part-Swedish government owned Telia Company AB, formerly TeliaSonera). Beeline and Ucell operate 2G, 3G, and 4G mobile networks and currently lead in terms of subscribers. A fi th subscriber, UMS (Universal Mobile Services), was controlled by Russian telecom giant Mobile TeleSystems OJSC (MTS) until August 2016, when it sold that share to the Uzbek government.[33] Telia has also announced plans to gradually exit the Eurasian region.[34] The foreign operators withdrew following a corruption investigation by U.S. prosecutors implicating MTS, Telia, and VimpelCom, in payments made to a relative of late President Karimov in order to secure business in Uzbekistan.[35]

State ownership already skews the market. On February 12, 2014, President Karimov signed a resolution that gave CDMA provider Uzmobile the legal status of a "national operator of mobile communications" with the aim of ensuring a "reliable and stable operation of mobile communications networks given the requirements of information security.[36] Until 2017, Uzmobile has been granted tax exemptions and licensing privileges in order to reach a target of 7,000 base stations and 8 million subscribers.[37] The Chinese government pledged US$500,000 in investments for Huawei Technologies to be an official supplier f telecommunications equipment to Uzmobile.[38]

Service providers are required to have a license to operate, and in 2005, the Cabinet of Ministers adopted Resolution No. 155, which stipulates that telecommunications providers must fi st register as a legal entity before being issued a license. Licensing is often encumbered by political interests.[39] As of March 2014, no licenses can be given to an internet cafe if the business premises are located in the basement of multistory buildings.[40] Compliance with other regulations for internet cafe owners mandating installation of surveillance equipment and cooperation with law enforcement are burdensome and expensive (see Surveillance, Privacy, and Anonymity).

32 Ministry of Development of IT and Communication, "Industry development indicators," 2009-2016, http://www.mitc.uz/ru/activities/indicators_industry_development/.

33 "МТС покидает рынок Узбекистана," (MTS is leaving Uzbek market), *Finanz*, August 5, 2016, http://www.finanz.ru/no osti/aktsii/mts-pokidaet-rynok-uzbekistana-1001342200.

34 "TeliaSonera to retreat from Central Asia," *Reuters,* September 17, 2015, http://www.reuters.com/article/teliasonera-eurasia-idUSL5N11N0BU20150917.

35 For details see U.S. District Court, Southern District of New York (Manhattan), "U.S. v. All Funds Held in Account Number CH1408760000050335300 at Lombard Odier Darier Hentsch & Cie Bank, Switzerland, on behalf of Takilant Ltd., and any property traceable thereto", case 1:16-cv-01257, 18 February 2016, at https://www.justice.gov/opa/file/826636/downl ad; Matthias Verbergt and David Gauthier-Villars, "Telia Asked to Pay $1.4 Billion to Settle Bribery Probe," *Wall Street Journal,* September 15, 2016, http://www.wsj.com/articles/telia-to-pay-1-4-billion-in-bribery-probe-1473921293.

36 Resolution of the President RU "О мерах по организации деятельсности национального оператора мобильной связи" [On the Measures Establishing the Activity of the National Operator of the Mobile Communications], No. ПП-2126, February 12, 2014, *SZRU* (2014) No. 7, item 73.

37 See Resolution of th Cabinet of Ministers RU No. 55, February 26, 2016.

38 «Китай выделит Узбекистану $550 млн. на развитие оператора «Узмобайл» — СМИ,» (China will give Uzbekistsan $500 million…) December 25, 2014, *Mobinfo.Uz*, http://bit.ly/1MgLzfV.

39 IREX, "Europe & Eurasia Media Sustainability Index 2013," http://www.irex.org/sites/default/files/u105/EE_MSI_2013_Uzbekistan.pdf.

40 Murat Sadykov, "Uzbekistan: Big Brother's Newest Eye—In Internet Cafes," *Eurasianet*, March 31, 2014, http://bit.ly/1L9lDmG.

Other factors impeding telecommunications company operations include an unstable regulatory environment, intricate customs procedures for the import of ICT equipment, and rules limiting currency conversion. Local authorities have also required international telecommunications companies to contribute to the cotton harvest, which watchdog groups say involves forced labor, as a condition of doing business.[41] Telia declined to comply in 2015.[42]

Regulatory Bodies

Regulation of the internet has never been independent. Since February 2015, the Ministry for the Development of Information Technologies and Communications (MININFOCOM) regulates telecommunications services related to the internet.

The Ministry combines the functions of a policy maker, regulator, and content provider, with no separation of regulatory and commercial functions. It is responsible for licensing ISPs and mobile phone operators; promotes technical standards for telecommunication technologies such as 4G; and provides e-governance services.

The Computerization and Information Technologies Developing Center (Uzinfocom) under the Ministry administers the ".uz" top-level domain. Twelve private ISPs were authorized to provide registry services in the ".uz" domain zone as of May 2016.[43] Rules for the assignment, registration, and use of the country's top-level domain create an obstacle to internet access.[44]

The Ministry is responsible for internet content regulation in order to prevent, among other things, the internet's "negative influence on the public consciousness f citizens, in particular of young people." To do so, the Ministry promotes development of the national segment of the internet (the *intranet*), with "modern national websites on different issues, including information resources to satisfy informational and intellectual needs of the population, particularly of the youth."[45] Uzinfocom is also the largest provider of web hosting services, including for the e-government project, government-backed *intranet*, national search engine, and social-networking sites.[46]

Limits on Content

The government of Uzbekistan monitors and controls online communications, and engages in pervasive and systematic blocking of independent news and any content that is critical of the regime, particularly related to foreign and domestic affairs or human rights abuses. The opaque system offers few details on how decisions are made or what websites are blocked at any given time.

41 Business-Human Rights, "Teliasonera/Telenor response," September 8, 2015, https://business-humanrights.org/sites/default/files/documents/_C_response_GM_Teliasonera_Telenor_rejoinder.pdf.

42 Telia AB, "Annual + Sustainability Report," 2015 https://www.teliacompany.com/globalassets/telia-company/documents/reports/2015/annual-report/teliasonera_annual-and-sustainability-report-2015-eng.pdf

43 Computerization and Information Technologies Developing Center, "Administrators," http://cctld.uz/reg/.

44 Law RU "On Telecommunications," at Arts. 8, 11.

45 See Resolution of the Cabinet of Ministers RU „Об утверждении Положения о Министерстве по развитию информационных технологий и коммуникаций Республики Узбекистан" [On the Establishment of the Ministry for the Development of Information Technologies and Communications of the Republic of Uzbekistan], No. 87, April 10, 2015, *SZRU* (2015), NO 15 (671), item. 178.

46 Uzinfocom Data Centre, „Услуги веб-хостинга," [Web Hostimg Services] http://dc.uz/rus/hosting/.

Blocking and Filtering

Significant blocking and fi ering limits access to online content related to political and social topics, particularly those related to human rights abuses in Uzbekistan. Websites permanently blocked in Uzbekistan do not appear on www. Поиск.uz - the official state-run search engine.

The websites of the international broadcasters Radio Free Europe/Radio Liberty, Deutsche Welle, and the Uzbek services of the BBC and Voice of America have been permanently inaccessible in Uzbekistan since 2005,[47] following a violent government crackdown on peaceful antigovernment protests in Andijan.[48] Websites of Uzbek human rights and opposition groups in exile are also blocked. Websites of international human rights organizations, such as Amnesty International, Freedom House, and Human Rights Watch, among others, are also blocked. In August 2015, the United Nations Human Rights Committee expressed concern that websites with content on "controversial and politically sensitive issues" are blocked in Uzbekistan.[49]

Stringent limits on content also appear on the ZiyoNET information network, which is the only mode of internet access for libraries, educational and other cultural institutions, and youth organizations (see Availability and Ease of Access). In July 2013, the government adopted a resolution calling for an official egistry of information resources to be made available on ZiyoNET.[50] As of June 2016, there were 50,100 "approved" educational resources, some of which are knock-offs of popular social media platforms such as Utube.uz, Fikr.uz (blogging platform), and uRadio.uz.[51]

Several government-linked entities monitor and control online communications, though the opaque system offers few details on how decisions are made or what websites are blocked at any given time. The Center for the Monitoring of the Mass Communications Sphere takes various measures to maintain compliance with national legislation that restricts free expression.[52] Among its key objectives are "to analyze the content of information disseminated online and ensure its consistency with existing laws and regulations."[53] The center has contributed to the takedown of independent websites (see Media, Diversity, and Content Manipulation).[54] The Expert Commission on Information and Mass Communications, a secretive body established in August 2011, oversees the monitoring center.[55] The commission is not independent and must submit quarterly reports to the Cabinet of Ministers.[56] Its

47 Committee to Protect Journalists, „Attacks on the Press 2010: Uzbekistan," February 15, 2011, http://cpj.org/x/40d0.

48 Alo Khodjayev, "The Internet Media in Uzbekistan," in OSCE Representative on Freedom of the Media (ed.), Pluralism in the Media and the Internet (OSCE Representative on Freedom of the Media, Vienna, 2006), 143-148, at 144.

49 See UN Docs. CCPR/C/UZB/CO/4, at para. 23.

50 Resolution of the Cabinet of Ministers RU "О мерах по дальнейшему развитию образовательной сети "ZiyoNET"" [On the Further Development of the Educational Network "ZiyoNET"], No. 198, July 10, 2013, *SZRU* (2013) No. 28 (580), item 362, at Art. 4.

51 «Библиотека» [Library], ZiyoNet.uz, accessed February 10, 2014, http://www.ziyonet.uz/ru/library/.

52 Zhanna Hördegen, "The Future of Internet Media in Uzbekistan: Transformation from State Censorship to Monitoring of Information Space since Independence," in *After the Czars and Commissars: Journalism in Authoritarian Post-Soviet Central Asia* ed. Eric Freedman and Richard Schafer, (East Lansing: Michigan State University Press, April 2011), 99-121.

53 Regulation No. 555, On the Measures of Improving the Organizational Structures in the Sphere of Mass Telecommunications, adopted by the Cabinet of Ministers of Uzbekistan on November 24, 2004. See OpenNet Initiative, "Country Profile: Uzbekistan" December 21, 2010, http://opennet.net/research/profiles/uzbekista .

54 A news website Informator.uz was shut down in 2007. See, "Pochemu zakrito nezavisimoe SMI Uzbekistana—Informator.Uz?" [Why the independent mass media of Uzbekistan, Informator.Uz, is closed?] *UZ Forum* (blog), September 20, 2007, www.uforum.uz/showthread.php?t=2565.

55 Resolution of the Cabinet of Ministers, О дополнительных мерах по совершенствованию системы мониторинга в сфере массовых коммуникаций,[On Supplementary Measures for the Improvement of the Monitoring System for the Sphere of Mass Communications] No. 228, August 5, 2011, *SZ RU* (2011) No. 32-33, item 336.

56 Ibid, Annex II, art. 31.

membership is not public,[57] although it is reportedly comprised exclusively of government employees. The commission is mandated to evaluate online publications for content with a "destructive and negative informational-psychological influence on the public consciousness of citizens;" content which fails to "maintain and ensure continuity of national and cultural traditions and heritage;" or aims to "destabilize the public and political situation," or commit other potential content violations.[58]

The commission also assesses publications referred to it by the monitoring center or other state bodies, including the courts and law enforcement, drawing on a designated pool of government-approved experts.[59] Commission members vote on whether or not a violation has been committed based on reports from those experts. State bodies act on the commission's decision, including courts and "other organizations," presumably private ISPs.[60] There are no procedures in place to notify those whose content is blocked, and no clear avenue for appeal.

It is not clear to what extent authorities filter text messages or other content transmitted via mobile phones. In March 2011, some news reports said mobile phone operators were required to notify the government of any attempts to circulate mass text messages with "suspicious content."[61]

Content Removal

Intermediaries can be held liable for third-party content hosted on their platforms and can be forced to remove such content. Under the 1999 Law on Telecommunications and several other government resolutions, the licenses of lower-tier ISPs may be withheld or denied if the company fails to take measures to prevent their computer networks from being used for exchanging information deemed to violate national laws, including ones that restrict political speech. Under Order No. 216 passed in 2004, ISPs and operators "cannot disseminate information that, *inter alia*, calls for the violent overthrow of the constitutional order of Uzbekistan, instigates war and violence, contains pornography, or degrades and defames human dignity."[62] Given these broad restrictions, many individuals and organizations prefer to host their websites outside the country.[63]

September 2014 amendments to the Law on Informatization brought bloggers and online news providers, including freelance citizen journalists, under state regulation subject to content removal requirements. By the law's broad definition, any person may qualify as a blogger by disseminating information "of socio-political, socio-economic and other character" to the public through a website.[64] The law requires bloggers to substantiate the credibility (*dostovernost'*) of "generally accessible information" prior to publishing or even reposting it, and obliges them to "immediately remove" information if it is not considered credible. The law entitles a special governmental body to limit access to websites that do not comply.

57 Ibid, Annex I, contains a list of the Commission's members that is not made public.

58 Resolution of the Cabinet of Ministers RU, No. 228, at art. 1 and Annex II, art. 5. See note 50 above.

59 Ibid, at art. 1 and Annex II, art. 14.

60 Ibid, at Annex II, art. 26 and 29.

61 Murat Sadykov, "Uzbekistan Tightens Control over Mobile Internet," *Eurasianet*, March 15, 2011, http://www.eurasianet.org/node/63076.

62 Regulation, О порядке предоставления доступа к сети Интернет в общественных пунктах пользования, [On Adoption of the Terms of Provision of Access to the Internet Network in Public Points of Use] promulgated by Order of the Communications and Information Agency of Uzbekistan No. 216, July 23, 2004, *SZRU* (2004) No. 30, item 350.

63 According to government figures, only about 30 percent of websites with ".uz" domain names were hosted on servers based in Uzbekistan as of December 2011. See Uzinfocom, "Только цифры," [Only Numbers] http://bit.ly/1jRuwui.

64 Law RU No. 3РУ-373, *SZRU* (2014) No. 36, item 452.

Media, Diversity, and Content Manipulation

The online media environment in Uzbekistan is severely restricted. Self-censorship is pervasive, given the government's tight controls over the media and harsh punishment of those who report on topics deemed "taboo," including criticism of the president, revelations about corruption, or health education.[65] As a result of the government's history of harassing traditional journalists, as well as their families, many online writers are cautious about what they post. The editorial direction of the online versions of state-run news outlets is often determined by both official and un fficial guidelines f om the government.

Under 2007 amendments to the 1997 law On Mass Media,"[66] any website engaged in the dissemination of mass information periodically (at least once every six months) is considered "mass media" and is subject to official p ess registration.[67] This procedure is generally known to be content-based and arbitrary, and inhibits editors and readers from exercising their freedom of expression and right to access information.[68] As of January 2015, 304 news-oriented websites, including online versions of traditional news media outlets, were registered as mass media in Uzbekistan.[69]

Independent news websites have been subject to arbitrary closure or retroactively unregistered.[70] Olam.uz, once Uzbekistan's second most-visited news site, remains closed since going offline for "technical reasons" in January 2013 after the authorities opened criminal proceedings against its editor-in-chief and the website owner, the Tashkent-based LLC Mobile Mass Media.[71] At the time of its closure, Olam.uz was reporting on state appropriation in the mobile telecommunications sector. In May 2015, a court ordered the closure of the news media website Noviyvek.uz, a weekly newspaper established in January 1992 and known for its balanced news reporting.

Facebook, YouTube, Twitter, and the Russian social networks Odnoklassniki (odnoklassniki.ru) and VKontakte (vk.ru) are available and widely used. In 2014, Facebook was the fourth most visited website in the country, followed by Odnoklassniки, VKontakte, and YouTube. Twitter became particularly popular in 2013, when President Karimov's daughter Gulnara Karimova used her account (@Gulnara-Karimova) to reveal secrets about her family and the corrupt practices of the Uzbek national security service.

As social-networking sites and blogging platforms have grown in popularity, the government attempts to influence the info mation circulated on them by creating and promoting Uzbek alterna-

65 "В Узбекистане закрывается лучший медицинский сайт" [The Best Medical Website is Going to be Shut Down in Uzbekistan], *Uznews,* March 25, 2010, http://www.uznews.net/news_single.php?lng=ru&cid=30&sub=&nid=13072; Catherine A. Fitzpatrick, "Uzbekistan: AIDS Activist Released, But Other Human Rights Defenders Harassed," September 6, 2011, http://www.eurasianet.org/node/64131.

66 Law RU, О средствах массовой информации, [On the Mass Media] No. 541-I, adopted December 26, 1997, as amended on January 15, 2007, *SZRU* (2007) No. 3, item 20, at art. 4.

67 Resolution of the Cabinet of Ministers RU, О дальнейшем совершенствовании порядка государственной регистрации средств массовой информации в Республике Узбекистан, [On the Further Development of the Procedure for State Registration of the Mass Media in the Republic of Uzbekistan] No. 214, October 11, 2006, in *SP RU* (2007) No. 14, item 141, at art. 8.

68 UN Human Rights Committee, "Mavlonov and Sa'di v. the Republic of Uzbekistan," Communication No. 1334/2004, Views adopted on April 29, 2009, UN Doc. CCPR/C/95/D/1334/2004, at par. 2.6, 2.11 and 8.3.

69 See Uzbek Agency for the Press and Information, "Состояние и динамика развития СМИ, издательств и полиграфических предприятий Узбекистана (01.01.2015г.)," last accessed on 27 May 2015, http://www.api.uz/ru/#ru/content/licence/statistics/.

70 See "Pochemu zakrito nezavisimoe SMI Uzbekistana—Informator.Uz?" ["Why the independent mass media of Uzbekistan, Informator.Uz, is closed?"], Uzinfocom blog U-FORUM (20 September 2007), http://www.uforum.uz/showthread.php?t=2565.

71 „Uzbek olam.uz news site shut down, staff accused of high treason," *Uznews,* January 29, 2013, http://bit.ly/19KDiic; „Is olam.uz trying to hide its criminal charges?" *Centre 1,* February 1, 2013, http://bit.ly/18eYayZ.

tives to popular global or regional brands. The most recent example is Davra launched in June 2016 by Uzinfocom (see Regulatory Bodies). Davra resembles Facebook, and enables users to post photos, videos, and comments,[72] but requires users to register their personal information and national IDs, facilitating monitoring by the authorities.[73] Observers believe law enforcement officials also manipulate online information through the website Zamamdosh. Though blocked in Uzbekistan, it frequently publishes allegations against journalists and human rights defenders who criticize the government (see Intimidation and Violence).

The role of blogs as opinion-shaping media on political and social issues in Uzbekistan is minimal. The blogosphere is largely of entertainment character.[74] A handful of blogs critical of the regime are run by Uzbek dissidents (for example, Jahonnoma.com, Turonzamin.org, and Fromuz.com) or are affiliated with independent online news websites and run by invited journalists.

Digital Activism

The stringent ideological policies of the government regarding the use of the internet and social media by Uzbek youth discourage digital activism as a significant form of political engagement. However, a handful of political activists and regime critics actively use the internet and social media as channels to reach supporters in and outside of Uzbekistan. Their efforts may raise awareness, but their actual impact on social mobilization is limited, largely due to the repressive environment for freedom of speech and assembly. Political Twitter and Facebook accounts are generally administered by Uzbek dissidents living abroad, rather than activists on the ground. Nevertheless, the #WithUzbeks hashtag gained traction on social media in 2015 to share opposition to the government, which had promoted a #WithKarimov hashtag prior to elections.[75]

In February 2015, the banned opposition group Birdamlik and human rights defender Mutabar Tadjibaeva protested against the unconstitutional presidential elections of March 29, 2015, by staging their own virtual alternative election. The organizers launched a virtual election committee website where people could cast a vote for eleven presidential candidates (excluding President Karimov).[76] Hackers defaced the website prior to the election.[77]

Violations of User Rights

State measures to silence dissent include persecution and criminal prosecution of regime critics and independent journalists, often on fabricated charges. The government has broad powers to punish ex-

72 Eugeniy Sklyarevskiy, "We will see us at Davra.uz!" *InfoCom,* May 17, 2016, in Russian, http://infocom.uz/2016/05/17/vstrechaemsya-v-socseti-davra-uz/.

73 Eugeniy Sklyarevskiy, "We will see us at Davra.uz!" *InfoCom,* May 17, 2016, in Russian, http://infocom.uz/2016/05/17/vstrechaemsya-v-socseti-davra-uz/.

74 Sarah Kendzior, „Digital Freedom of Expression in Uzbekistan: An Example of Social Control and Censorship in the 21st Century," New America Foundation, July 18, 2012, http://newamerica.net/publications/policy/digital_freedom_of_expression_in_uzbekistan.

75 See Freedom House, Nations in Transition 2016: Uzbekistan, at 7-8, https://freedomhouse.org/report/nations-transit/2016/uzbekistan.

76 "Virtual Election Seeks To Give Uzbeks Real Choice," *Radio Free Europe Radio Liberty,* February 10, 2015, http://bit.ly/1P1fWx3.

77 „Узбекистан: Виртуальная избирательная комиссия прекратила работу в связи с хакерской атакой на веб-сайт," (Uzbekistan: Virtual election commission ceased functioning after hackers attacked webstie) *Fergana,* March 24, 2015, http://bit.ly/1DTT3Xh.

pression online, and amended the criminal code in the coverage period to increase penalties for threatening security and order through telecommunications networks or mass media. The security services systematically eavesdrop on citizens' communications over email, mobile phone and Skype, in online forums, and social networks.

Legal Environment

Uzbekistan's constitution protects the rights to freedom of expression and of the mass media, and prohibits censorship. Article 29 of Uzbekistan's constitution guarantees the right to gather and disseminate information. However, the implementation of these protections is minimal under the current authoritarian regime with its weak attachment to democratic principles. National courts have generally failed to protect individuals, including professional journalists, against government retaliation for exercising their free speech rights. Rampant corruption, particularly within law enforcement bodies, as well as weak legislative and judicial bodies, continue to have a deleterious impact on freedom of speech.

The Uzbek criminal code contains several provisions that have been used extensively to prosecute reporters and internet users for threatening constitutional order (Article 159); the prohibition of propaganda for national, racial, ethnical and religious hatred (Article 156); the production and dissemination of materials containing a threat to public security and order with foreign financial help (Article 244); slander (Article 139), insult (Article 140), and insult of the president (Article 158). Both slander and insult are punishable with fines ranging f om 50 to 100 times the minimum monthly wage, correctional labor of two to three years, arrest of up to six months, or detention for up to six years.[78] Further restrictions typically placed on journalists and internet users are based on vague information security rules.[79]

On April 25 2016, amendments to Article 244(1) of the criminal code increased the penalty for the "manufacture, storage, distribution or display of materials containing a threat to public security and public order" committed using mass media or telecommunication networks from 5 to 8 years imprisonment.[80] The vaguely formulated offence prohibits "any form of dissemination of information and materials containing ideas of religious extremism, separatism and fundamentalism, calls for pogroms or violent eviction, or aimed at spreading panic among the population, as well as the use of religion to violate civil concord, dissemination of defamatory fabrications, and committing other acts against the established rules of behaviour in society and public safety, as well as dissemination or demonstration of paraphernalia or symbols of religious-extremist, terrorist organizations." Observers, including the OSCE, regarded this as a further move to suppress freedom of expression online.[81]

Prosecutions and Detentions for Online Activities

The regime's hostility towards its critics, including independent journalists, human rights activists, and critically-minded internet users, is notorious in Uzbekistan.[82] As of May 2015, two Uzbek online

78 Criminal Code of the Republic of Uzbekistan, art. 139 and 140, http://bit.ly/1aA516n.

79 Kozhamberdiyeva, "Freedom of Expression on the Internet: A Case Study of Uzbekistan."

80 Mushfig Bayram, Forum 18, "Uzbekistan: Ha shened Criminal And Administrative Code punishments," June 15, 2016, http://www.forum18.org/archive.php?article_id=2189.

81 OSCE Representative on Freedom of the Media, "Recent legislative amendments in Uzbekistan worrying, OSCE Representative says," April 29, 2016, http://www.osce.org/fom/237641.

82 Human Rights Watch,"*The very end*," September 26, 2014, http://bit.ly/1IXpa50.

journalists remained in jail on criminal charges international observers say were fabricated in retaliation for their reporting.[83] Solidzhon Abdurakhmanov, a 63-year-old journalist and reporter for *Uznews,* an independent news website forced to shut down in December 2014, continues to serve a 10-year sentence imposed in October 2008 for allegedly selling drugs. Prior to his arrest, he had reported on human rights and economic and social issues, including corruption in the Nukus traffic police ffice [84] Dilmurod Saiid, a freelance journalist and human rights activist, is serving a 12.5 year sentence imposed in July 2009 on extortion charges. Before his detention, he had reported on government corruption in Uzbekistan's agricultural sector for local media and independent news websites.[85]

Both independent and licensed journalists have faced selective and arbitrary prosecution for their online publications in the past. They include Abdumalik Boboyev, a reporter for Voice of America's Uzbek Service, Vladimir Berezovsky, the editor of *Vesti*, Viktor Krymzalov, a reporter for *Centrasia* and *Fergananews*, and Elena Bondar, a reporter for *Uznews* and *Fergananews*, and Said Abdurakhimov (freelance reporter for Fergananews.com). Some of these journalists were convicted under criminal law and had to pay exorbitant fines as a punishment. The cases ha e shown that recommendations by the internet state censorship authority, the monitoring center, which determines which online news articles violate national legislation, are being used to legitimate prosecution and conviction of online reporters.

Surveillance, Privacy, and Anonymity

The space for anonymous online communication in Uzbekistan is steadily shrinking, and government surveillance of ICTs is extensive. Although Article 27 of the constitution guarantees the privacy of "written communications and telephone conversations," there is no data protection legislation in Uzbekistan. Article 27 further guarantees respect for human rights and the rule of law, though these are frequently violated in surveillance operations.

Since 2006, the national security service (SNB) conducts electronic surveillance of the national telecommunications network by employing the "system for operational investigative measures" (SORM), including for the purposes of preventing terrorism and extremism.[86] ISPs and mobile phone companies must install SORM and other surveillance equipment on their networks in order to obtain a license.[87] Telecommunications providers are prohibited by law from disclosing details on surveillance methods and face possible financial sanctions or license evocation if they fail to design their networks to accommodate electronic interception.[88]

The Israeli branch of the U.S. Verint technology company, and the Israel-based NICE systems, also

83 Human Rights Watch, "Submission to the UN Human Rights Committee on Concerns and Recommendations on Uzbekistan," August 13, 2014, http://bit.ly/1BgbHFw.

84 Committee to Protect Journalists, "Government increases pressure on Uzbek journalists," letter, February 17, 2010, http://cpj.org/x/37de.

85 Committee to Protect Journalists, "Uzbek appeals court should overturn harsh sentence," September 3, 2009, http://cpj.org/x/34ea

86 Resolution of the President RU, О мерах по повышению эффективности организации оперативно-розыскных мероприятий на сетях телекоммуникаций Республики Узбекистан, [On Measures for Increasing the Effectiveness of Operational and Investigative Actions on the Telecommunications Networks of the Republic of Uzbekistan] No. ПП-513, November 21, 2006, at Preamble and art. 2-3.

87 Ibid, art. 5.8. Infra., note 110. Also, tax and custom exemptions apply for import of the SORM equipment by domestic ISPs, see Tax Code of RU, art. 208, 211, 230 part 2, and 269.

88 See Law RU, "On Telecommunications".

supply the security services with monitoring centers allowing them direct access to citizens' telephone calls and internet activity, according to UK-based Privacy International. Privacy International reported that Verint Israel has also carried out tests to gain access to SSL-encrypted communications, such as those now offered by default by Gmail, Facebook, and other service providers, by replacing security certifica es with fake ones using technology supplied by the U.S.-based company Netronome.[89] In July 2015, documents leaked from the Milan-based surveillance software company "Hacking Team" revealed that NICE systems was supplying Hacking Team's Remote Control System spyware to Uzbekistan.[90] RCS offers the ability to intercept user communications, remotely activate a device's microphone and camera, and access all of the phone's content including contacts and messages without the user's knowledge.

There is no independent oversight to guard against abusive surveillance, leaving the SNB wide discretion in its activities.[91] If surveillance is part of a civil or criminal investigation, content intercepted on telecommunications networks is admissible as court evidence.[92] Opposition activist Kudratbek Rasulov was sentenced to 8 years in prison on charges of extremism in 2013, based on intercepted digital communications with an exiled opposition group.[93] The law requires a prosecutor's warrant for the interception of telecommunication traffic by law enfo cement bodies; however, in urgent cases, the authorities may initiate surveillance and subsequently inform the prosecutor's office wit - in 24 hours.[94] In April 2016, the president signed a new law, On Parliamentary Control, which local reports characterized as part of a reform effort to reinforce parliament's role in upholding the rule of law. However, the law diminshed parliamentary oversight of surveillance practices undertaken by law enforcement agencies.[95]

There is limited scope for anonymous digital communication. Proxy servers and anonymizers are important tools for protecting privacy and accessing blocked content, although they require computer skills beyond the capacity of many ordinary users. There are no explicit limitations on encryption, though in practice the government strictly regulates the use of such technologies.[96] In September 2012, Uztelecom started blocking of websites offering proxy servers, including websites listing free proxies that operate without a web interface.

There are few options for posting anonymous comments online, as individuals are increasingly en-

89 Privacy International, „Private Interests: Monitoring Central Asia", Special Report, November 2014, at pp. 38-43, https://www.privacyinternational.org/sites/default/files/Pri_ate%20Interests%20with%20annex_0.pdf.

90 Edin Omanovic, "Eight things we know so far from the Hacking Team hack," Privacy International, July 9, 2015, https://www.privacyinternational.org/node/619.

91 Resolution of the President RU, О мерах по повышению эффективности организации оперативно-розыскных мероприятий на сетях телекоммуникаций Республики Узбекистан, [On Measures for Increasing the Effectiveness of Operational and Investigative Actions on the Telecommunications Networks of the Republic of Uzbekistan] No. ПП-513, November 21, 2006, at Preamble and art. 2-3; See, Criminal Procedural Code of RU, *Vedomosti Oliy Mazhlisa RU* (1995) No. 12, item 12, at art. 339 part 2, "Tasks of Investigation," and art. 382, "Competences of the Prosecutor." Resolution of the President RU No. ПП-513, note 87 above, art. 4.

92 Law RU, Об оперативно-розыскной деятельности, [On Operational and Investigative Activity] No. ЗРУ – 344, December 26, 2012, SZ RU (2012) No. 52 (552), item 585, art. 16, 19.

93 "Uzbekistan: Namangan Resident Faces 8 Years in Jail for Skype Call with Political Exiles," Fergana News, December 23, 2015, http://enews.fergananews.com/news.php?id=2786.

94 Resolution of the Cabinet of Ministers, "On the National Security Service of the Republic of Uzbekistan, " November 2, 1991, No. 278, at Part IV (3).

95 Law RU „О парламентском контроле" [On Parliamentary Control] No. ЗРУ – 403, April 12, 2016, *SZRU* (2016) No. 15, item 141, at Art. 4.

96 Resolution of the President RU, О мерах по организации криптографической защиты информации в Республике Узбекистан, [On Organizational Measures for Cryptographic Protection of Information in the Republic of Uzbekistan] No. ПП-614, April 3, 2007, *SZ RU* (2007) No 14, item 140, at art. 1.

couraged to register with their real names to participate in discussions forums such as Uforum,[97] which is administered by the state-run Uzinfocom.[98] Individuals must also provide passport information to buy a SIM card.[99]

ISPs and mobile operators are required to store user data for three months. Since July 2004, operators of internet cafes and other public internet access points are required to monitor their users and cooperate with state bodies. Under regulatory amendments in March 2014, operators of internet cafes and public access points must install surveillance cameras on their premises to "ensure [the] safety of visitors." Additionally, they are required to retain a "registry of internet web-resources (log-files)" used by cus omers for three months.[100]

Intimidation and Violence

Law enforcement agencies, including the SNB are known to systematically employ various intimidation tactics to restrict freedom of expression online. In the past, SNB office s were reported confi - cating electronic media devices at the airport, checking browsing histories on travelers' laptops, and interrogating individuals with a record of visiting websites critical of the government.[101] Law enforcement officials also invi e journalists and human rights activists and ordinary citizens to "prophylactic talks" which often include warnings and threats.[102]

Dmitry Tikhonov, a human rights activist and freelance journalist for Uznews.net, Fergana News Agency and AsiaTerra, fled the count y following a campaign of intimidation in the coverage period. He had published critical coverage of the demolition of a World War II memorial in Angren city in March 2015,[103] and regularly monitors labor rights abuses during the fall cotton harvests. Other media outlets denounced him for inciting national hatred,[104] calling him a "collector of slander and rumors about Uzbekistan" and a Western spy.[105] On September 20, he was detained for fi e hours, and reported that a police officer had assaul ed him in custody.[106] His private email account was sub-

97 "Правила форума," [Terms of Use] *UZ Forum* (blog), http://uforum.uz/misc.php?do=cfrules.

98 U.S. Department of State, "Uzbekistan," *Counter Reports on Human Righst Practices for 2011*, http://1.usa.gov/1L9qfsZ.

99 MTC Uzbekistan, "How to subscribe," http://www.mts.uz/en/join/.

100 See Resolution of the SCCITT RU, "О внесении изменений и дополнений в Положение о порядке предоставления доступа к сети Интернет в общественных пунктах пользования [On making amendments and additions to the Regulations on the procedure for providing access to the Internet in the public areas of use]," March 19, 2014, No. 79-мх, SZRU (2014) NO. 13, item 150.

101 "Farg'ona aeroportida yo'lovchilar noutbuki tekshirilmoqda" [At Ferghana Airport, Laptop Computers of Passengers Are Being Checked], Ozodlik.org, June 2, 2011, http://www.ozodlik.org/content/fargona_aeroportida_yolovchilar_noutbuki_tekshirilmoqda/24212860.html.

102 "Около 150 тысяч человек взяты на учет в Узбекистане", (Approximately 150,00 people were taken for registration in Uzbekistan) March 25, 2016, *Radio Ozodlik*, http://rus.ozodlik.org/a/27634490.html.

103 "Узбекистан: В Ташкентской области снесли обелиск воинам, погибшим в Великой Отечественной войне," (Uzbekistan: World War II memorial taken down In Tashkent province) March 20, 2015, http://www.fergananews.com/articles/8453.

104 "Узбекистан: После сноса памятника в Ангрене журналиста преследуют за «национализм»," (Uzbeksitan: Following the demolition of a memorial in Angren, journalist prosecuted for nationalism) April 6, 2015, http://www.fergananews.com/articles/8479.

105 "Кому выгодно искать «пятую колонну» среди узбекских правозащитников?", (Who benefits f om searching for the "fi th column" among Uzbek human rights defenders?" July 7, 2015, Fergana News Agency, http://www.fergananews.com/articles/8612.

106 "Узбекистан: Обвинили в шпионаже и запретили «связываться с Еленой Урлаевой»," (Uzbekistan: Convicted of spying and banned from contanting Elena Urlaeva," *Fergana,* September 2015, http://www.fergananews.com/article.php?id=8695.

sequently hacked, and stolen personal and professional data exposed online.[107] On October 20, his office and house bu ned down, destroying records of his investigations into human rights abuses.[108] In December 17, a criminal court found him guilty of petty hooliganism and fined for app oximately US$234.[109] On December 20, the website Zamandosh, which observers believe is covertly operated by officials, accused him f terrorism.[110] Tikhonov's lawyer also reported receiving anonymous threats.[111] Uzbek authorities have repeatedly denied Tikhonov an exit visa to leave the country, but he fled Uzbekistan in Februa y 2016 and sought political asylum overseas.

Technical Attacks

Distributed denial-of-service (DDoS) attacks on independent news media websites reporting on Uzbekistan, including the websites Centrasia.ru, Fegananews.com, UzMentronom.com, and Ozodlik.org (the Uzbek service of Radio Free Europe/Radio Liberty), have been frequent in the past. Human rights activist Dmitry Tikhonov reported that his personal email account had been subject to targeted hacking in the coverage period (see Intimidation and Violence).

The state-run Information Security Centre, established in September 2013, ensures the security of "the national segment of the internet" and state information networks, including the e-governance infrastructure.[112] The Centre took over most of the functions of the Uzbekistan Computer Emergency Readiness Team (UZ-CERT), established in 2005.[113] The Centre collects and analyzes information on computer incidents, including DDoS attacks, and alerts internet users to security threats. Moreover, the Centre interacts with domestic ISPs, mobile phone operators, and state bodies—including law enforcement agencies—on the prevention and investigation of "unsanctioned or destructive actions in information space."[114]

107 "Dimitrii Tikhonov: ideological saboteur or how they fabricated my case," *AsiaTerra,* February 29, 2016, http://www.asiaterra.info/obshchestvo/dmitrij-tikhonov-ideologicheskij-diversant-ili-kak-na-menya-fabrikovali-dela. See also "В Узбекистане разоблачили журналиста-мошенника, обкрадывающего международную организацию," ("Jounalist robs international organization") October 23, 2015, *Uz24*, http://uz24.uz/society/v-uzbekistane-razoblachili-zhurnalista-moshennika-obkradivayushego-mezhdunarodnuyu-organizaciyu.

108 Frontline Defenders,"Case History: Dimitrii Tikhonov," 2015, https://www.frontlinedefenders.org/pt/node/1062.

109 "Узбекистан: В Ангрене снова задержан правозащитник и журналист Дмитрий Тихонов," ("Uzbekistan: Rights defender and journalist Dimitrii Tikhonov once again arrested in Angren") *Fergana News Agency*, December 17, 2016, http://www.fergananews.com/news/24273.

110 "Dimitrii Tikhonov: ideological saboteur or how they fabricated my case," *AsiaTerra,* February 29, 2016, http://www.asiaterra.info/obshchestvo/dmitrij-tikhonov-ideologicheskij-diversant-ili-kak-na-menya-fabrikovali-dela.

111 „Правозащитник Тихонов покинул Узбекистан из-за публикации клеветнических материалов," ("Rights defender TIkhonov quits Uzbekistan after publication of slanderous material") *Radio Ozodlik,* February 13, 2016, http://rus.ozodlik.org/a/27550056.html.

112 Resolution of the Cabinet of Ministers of RU "О мерах по организации деятельности Центра развития системы Электорнное правительство и Ценра обеспечения информационной безопасности при Государственном комитете связи, информатизации и коммуникационных технологий Республики Узбекистан" [On Measures Establishing the Development Centre on "E-governance" System and Cybersecurity Centre at the State Committee on the CITT], No. ПП-2058, September 16, 2013, *SZRU* (2013) No. 38, item 492, at Art. 3.

113 See Resolution of the President RU No. ПП-2058, note 39 above (check cross-reference), at Annex 3, Art. 1

114 See Criminal Code Article 278-1 "Violation of the Rules of Informatization"; Article 278-2 "Illegal (Unsanctioned) Access to Computer Information"; Article 278-3 "Production and Dissemination of Special Tools for Illegal (Unsanctioned) Access to Computer Information"; Article 278-4 "Modification f Computer Information"; and Article 278-5 "Computer Sabotage."

Freedom House

Venezuela

	2015	2016
Internet Freedom Status	Partly Free	Partly Free
Obstacles to Access (0-25)	17	18
Limits on Content (0-35)	18	17
Violations of User Rights (0-40)	22	25
TOTAL* (0-100)	**57**	**60**

* 0=most free, 100=least free

Population:	**31.1 million**
Internet Penetration 2015 (ITU):	**62 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- Telecommunications services continued to deteriorate with the economic crisis and foreign currency controls. While according to official fig es internet penetration increased, some fi ms have been forced to scale back certain services and the country's average internet speed still lagged behind (see **Obstacles to Access**).
- Independent media and citizens actively used digital platforms to cover and monitor the electoral process in December 2015, which saw the opposition party gaining a majority of seats in the National Assembly (see **Limits on Content**).
- In September 2015, opposition leader Leopoldo López was sentenced to nearly 14 years in prison after prosecutors claimed he incited violence through "subliminal messages" during anti-government protests. As evidence in his trial, prosecutors analyzed hundreds of tweets and a YouTube video (see **Prosecutions and Detentions**).
- Security forces continued to arbitrarily arrest online reporters, confisca e cellphones, or oblige users to delete images while covering protests and queues to buy food. Physical attacks by pro-government groups also targeted ICT users (see **Prosecutions and Detentions** and **Violence and Intimidation**).

Introduction

Venezuela's internet freedom climate continued to decline in the midst of deepening political and economic turmoil.

Venezuela's deteriorating economic situation has entailed less overt – but more effective – limitations on internet freedom. A combination of factors, including strict foreign currency exchange controls, high inflation, and price cont ols have hindered the country's telecommunication sector and the quality of internet access. In April 2016, the regulatory body announced that some operators had been forced to suspend some services.[1] Venezuela's average broadband speed was the lowest in Latin America, according to the Economic Commission for Latin America and the Caribbean.[2]

Freedom of expression and information has progressively declined under the governments of Hugo Chávez and Nicolás Maduro. However, the widespread use of online media and social networks during parliamentary elections on December 6, 2015 demonstrated the growing importance and vigor of digital platforms. By forging strategic alliances with NGOs, new digital media have opened up space for discussion in a communication landscape largely dominated by the government. Parliamentary elections marked a shift in power in the legislative branch. Winning a super majority in the National Assembly, the opposition alliance announced discussions on reforming the Law of Telecommunications and the Law on Social Responsibility on Radio, Television, and Digital Media (Resorte-ME), which grants the regulatory body the power to rule over the blocking or deletion of content and to sanction service providers.[3] However, recent legislative efforts have had contend with the Supreme Court's power to rule against new legislation pushed forward by the opposition.[4]

At the same time, the government has sought to expand its influence by e erting control over the online sphere: blocking websites, encouraging self-censorship and content removal through third-party liability, and implementing sweeping laws that prohibit any content that threatens public order or promotes anxiety in the public. During the coverage period, three Twitter users arrested in 2014 remained in detention, while six users were subsequently released in 2015, at least on probation. Despite these releases, online reporters continued to face arbitrary arrests and confiscation f equipment while covering political events, protests, or queues to buy supplies. One of the most fl - grant events was the trial and conviction of opposition leader Leopoldo López, who was sentenced to almost 14 years in prison after a lawsuit supported by evidence based on the analysis of hundreds of tweets and a video on YouTube. Physical attacks against journalists and ICT users by pro-government groups were also reported.

Obstacles to Access

Internet subscriptions decreased by at least one percent, and the average broadband speed did not surpass 2 Mbps: out of all connections, less than 5 percent are faster than 4 Mbps. According to official figures, internet penetration remained above 60 percent, although the total number of subscribers

1 CONATEL, "CONATEL informa al país," [CONATEL informs the country], April 5, 2016, http://bit.ly/1YeUXYR.

2 ECLAC, "Estado de la banda ancha en América Latina y el Caribe 2015" [State of broadband in Latin America and the Caribbean], July 2015, http://bit.ly/1Nvh8H3.

3 "Comisión de Medios reformará la Ley de Telecomunicaciones y la Ley Resorte," [Media Commission will reform Telecommunications and Resorte Laws], *El Universal*, February 3, 2016, http://bit.ly/2dUZiU5.

4 Anatoly Kurmanaev, "Venezuela Top Court Annuls Amnesty Law," *The Wall Street Journal,* April 11, 2016, http://on.wsj.com/1Mqz9c7.

has dropped, and there is a significant gap between rural and urban areas. Foreign currency controls adversely impacted the telecommunication industry, while electricity shortages and rationing impeded access for users. The state dominates the ICT market through its ownership of CANTV, which has a market share of 70 percent.

Availability and Ease of Access

Venezuela's economic crisis, marked by foreign currency controls, falling oil prices and high inflation, has hindered the country's telecommunication infrastructure and the quality of internet access.[5] In August 2015, the Chamber of Business Telecommunications Services (CASETEL) warned that a lack of investment could impact service provision.[6] According to CASETEL'S President, Ricardo Martínez, by the end of 2015, service providers accumulated debt to suppliers that exceeded USD $1 billion. Some companies have been unable to convert profits in o foreign currency for over a year.[7]

According to the National Telecommunication Union (ITU), internet penetration reached 62 percent in 2015, up from 57 percent in 2015,[8] while some private surveys pointed to higher and also lower figu es.[9] According to CONATEL however, the total number of subscribers dropped from 3.68 million at the end of 2014 to 3.65 at the end of 2015.[10] Of these subscriptions, 93 percent were broadband (approximately 75 percent fi ed and 25 percent mobile).

Despite growing demand, mobile subscriptions regressed in the past year amidst the country's economic crisis.[11] Mobile phone penetration reached close to 100 percent in 2015, though the number of subscriptions actually decreased from over 30.5 million subscribers in 2014 to 29 million in 2015.[12] Similarly, mobile internet subscriptions fell from more than one million in 2014 to close to 815,000 in 2015.[13]

5 "Afi man que falta de divisas deteriora servicios de telecomunicaciones en Venezuela," [They affi m that lack of currency deteriorates telecommunications services in Venezuela], *Finanzas Digital*, September 17, 2015, http://bit.ly/2cNUomY.

6 The National Commission of Telecommunications estimated a 60 percent growth in revenues in the sector, but with inflation above 100 percent, this would result in a decline in real income between 2014 and 2015. According to CASETEL, price adjustments have been far below inflation in recent years, which hampers investment in this capital intensive industry. See: CASETEL, Press release, August 2015, http://bit.ly/2dpQ00d.

7 Roberto Deniz, "La deuda del gobierno con el sector telecomunicaciones ya llegó a más de mil millones de dólares" [Government debt to telecommunications sector now exceeds one billion dollars], *Konzapata,* October 28, 2015, http://bit.ly/1Wi4MbU.

8 International Telecommunication Union, "Percentage of Individuals using the Internet, 2000-2015," accessed October 3, 2016, http://bit.ly/1cblxxY. Venezuela's National Telecommunications Commission (CONATEL) measured internet penetration at 62.5 percent at the end of 2015, with more than 16.7 million users. In the third quarter of 2014, Conatel changed the methodology for calculating the number of users to include anyone with a cell phone with mobile data access. See: CONATEL, "Cifras del sector: Telecomunicaciones, 1998-2015" [Statistics: Telecommunications], accessed October 3, 2016, http://bit.ly/2dYLHb4 .

9 Other private studies, including one mentioned by the digital communication strategist Carmen Beatriz Fernandez, reported 75 percent internet penetration, with 18 percent of users who only connect via cell phone (Personal communication via email). Tendencias Digitales, on the contrary, estimated penetration at 53 percent. See: "Foro Tendencias Digitales 2015: Venezuela tiene el ancho de banda más bajo de los países de Latinoamérica" [Digital Trends 2015 Forum: Venezuela has the lowest broadband in Latin American countries], *Computer World*, September 29, 2015, http://bit.ly/1TWmw9n.

10 CONATEL, "Cifras del sector: Telecomunicaciones, 1998-2015" [Statistics: Telecommunications], accessed October 3, 2016, http://bit.ly/2dYLHb4.

11 Arnaldo Espinoza, "Operadoras prevén colapso de redes de telefonía celular este año," [Operators predict collapse of mobile telephone networks this year], *El Estímulo*, August 24, 2015, http://bit.ly/2dEHJ7g; See also: "World Hangs Up on Venezuela as Phone Companies Can't Pay," *Bloomberg,* August 2, 2016, http://bloom.bg/2aFInBU.

12 CONATEL, Statistics 2015.

13 CONATEL, Statistics 2015.

Mobile access further contracted in August 2015, when the telecom Movistar Venezuela, a subsidiary of the Spanish company Telefónica and second largest mobile operator in the country, suspended new activations of its mobile internet service.[14] Unable to meet financial obligations ag eed with suppliers in U.S. dollars, Movistar announced that it was eliminating long distance and roaming services in April 2016; Digitel did the same.[15] Users of state-owned Movilnet also reported cutbacks in certain services such as international roaming. CONATEL officially announced in April 2016 that di - ficulties arising f om the country's economic situation had forced some operators to suspend some services.[16]

Facing deteriorating infrastructure and outdated equipment, the quality of internet connections for the majority of the population remained very poor. The landing station for submarine cables in Camurí Chico, which handles 89 percent of international communications in the country, did not undergo specialized maintenance in 2015.[17] Due to the lack of maintenance and improvements of networks, users have reported speeds amounting to a fraction of the advertised speeds of 5 or 10 MB.[18] According to Akamai, Venezuela's average connection speed barely reached 1.9 Mbps in the fi st quarter of 2016.[19] Out of all the connections, only 4.3 percent were faster than 4 Mbps and only 0.3 percent exceeded 10 Mbps. Venezuela's peak connection speed (12.1 Mbps) was the worst out of 15 countries in the region assessed in Akamai's report. Compounding poor access speeds, electricity rationing extended to the capital in early 2016, which up until 2015 only occurred in rural areas.[20]

While accurate calculations are almost impossible to make in an economy with exchange controls and very high inflation, sma tphones are prohibitively expensive for the majority of the population and are increasingly scarce.[21] Although operators are forced to sell at controlled prices based on a preferential exchange rate, shortages prevail and products end up on the market at a price calculated at the free dollar rate, which was more than 1,000 bolivars per dollar in January 2016.[22]

On the other hand, telecommunications services have lost relative value in the basket of consumer

14 Movistar suspende nuevas activaciones de Internet Móvil" [Movistar suspends new activations of Mobile Internet], *Entorno Inteligente,* August 16, 2015, http://bit.ly/2dCGPaF.

15 "Movistar suspende servicio de larga distancia," [Movistar suspends long-distance service], *El Universal*, April 8, 2016, http://bit.ly/2dzbyJs; See also: "Telefonica subsidiary halts international calls from Venezuela," *Reuters,* April 9, 2016, http://reut. rs/2dqq7NK; "Digitel suspende servicios de roaming y larga distancia a partir del 9 de abril," [Digitel suspends roaming and long distance services from April 9], *El Estímulo*, April 7, 2016, http://bit.ly/2cNHOsM.

16 "Venezuela se queda sin llamadas por celular al extranjero," [Venezuela left without mobile calls abroad], *La Nación,* April 11, 2016, http://bit.ly/2dVoYQt.

17 "Sin "vidas" en el Internet más lento," [Without "lives" in the slowest Internet], *El Nacional,* April 24, 2016, http://bit. ly/2dnwly9.

18 Florantonia Singer, "Internet se estrecha en Venezuela," [Internet is constricting in Venezuela], *El Nacional,* February 14, 2015, http://bit.ly/2dmbYVA.

19 Akamai, State of the Internet, Q1 2016, http://akamai.me/2ecyiAU.

20 "Punto Fijo pasó más de 12 horas sin luz," [Punto Fijo spent more than 12 hours without light], *El Pitazo,* August 3, 2015, http://bit.ly/2dVOk0y; "Horarios especiales en centros comerciales por el racionamiento eléctrico," [Special schedules at malls due to electricity rationing], *El Universal,* February 1, 2016, http://bit.ly/2dmrvo3; "Mapa: Así se vio Venezuela durante 27 días de apagones programados cuatro horas diarias," [Map: This is how Venezuela looked during 27 days of programmed blackouts four hours a day], *El Pitazo,* May 23, 2016, http://bit.ly/1XQLKIg.

21 "100 salarios mínimos cuesta un iPhone en Venezuela," [Iphone costs 100 minimum salaries in Venezuela], *El Nacional,* September 28, 2015, http://bit.ly/1FFglC8; Patricia Laya, "Why the iPhone 6 Costs $47,678 in Venezuela," *Bloomberg, June 21, 2015,* http://bloom.bg/1FwJuZb; Capriles Prensa, Twitter post, April 1, 2016, 5:35pm, http://bit.ly/2dEUEGH; Humberto González, Twitter post, January 25, 2016, 6:30am, http://bit.ly/2dLUuRY.

22 Sebastian Boyd, "Black-Market Bolivars Crash Past 1,000 Per Dollar in Venezuela," *Bloomberg, February 3, 2016, http:// bloom.bg/1QHXB6R.*

goods, and Venezuela has the cheapest rates in Latin America, according to CASETEL.[23] CASETEL has called for a price increase, given that the variation of prices in the telecommunications basket represented 95 percent, compared to other goods or services that went up by 770 percent.[24] Movistar and Digitel also announced the possibility of raising the price of their plans, but CONATEL threatened them with sanctions.[25]

Figures from CONATEL show that the average cost of an internet service plan is VEF 219 a month. At the new official floating DICOM exchange rate on May 24 (VEF 472/US$),[26] this would represent less than US$0.50. Mobile data, according to the same source, cost around 0.50 VEF/MB, equivalent to US$0.001/MB. More than 90 percent of mobile data plans are prepaid.[27] Since July 2015, Movistar's basic plan cost 418 VEF a month (US$0.88). A similar plan from Digitel cost 359 VEF (US$0.76). Postpaid plans cost nearly 250 VEF (US$0.52) a month, which is less than 3 percent of the minimum wage.[28]

The digital gap between the capital and rural areas has in turn widened. While the Capital District boasted a penetration rate of 103 percent, Amazonas was under 20 percent. Out of 24 states, only 11 have an average larger than 50 percent.[29] Mobile broadband offers are concentrated in cities with populations of more than 50,000 people and in high-income zones. Some ISPs such as IPNet also offer speeds up to 25 Mbps in wealthy areas of Caracas. Among this elite minority with access to superior connections, some small online TV initiatives, such as Vivo Play, also gained users.[30]

The government has made some effort to increase connections, launching *Wi-Fi Plan for All* in 2013 in order to introduce Wi-Fi in public spaces, but has not been able to meet the demand.[31] The National Transportation Network, which was supposed to take optical fiber o rural and neglected areas of the country, was meant to be completed in 2012, but CONATEL'S website does not show any new information regarding this project. In April, in a meeting with ICT businessmen, the director of CONATEL announced that the National Transportation Network was moving forward,[32] but some of those present, who preferred not to be mentioned, said that "no figu es were shown in detail."

The government claims that the Simón Bolívar satellite has provided internet and mobile connec-

23 CASETEL press release, August 2015, http://bit.ly/2dpQ00d; See also: "Conozca las nuevas tarifas de Internet de Cantv," [See the new internet tariffs of Cantv], *El Estímulo*, July 1, 2015, http://bit.ly/2eJMT2m; Cantv, "Plans and Prices," http://bit.ly/1Izsof1.

24 Arnaldo Espinoza, "Casetel pide a la Asamblea realizar ajustes a tarifas de telecomunicaciones," [Casetel asks Assembly to make tariff adjustments in telecommunications], *El Estímulo,* February 19, 2016, http://bit.ly/2dM0oCj.

25 CONATEL, "Conatel ante el aumento de precios publicado por Digitel," [CONATEL facing the increase of prices published by Digitel] February 20, 2016, http://bit.ly/2dDg4Tp.

26 In March 2016, the Central Bank implemented changes to Venezuela's foreign currency exchange regime. DIPRO (VEF 10 / US$) is limited to essential food and medicine needs. DICOM is a free-fl ating exchange rate used for most other items. See: "Venezuela's new dual forex rate to start on Thursday," *Reuters, March 9, 2016, http://reut.rs/2ewJ3sr.*

27 Arnaldo Espinoza, "Venezuela tiene 27 millones de líneas celulares prepago" [Venezuela has 27 million prepaid cellphone lines], *El Estímulo,* November 17, 2015, http://bit.ly/2cYmSNY.

28 Movistar Plan (280MB, 300 minutes and 800 SMS), http://bit.ly/2cNIuhH; Digitel Plan (512MB, 300 minutes and 800 SMS), http://bit.ly/2dzcY6S; Movilnet Plan, http://bit.ly/2dqs6l8.

29 CONATEL, Statistics 2015.

30 Karla Franceschi, "La televisión en línea crece a pesar de las dificultades" [Online TV grows despite difficulties], *El Nacional*, September 21, 2014, http://goo.gl/BKFztm.

31 Daniel Pardo, "¿Por qué internet en Venezuela es tan lento?" [Why is internet in Venezuela so slow?] *BBC Mundo,* September 22, 2014, http://bbc.in/1WtaWSU.

32 William Castillo B (Tweet), April 12, 2016, 6:57am, http://bit.ly/2cOmEWB.

tivity to remote areas of the country, but independent sources could not yet verify these claims.[33] Meanwhile, a state-funded initiative for digital inclusion developed by the Infocentro Foundation has created some 900 centers offering free computer and internet access, and has progressively been handed over to the communities, although its sustainability is not guaranteed.[34]

During the 2015 electoral campaign, socialist party candidates accompanied by government official distributed free tablets to young university students in various areas of the country, in acts that were criticized as proselytism and created disturbances.[35] Other complaints denounced cellphones from state-owned company Movilnet being given to groups aligned with the ruling party.[36]

Restrictions on Connectivity

Although exact figu es are not available, the state owns the majority of the national level backbone infrastructure through the state provider CANTV.[37] The government discussed plans to establish an internet exchange point (IXP) in 2015 but has not indicated whether it will move ahead with this plan in the future.[38]

Internet service failures are common and often take a long time to fix. In August and Sep ember 2015, users in various states reported service breakdowns that lasted for several hours, particularly affecting the largest internet provider (ABA, from the state-owned CANTV).[39] ISPs that use the state-owned carrier were also reportedly unable to operate.[40] According to Juan Véliz, President of the Union of Telecommunication Workers, 126,000 failures were reported throughout the country in just three weeks.[41] In October 2015, the president of CANTV, Manuel Fernández, blamed these failures

33 CONATEL, "Satélite Simón Bolívar conectó zonas más remotas de Venezuela," [Simón Bolívar satellite connected most remote zones in Venezuela], October 29, 2015, http://bit.ly/1JEwJFh; See also: Jeanfreddy Gutiérrez, "Satélite Simón Bolívar solo usa 60% de su capacidad tecnológica a 7 años de su puesta en órbita," [Simón Bolívar satellite only uses 60 percent of its technological capacity after 7 years in orbit], *El Cambur*, October 29, 2015, http://bit.ly/2drwiRf.

34 "Infocentro celebra 15 años con más de 900 centros en Venezuela," [Infocentro celebrates 15 years with more than 900 centers in Venezuela], *La Red*, November 3, 2015, http://bit.ly/2cYuKPz.

35 César Batiz, "Al Psuv le dieron "una Tablet," [They gave PSUV a tablet], *El Pitazo*, December 8, 2015, http://bit.ly/1IPMmno; See also: Julio Mendoza, "En Apure denuncian irregularidades en donaciones de tablets a estudiantes universitarios," [Irregularities in tablet donations to university students denounced in Apure], *El Pitazo,* November 23, 2015, http://bit.ly/1lgmkEg; Bianile Rivas, "Entre angustia y trancas entregaron tablets en Portuguesa," [Between anguish and problems, tablets are delivered in Portuguesa], November 23, 2015, http://bit.ly/2dnyz1l; Julio Mendoza, "Bachilleres de Misión Sucre en Apure fueron golpeados y apresados por protestar y exigir tabletas" [Students in Apure were beaten and detained for protesting and demanding tablets], November 25, 2015, http://bit.ly/1NtLrAq.

36 Edecio Brito, "Gobierno entregó 387 celulares a Frente de Mototaxistas en Barinas," [Government distributed 387 cellphones to mototaxi front in Barinas], *El Pitazo,* August 23, 2015, http://bit.ly/2dmmlZp.

37 Personal interviews with a variety of telecommunications experts, and information about the holdings of the state-owned CANTV seem to indicate that the government may control roughly 60 percent of the national-level backbone infrastructure.

38 Crisbel Villaroel, "Conatel idea plan para modernizar el Internet" [Conatel devises plan to modernize the internet], *El Mundo,* August 13, 2015, http://bit.ly/2dmofcE.

39 "Reportan falla de ABA Cantv en varios estados de Venezuela," [Failure of ABA Cantv reported in various states in Venezuela], *Entorno Inteligente,* August 13, 2015, http://bit.ly/2dEZgRk; See also: IPYS Venezuela, "Usuarios reportaron falla de internet a través del servicio ABA – CANTV," [Users report internet failures through ABA Cantv service], September 11, 2015, http://bit.ly/2cNTYSc; "Fuertes lluvias afectaron sistema eléctrico e internet" [Heavy rain affected the electricity and internet system], *Entorno Inteligente,* September 15, 2015, http://bit.ly/2dzo4Zz; "Reportan fallas en servicio de internet ABA de Cantv," [ABA Cantv internet service failures reported], *Entorno Inteligente*, October 1, 2015, http://bit.ly/2dmrnFm.

40 "Clientes de Vearco Telecom sin internet por culpa de CANTV," [Clients of Vearco Telecom without internet because of CANTV], *Entorno Inteligente,* September 17, 2015, http://bit.ly/2dzpkMe.

41 "Sindicato de CANTV: Mal servicio de la empresa se debe a la falta de inversión" [CANTV union: bad service due to lack of investment], *Noticias al día ya la hora*, October 30, 2015, http://bit.ly/2dryFUj.

and slow connection speeds on the widespread growth of services,[42] and announced an investment of 200 million dollars to modernize CANTV and Movilnet networks.[43]

Digital activists have questioned whether constant service blackouts were a trial for larger service problems in the lead-up to December 2015 elections.[44] On election day, two NGOs—the Institute for Press and Society (IPYS-Venezuela) [45] and Acceso Libre (Free Access)[46]—noted interruptions of CANTV-ABA and Inter services in 12 states of the country. Venezuelan journalist Fran Monroy observed that "internet providers in Venezuela 'suspiciously' lowered their normal bandwidth" in the lead-up to election day.[47] *Dyn Research* confi med a minor reduction in traffic le els that weekend. Though not a total blackout, the research showed some level of connectivity impairment.[48] CANTV blamed the disruptions on the massive use of internet for election-related purposes,[49] whereas CONATEL argued that these reports were part of "operations of disinformation" aimed at creating anxiety and uncertainty.[50] A study by IPYS-Venezuela after the election observed improvements in network performance.[51]

ICT Market

Although there are 86 private providers, the state dominates the ICT market. Almost 70 percent of users access the internet through CANTV's ABA (Broadband Access), or through the state-owned mobile provider, Movilnet.[52] One of the objectives of the Second Socialist Plan for the Economic and Social Development of the Nation (2013-2019) is for Venezuela to reach "non-vital levels" of connection with communication and information networks "dominated by neo-colonial powers."[53]

Foreign currency controls prevented private companies from repatriating their earnings and accessing the foreign currency necessary for investment, which led to a deterioration of their services. It also created a substantial barrier to new fi ms who might seek to enter the market. The shortage of equipment was also rampant due to the lack of dollars to pay for imports. On special occasions like Mother's Day, cell phones were offered at exorbitant prices.[54]

CANTV, the only provider offering ADSL services, dominates the fi ed broadband market, providing

42 "Manuel Fernández niega que Venezuela ocupe los últimos lugares en velocidad de internet," [Manuel Fernández denies that Venezuela ranks one of the last in internet speed], *Contrapunto*, October 15, 2015, http://bit.ly/2d9LYYd.

43 María Jorge, "Hasta un año pueden durar las averías telefónicas y de red de Cantv," [Cantv telephone and network failures can last up to one year], *El Nacional*, November 22, 2015, http://bit.ly/2cYwSaf.

44 Luis Carlos Díaz, "Cantv: ¿Fallas o nuevos ensayos de bloqueos de Internet en Venezuela?" [Cantv: Failures or new trials to block internet in Venezuela?], *Medium,* October 2, 2015, http://bit.ly/2dM9grA.

45 Mariengracia Chirinos, Ipys Venezuela office , personal email, December 17, 2015.

46 Acceso Libre, "Al menos doce estados venezolanos presentaron fallas de Internet durante el fin de semana electoral," [At least twelve Venezuela states had internet failures during the electoral weekend], December 11, 2015, http://bit.ly/2dDlGgt.

47 Sabrina Martín, "Denuncian bloqueo intencional de las comunicaciones en Venezuela," [Intentional blocking of comunications in Venezuela is denounced], *Panampost*, December 3, 2015, http://bit.ly/2dNoKrY.

48 Doug Madory, Director of Internet Analysis at Dyn Research, personal email.

49 CANTV, "Cantv garantiza servicios de telecomunicaciones," May 12, 2015, http://bit.ly/2dzr9bO.

50 CONATEL, "Directorio de Responsabilidad Social y Conatel al país," [Directorate of Social Responsibility and Conatel to the country], December 3, 2015, http://bit.ly/2cYzbtR.

51 IPYS Venezuela, "Principales hallazgos de la navegación en Venezuela," [Main findings on in ernet surfing in enezuela], March 29, 2016, http://bit.ly/2aOk7jS.

52 Andrés Herrera, "94,2% de las conexiones fijas a In ernet en Venezuela son lentas," [94.2 percent of fi ed internet connections in Venezuela are slow], *Sumarium*, June 11, 2015, http://bit.ly/1OCbV1Y.

53 Homeland Plan, 4.4.2.3, http://bit.ly/1MpSdlZ.

54 "Los nuevos y altos precios de Movilnet para el Día de las Madres," [The new and high prices of Movilnet for Mother's Day], *El Nacional*, May 5, 2016, http://bit.ly/1T0tMQo.

service to nearly 70 percent of users in this market. The rest of the population accesses the internet through one of several private telecommunications providers.[55] Three companies offer internet access via cable modem. Inter, the second most widely used ISP, offers services only in major cities. Although it used to offer a connection speed of 10 Mbps, this plan is no longer available; currently, this company is primarily selling its 1 MB plan, which, in comparison, is more expensive than the plan offered by ABA-CANTV.[56]

Movilnet, the state telecommunication provider, is also dominant in the mobile market with approximately half of the users of CDMA/EvDo technologies. Movistar, with HSPA+ technology and a reduced LTE offer, holds 34 percent of the market. Digitel, which holds 16 percent of the market, is the leading LTE network operator, a technology that has not been fully utilized due the shortage of smartphones.[57]

Regulatory Bodies

The state controls CONATEL, the entity responsible for regulating and licensing of the telecommunications sector. The Law on Social Responsibility on Radio, Television, and Digital Media (Resorte-ME) grants the regulatory body the power to rule over the blocking or deletion of content and to sanction service providers, an ability it has exercised without granting due process to the affected parties (see Blocking and Filtering).[58]

While Article 35 of the Organic Law of Telecommunications provides for CONATEL's operational and administrative autonomy, Article 40 states that the president has the power to appoint and remove the agency's director and the other four members of its board,[59] pointing to CONATEL's lack of independence from the executive. Venezuela's political and regulatory environment was ranked last out of 143 countries in the World Economic Forum's Networked Readiness Index, which measures the capacity of countries to leverage ICTs for increased competitiveness and well-being.[60]

Limits on Content

Websites related to the black market were most frequently blocked in Venezuela, but media sites and blogs critical of the government were also targeted. Third-party liability encourages self-censorship and content removal, as does the threat of harassment of critical journalists by government sympathizers. Despite these limitations, the online landscape remains vibrant in Venezuela, thanks to the emergence of new digital media and increasingly critical users.

55 "Venezuela - Telecoms Infrastructure, Operators, Regulations - Statistics and Analyses," Budde.com.au, http://bit.ly/2dnMTqV.

56 For Intercable's plans, see http://bit.ly/1LX2HXF; For CANTV's plans, see http://bit.ly/1NOAj0t

57 Heberto Alvarado, "Internet venezolana: desigual, lenta y arcaica ¿Cómo se sale del sótano sudamericano?" [Venezuelan Internet: unequal, slow and archaic: how does one exit the South American basement?] *Runrun.es*, December 2, 2015, http://bit.ly/2dNy66N.

58 Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos, 2012, [Law on Social Responsibility in Radio, Television and Electronic Media] http://bit.ly/1LK14B4.

59 Ley Orgánica de Telecomunicaciones [Organic Law on Telecommunications] art. 35-48, http://bit.ly/1GcpLA4.

60 The ranking took into consideration judicial independence, effectiveness of law-making bodies, efficiency f legal framework in settling disputes, efficiency f legal framework in challenging regulations and Intellectual property protection. See: World Economic Forum, The Global Information Technology Report 2015, accessed October 3, 2016, http://bit.ly/1FT9apa.

Blocking and Filtering

Blocking of political, social, and economic content continued during this coverage period. In July 2015, Infobae reported that its information portal was blocked following the publication of two critical articles about the human rights situation in Venezuela. It has used alternative sites such as "Infobae.media" and "Infobae.press" to circumvent blocking.[61]

On October 1, 2015, Alberto Ravell, director of *La Patilla,* the top digital outlet in the country, reported that traffic on his si e had been blocked by CANTV in Caracas.[62] Users also reported that other news sites with political content, such as *Maduradas, Aporrea* and *Informe 21*, were inaccessible through CANTV on the morning of October 1.[63] Other complaints involved websites related to Bitcoin,[64] and news websites such as "diariodecuba.com" and "infodio.com." While there were suspicions of blocking of specific ages, a large number of portals were reportedly inaccessible. As reported by DolarToday, a test by CloudFlare engineers found that "the issue seems to be due to a router loop near the client," concluding that other sites using CloudFlare were affected by an attempt to block DolarToday.[65]

A study conducted by NGO Ipys-Venezuela during the parliamentary election campaign between November 2015 and January 2016 also confi med a number of blockings. The study, which covered a sample of three states of the country and the metro area, noted that 43 websites were systematically blocked by one or more ISPs. The fi e most important ISPs blocked NTN24 website and Infobae. Some 44 percent of the websites blocked were related to the black market of currency, while 19 percent were media-related. Others included blogs critical of the government and gambling sites. The study also confi med that the domains of advocacy and human rights organizations were freely accessible.[66]

In June 2015, CONATEL's director, William Castillo, told a delegation from the UN Human Rights Committee, investigating whether Venezuela has breached the International Covenant on Civil and Political Rights, that it "legally" blocked 1,060 websites.[67] Although he denied that this was an official policy, he recognized that over 900 links of the website DolarToday were blocked.[68]

CONATEL has denied requests by NGO Espacio Público about the legal procedures followed to order

61 "El régimen de Maduro volvió a bloquear Infobae en Venezuela," [Maduro regime blocked Infobae in Venezuela again], Infobae, July 20, 2015, http://bit.ly/2cQx3RH; See also: "La Fundación LED repudió el bloqueo de Infobae en Venezuela," [LED foundation condemned blocking of Infobae in Venezuela], Infobae, July 21, 2015, http://bit.ly/2dG6Upd.

62 Alberto Ravell (Tweet): "LaPatilla bloqueada por CANTV en la Gran Caracas" [La Patilla blocked by CANTV in Gran Caracas], October 1, 2015, http://bit.ly/2dPFlet.

63 María Fermín, "Afi man que servicio de ABA impidió acceso a páginas web," [They affi m that ABA service prevented access to web pages], El Nacional, October 3, 2015, http://bit.ly/1Z0rcwV.

64 "State owned and biggest ISP in Venezuela have blocked all Bitcoin related domains, websites and pools," Reddit, October 1, 2015, http://bit.ly/2dHencX.

65 "¡CONFIRMADO! CANTV y Conatel bloquean a medio Internet para sacar a DolarToday del aire ¡SIN ÉXITO!" [Confi med! CANTV and Conatel blocked half of the internet to take DolarToday offline, without success!], Dolar oday, October 1, 2015, http://bit.ly/1P88VJK.

66 Ipys-Venezuela, "Principales hallazgos de la navegación en Venezuela," [Main findings on surfing in enezuela], March 29, 2016, http://bit.ly/2aOk7jS.

67 Mayela Armas, "Castillo: "Legalmente" 1.060 sitios han sido bloqueados por requerimiento de otras autoridades," [Castillo: 1,060 were "legally" blocked by request of other authorities], *Crónica Uno*, June 30, 2015, http://bit.ly/2dof3V6.

68 Dólar Today is a prominent site run out of Florida which publishes the black market exchange rate.

the blocking of websites.[69] Similarly, the Second Court of Administrative Settlements rejected Espacio Publico's appeal against CANTV for failing to report blockings in Venezuela.[70]

Content Removal

Content related to economic issues or political criticism were regularly targeted for removal during the coverage period.

The Law on Social Responsibility on Radio, Television, and Electronic Media (the Resorte-ME law) establishes that intermediary websites can be held liable for content posted by third parties, and grants CONATEL the discretional capacity to impose severe penalties for violations. Its provisions notably forbid messages that promote anxiety among the population, alter public order, disregard legal authorities, or promote the violation of existing laws. This legal framework has resulted in self-censorship and preemptive censorship, as webmasters and editors may avoid publishing information that contradicts the government.

In November 2015, the Organic Law of Fair Prices was modified o include a provision about "fraudulent dissemination of prices," giving the Superintendence of Fair Prices (SUNDEE) the power to punish media outlets and webpages for economic crimes prescribed in the law (see Legal Environment).[71] Shortly after, the Vice President and the Minister for Industry and Trade ordered the managers of Mercadolibre.com to take down ads for regulated products from the website, as well as drugs, tires and batteries.[72]

There were few reports of judicial measures to request deletion of content during the coverage period. In June 2015, the Violence against Women Court forced journalist Saúl Acevedo to delete Twitter posts that satirized the governor of Táchira state and his the wife, Karla Jiménez de Vielma, who had filed a complaint against Ace edo for abuse and bullying. The court also banned him from "intervening (…) on any media outlet or communication platform violating the rights" of Jimenez and her family.[73]

Several videos posted on YouTube and other media sites were also targeted for removal. In November 2015, the National Electoral Council (CNE) launched administrative procedures against the Venezuelan Chamber of Food Industry (CAVIDEA) and the Catholic University Andrés Bello (UCAB), urging them to remove a series of videos on their YouTube channels that promoted the right to vote in the December elections.[74] According to the CNE, the videos violated campaign rules prohibiting the dissemination of political propaganda and voting by unauthorized persons. The outcome of the procedures remain unknown as of mid-2016, though the videos were never removed.[75]

69 Espacio Público, "CONATEL niega información sobre páginas web bloqueadas," [CONATEL denies information on blocked websites], May 28, 2015, http://bit.ly/2dbkvVX.

70 Edgar López, "El Gobierno tiene el secretismo como política de Estado," [The government has secretism as a state policy], *El Nacional,* September 27, 2015, http://bit.ly/1Vhlbg0.

71 Gaceta official de la República Bolivariana de Venezuela [Official Gazette of the Bolivarian Republic of Venezuela, Nr. 40.787], November 12, 2015, http://bit.ly/2d48FiR.

72 "El régimen de Nicolás Maduro restringió las ventas en el sitio de Mercado Libre," [Maduro regime restricted sales on Mercado Libre website], *Infobae,* November 27, 2015, http://bit.ly/2dqI8xI.

73 Ipys-Venezuela, "Tribunal ordenó a locutor eliminar mensajes publicados en su cuenta de Twitter," [Court ordered newscaster to delete messages published on his Twitter account], June 8, 2015, http://bit.ly/2dtaqFr.

74 IPYS Venezuela, "Poder electoral dictó una medida de censura previa," [Electoral power dictated preventive censorship measure," November 21, 2015, http://bit.ly/2d0U87t.

75 The videos are still available on the Youtube channel "PolítiKa UCAB," accessed October 4, 2016: http://bit.ly/1SJvnbE.

Meanwhile, observers have commented on the disappearance of politically sensitive information from some media websites and platforms, many of them without clear explanation. Such was the case of an October 2015 interview conducted by the well-known journalist César Miguel Rondón with the director of *El Pitazo* and *Poderopedia,* César Batiz, and the director of Transparency Venezuela, Mercedes de Freitas. The interview segment, which discussed corruption allegations against a nephew of President Maduro's wife, was inexplicably removed from the website of the Éxitos FM radio station.[76]

In February 2016, an opinion poll conducted by state television station Venezolana de Television (VTV), was removed from all media, including a screenshot posted on Twitter.[77] The survey suggested majority support for an amnesty law to release jailed dissidents, which was being discussed in the National Assembly at the time.

In November 2015, a fictional video called "La umba" (The Tomb) depicting the situation of Venezuelan political prisoners was removed from Facebook, with no clear explanation.[78] According to Marianne Díaz, director of the NGO Acceso Libre, Facebook did not respond to inquiries about the case, concluding: "Although no technical tests were conducted, according to Citizen Lab, this could be a case of preemptive censorship."[79]

Media, Diversity, and Content Manipulation

Compared to traditional media, the digital sphere presents a more vibrant space for political and social expression and is becoming a popular way to access information. However, the government has increasingly sought to expand its influence online, using sta e-controlled media and encouraging pro-government social media users to harass opposing views.

The economic crisis has impacted media outlets with scarce resources to pay for qualified p ofessionals, generate quality content, and promote goods and services through advertising. Censorship and self-censorship have in turn constrained critical reporting. In the lead-up to parliamentary elections in December 2015, a survey of 227 journalists found that 18 percent did not report certain news for fear of legal and administrative reprisals. Complaints filed by senior go ernment officials are often based on defamation and libel (see Legal Environment).[80]

Despite economic constraints and a climate of censorship, the emergence of new digital ventures over the past few years has been remarkable.[81] Print media have migrated to the web due to restrictions on newsprint, [82] while broadcast media have also forged an online presence. Only two state outlets—the Venezuelan News Agency, and state TV station Venezolana de Televisón—are among the top 25 Venezuelan digital media outlets (in positions 24 and 26 respectively), according to a

76 IPYS Venezuela, "Circuito radial bajó de su página web entrevista sobre opacidad, [Circuito Radial removed interview on opacity from its website], October 2, 2015, http://bit.ly/2cQXaI4.

77 Geraldine Lucero, "La encuesta de VTV que está dando de qué hablar," [VTV poll is creating a lot of talk], *El Pitazo*, February 16, 2016, http://bit.ly/1ontTel.

78 Marianne Díaz, "Facebook Disappearing Act," Online Censorship, December 11, 2015, http://bit.ly/1OuoTKe.

79 Marianne Díaz, personal communication via Twitter.

80 IPYS Venezuela and Venezuelan Electoral Observatory (OEV), "Mutismo en la antesala electoral," [Mutism in the electoral anteroom], 2015, http://bit.ly/2aPQdJX.

81 John Otis, "In Venezuela, online news helps journalists get their voices back," *Committee to Protect Journalists (blog)*, June 1, 2015, http://bit.ly/2duKSHA.

82 In Venezuela the sale of paper for printing is an activity reserved to the government. The restriction on the distribution of this input is used as a mechanism to punish critical media.

ranking produced by Medianálisis in March 2016. Of those supportive of the ruling party, Laiguana.tv appears better ranked, in sixth place, while openly pro-opposition outlet *La Patilla* leads the ranking.[83]

New outlets linked to non-governmental organizations have also emerged, such as *Crónica Uno*, an initiative of Espacio Público focusing on low-income sectors that traditionally lack coverage, and *El Pitazo*, incubated by IPYS Venezuela, which has also developed a network of journalists located in various states, allowing them to broaden sources of information beyond the capital.[84] The emergence of initiatives such as VivoPlay.net is also noteworthy: an over-the-top content (OTT) platform which, through its live signal, transmits its own news production. According to journalist Eugenio Martínez, Vivo Play counted some 60,000 subscribers in early 2016, which, in a country with an average speed of 1.5 Mbps is nothing short of remarkable.

The polarization of media coverage was especially acute during the electoral period in the second half of 2015. A study by the Global Observatory of Communication and Democracy found that, while traditional media disproportionately privileged government voices, new digital media such as *Efecto Cocuyo* were able to offer different perspectives on the electoral process. Citizen voices were also found to dominate election-related conversations on Twitter, more than accounts linked to the government or media outlets.[85] On the other hand, efforts to capture online platforms in favor of the ruling party were apparent: in open violation of the electoral law, some official platfo ms were used to disseminate partisan information rather than official info mation from the state. For example, the Ministry of Information and Communication posted videos in favor of ruling party candidates on its YouTube channel.[86]

The creation of a "cyber army of militants," known as la "tropa" (the troop), has in turn enabled the government to position itself online. Some government supporters linked their accounts with the president's website to replicate his messages. "Maduro's account received the third largest amount of retweets recorded among all world leaders," noted cyber activist Luis Carlos Díaz.[87] Social media analysts have also found that automated accounts (bots) are being used to disseminate progovernment content.[88] However, academic studies have concluded that while the government uses bots to extend its impact on social media, "the most active bots are those used by Venezuela's radical opposition" and that "they promote innocuous political events more than attacking opponents or spreading misinformation."[89]

While most government officials decline media in erviews, they offer biased information, or target-

83 Medianálisis, "Top Ranking de Medios Digitales en Venezuela del mes de marzo 2016" [Top ranking of digital media in Venezuela – March 2016], April 4, 2016, http://bit.ly/2dtmzKP.

84 Other outlets include, among others: EfectoCocuyo.com; Runrunes.es; Armando.Info; Prodavinci.com; Notiminuto.com; elestimulo.com; contrapunto.com; elcambur.com.ve; See also: Jeanfreddy Gutiérrez, "La aparición de medios digitales nativos en el periodismo venezolano," [The appearance of native digital media in Venezuelan journalism], *El Cambur*, June 27, 2015, http://bit.ly/1Joj694.

85 OGCD, "La cobertura mediática del proceso electoral parlamentario 2015," [Media coverage of the parliamentary election process 2015], June 2016, http://bit.ly/2cRbnVq.

86 IPYS Venezuela, "Minci convierte su canal de Youtube en un espacio de propaganda para candidatos del PSUV," [Ministry of Information turns its YouTube channel into a propaganda platform for PSUV candidates], December 3, 2015, http://bit.ly/2dtw7FA.

87 Franz Von Bergen, "Maduro lucha por ser trending topic," [Maduro fights o be a trending topic], *El Nacional*, June 28, 2015, http://bit.ly/1edI3t5.

88 Hannah Dreier, "Venezuela ruling party games Twitter for political gain," AP, August 4, 2015, http://apne.ws/1MKOxhI.

89 Forelle, M et al., Political Bots and the Manipulation of Public Opinion in Venezuela, July 2015, http://arxiv.org/abs/1507.07109.

ed information, via Twitter, which often gets retweeted by followers. Analyzing fi e hashtags promoted by the government in May 2015, an investigation by IPYS-Venezuela found that these were promoted by public accounts. The report concluded that progovernment cooptation of the state media platform, including digital media, prevents Venezuelans from accessing timely and adequate information.[90]

Digital Activism

Despite limitations, Venezuelans are avid internet users, and social networks have become important tools for activism and political mobilization.[91] According to Tendencias Digitales, Venezuelans often go online to use social networks (75 percent), consume news (74 percent), and search for information (51 percent). The most popular social network is Facebook with over 13 million users.[92] Some 70 percent of Venezuelans on the net use Twitter, considerably higher than the regional average of 50 percent.[93] Some 50 percent of Venezuelan internet users also have Instagram, compared to 35 percent in the region.

Social media was an important battlefield bet een competing political factions during the elections, as hashtags such as #PaLaAsambleaComoSea and #VenezuelaQuiereCambio sought to mobilize for change.[94] A study published by IPYS-Venezuela in February 2016 noted that the word "war**"** was a trending word among candidates on Twitter.[95] The positioning of hashtags on Twitter's trending topics also intensified during the elec oral campaign, as ministries and some public enterprises worked to promote hashtags such as #PorMásSaludel6DGanaChávez, #RumboALaVictoriaChavista, and #YoVotoPorLaGenteDeChávez.[96]

Ahead of the December 2015 elections, candidates to the National Assembly launched websites, created Facebook profiles and made ex ensive use of social networks such as Twitter, Instagram, YouTube, and even Periscope.[97] For example, Miranda state governor Henrique Capriles—who some say is the Spanish-speaking politician with the most followers worldwide, with more than six million followers[98]—covered the launch of his campaign through the Facebook Mentions application and

90 IPYS Venezuela, "El tuitómetro del gobierno en Venezuela" [The government's tweet-o-meter in Venezuela], http://bit.ly/2d3JKfc.

91 Margaret López, "Venezuela tuvo "crecimiento pírrico" en penetración de Internet," [Venezuela had "Pyrrhic growth" of internet penetration], *Analitica,* September 24, 2015, http://bit.ly/2dLaeoB; Daniela Dávila, "INFOGRAFÍA: Así repercute la realidad venezolana en la conectividad y los usos de Internet," [Infographic: this is how the Venezuelan reality affects connectivity and internet usages], *RunRunes*, September 24, 2015, http://bit.ly/1WFPD0C.

92 Owloo, Facebook Statistics, accessed February 16, 2016, http://bit.ly/2dKxpuz.

93 "Colombia es el segundo país con más tuiteros en América Latina," [Colombia is the second country with most Twitter users in Latin America] *La República,* March 13, 2015, http://bit.ly/1BdKUG6.

94 Mar Pichel, "¿Qué papel juegan las redes sociales en las elecciones de Venezuela?" [What role do social media play in Venezuelan elections?], *CNN en español*, December 3, 2015, http://cnn.it/1O7QbWN; See also: Gerardo GUARACHE, "La batalla electoral venezolana arde en las redes sociales," [The electoral battle is ablaze on social networks], AFP, November 28, 2015, http://yhoo.it/2dvJF3e.

95 El *Tuitómetro parlamentario* examined the profiles f 67 candidates for deputies in the National Assembly of the United Socialist Party of Venezuela (PSUV) and the Democratic Unity Roundtable (MUD) between January 2015 and January 2016. See: IPYS Venezuela, El Tuitometro parlamentario, http://bit.ly/1QnBfc0.

96 Arysbell Arismendi, "Maduro llama a respetar la veda electoral y el Psuv bombardea en Twitter para votar por el oficialismo" [Maduro calls to respect the electoral ban and PSUV bombs Twitter to vote for the governing party], *El Pitazo,* December 5, 2015, http://bit.ly/1Q7q0We.

97 Abraham Salazar, "MUD y PSUV hacen la batalla de campaña por redes sociales en Libertador," [MUD and PSUV fight the campaign on social networks in Libertador], *Efecto Cocuyo,* November 24, 2015, http://bit.ly/2dffyex.

98 Carmen Beatriz Fernández, Twitter post, May 25, 2016, 1:17am, http://bit.ly/2dxSRDX.

transmitted his press conferences via Facebook, Periscope, and his channel on IP CaprilesTV.[99] Opposition party MUD launched a news channel on YouTube three days before the election,[100] making heavy use of social networks and using material from citizen journalists who submitted videos via WeTransfer or Periscope.[101]

After the election and inauguration of new opposition deputies, the National Assembly official V channel was "dismantled" by government officials, making way for the new chamber o begin transmitting its sessions via YouTube.[102] In February 2016, President Nicolás Maduro also announced a new Facebook page,[103] and his new TV show *En Contacto con Maduro* is disseminated via Twitter, Facebook, YouTube, Periscope and LiveStream.[104]

New digital media and social networks also strongly impacted the coverage of the elections. The network of activists @reporteya and the newspaper @elnacionalweb conducted workshops throughout the country to train citizens on how to monitor and cover the electoral process online.[105] Digital media and NGOs created alliances to monitor incidents before and during the electoral process, including the newspaper *Tal Cual* and digital media outlets *Runrunes, El Pitazo, Poderopedia* and *Crónica Uno*, which provided coverage through nearly 100 journalists in 23 cities.[106] The coalition included the NGO Transparencia Venezuela, offering a platform for citizen complaints, Dilo Aquí.[107]

To monitor electoral irregularities, the citizen oversight platform, El Guachimán Electoral, created a digital map of electoral incidents by using SMS, Twitter (#GUACHIMAN6D), WhatsApp and its website.[108] At the end of the election, it reported that more than 85 percent of the information received came from citizens: 5,337 messages through its platform, 1,179 emails, 1,000 SMS, and 3,704 tweets with the hashtag #guachiman6D.[109] The NGOs Acceso Libre and IPYS-Venezuela, also monitored internet access restrictions during the elections.[110] Finally, during the tense vote count between December 6 and 7, when CNE had yet to announce the fi st results, Lilian Tintori, wife of political prisoner Leopoldo López, sent a tweet with a video announcing the opposition's victory. With over 2 million Twitter followers, the post went viral within minutes.[111]

---

99 Carmen Beatriz Fernández, Twitter post, February 17, 2016, 4:47am, http://bit.ly/2dsp9nV; See also: Luis Carlos Díaz, Twitter post, February 18, 2016, 7:02am, http://bit.ly/2dso9QJ.

100 Democratic Unity Roundtable, "Unidad lanzó Sala de Prensa en Internet," [Unity lauched pressroom on Internet], December 3, 2015, http://bit.ly/1Q3ImHE.

101 Aliana González, "Canal de la oposición venezolana por YouTube hizo historia al ofrecer por primera vez una cobertura electoral full HD en vivo por streaming," [Venezuelan opposition YouTube channel made history by offering for the fi st time full HD livestreaming of election coverage], December 7, 2015, http://bit.ly/2dLf1Gw.

102 National Assembly YouTube channel, http://bit.ly/1mbePOX.

103 "Maduro utilizará Facebook para "ampliar" su uso de redes sociales," [Maduro will use Facebook to "widen" his use of social networks], *El Pitazo,* February 9, 2016, http://bit.ly/2dfhzHF.

104 See: www.nicolasmaduro.org.ve and livestream.com/encontactoconmaduro

105 "El Nacional y Reporte Ya forman a los venezolanos para cobertura 2.0 el 6D," [El Nacional and Reporte Ya train Venezuelans on 2.0 coverage for December 6], *El Nacional*, November 11, 2015, http://bit.ly/2duc4Hk.

106 "Cinco medios y una ONG se unen para informar sin censura sobre el proceso electoral del 6D," [Five media and one NGO unite to inform on the election without censorship], *RunRunes,* December 3, 2015, http://bit.ly/2dLguww.

107 See: www.transparencia.org.ve/diloaqui

108 Platform developed by IPYSVenezuela, see: guachimanelectoral.com

109 Silvia Higuera y Teresa Mioli, "Redes sociales, crowdsourcing y periodismo ciudadano ayudaron a los medios a cubrir las elecciones venezolanas" [Social networks, crowdsourcing and citizen journalism helped media cover Venezuelan elections], *Knight Center (blog),* December 8, 2015, http://bit.ly/1XWIjSu.

110 Acceso Libre, "Al menos doce estados venezolanos presentaron fallas de Internet durante el fin de semana elec oral" [At least twelve states presented internet failures during the electoral weekend], December 11, 2015, http://bit.ly/2dDlGgt.

111 "Video de celebración de Lilian Tintori revoluciona las redes sociales," [Lilian Tintori's celebration video revolutionizes social networks], *El Nacional,* December 6, 2015, http://bit.ly/1OdoYlx.

In March 2016, the website revocalo.com was launched to collect signatures and mobilize citizens in favor of a referendum to revoke the mandate of President Maduro. Venezuelans have also created websites, applications, and Twitter accounts in order to exchange information to overcome the shortage of medicines caused by the country's economic crisis.[112]

Violations of User Rights

In September 2015, prominent opposition leader Leopoldo López was sentenced to 14 years in prison. In his conviction for "instigation to commit crimes" during anti-government protests in 2014, prosecutors analyzed hundreds of tweets and a YouTube video. While six of the nine imprisoned Twitter users who were detained until May 2015 were released, the digital sphere has been progressively more restricted through coercive laws and surveillance mechanisms. Meanwhile, journalists, cyber activists, and ordinary users experienced routine harassment and violence for their online activities.

Legal Environment

Although the Constitution guarantees freedom of expression,[113] the government has passed a number of laws and regulations that curtail this right online.

In 2010, the National Assembly amended the Law on Social Responsibility in Radio, Television and Electronic Media (Resorte-ME) to include vague prohibitions and severe sanctions that grant authorities sweeping discretion to restrict speech.[114] Article 27, for example, forbids messages that promote anxiety among the population, alter public order, disregard legal authorities, or promote the violation of existing laws. The law also establishes intermediary liability for content posted by a third-party and requires online media to establish mechanisms to restrict prohibited content. Websites found in violation of these provisions may be heavily fined, and se vice providers who do not comply risk temporary suspension of operations.[115]

Activists and journalists also face charges of defamation under the penal code, which sets out prison sentences for defamation against public officials and the publication f false information.[116] Other laws provide additional avenues for limiting speech: for example, the Law of National Security, which was passed in January 2015, outlines prison sentences for individuals who "compromise the security and defense of the nation."[117]

In November 2015, a reform of the Law of Fair Prices established prison sentences and heavy fines for electronic media that publicize information about the alteration of prices of goods and ser-

112 See websites such as "akizta.com," applications such as "Redes Ayuda" and Twitter accounts such as "SeBuscaSeDona"; See also: "Las redes sociales se convierten en 'farmacias virtuales' en Venezuela," [Social networks become "virtual pharmacies" in Venezuela], CNN en español, March 31, 2016, http://cnn.it/22TDjjT; "¿Cómo encontrar medicamentos en Venezuela a través de redes sociales?" [How to find medicine in enezuela through social networks?], *Efecto Cocuyo*, March 25, 2016, http://bit.ly/1LN7yl3.

113 Constitution of the Bolivarian Republic of Venezuela, art. 56 and 57, http://bit.ly/1ZlAgdc.

114 "Ley Resorte restringe la libertad de expresión en internet y medios electrónicos," [The Resorte Law restricts liberty and expression on the internet and electronic media], *Espacio Público*, December 10, 2010, http://bit.ly/1RbGg5W.

115 Law on Social Responsibility on Radio and Television reformed, 2010, http://bit.ly/1LK14B4.

116 Gaceta Oficial, N5.494, Código enal de Venezuela, [Penal Code of Venezuela], art. 444, October 20, 2000, http://bit.ly/1hBfNfy.

117 "Presidente Nicolás Maduro usó ley habilitante para legislar contra la libertad de expresión," [President Nicolas Maduro used enabling law to legislate against freedom of expression], *Espacio Público,* January 22, 2015, http://bit.ly/1MUKnEN.

vices.[118] Under Article 61, "Whoever disseminates by any media, false news, employs violence, threats, deceit any other scheme to alter the prices of goods or services [...] shall be sanctioned with imprisonment of two to four years." As a result, at least 15 people were arrested on the same month it came into force (see Prosecutions and Detentions for Online Activities).[119]

Parliamentary elections in December 2015 marked a shift in power in the legislative branch from the ruling United Socialist Party of Venezuela (PSUV). The opposition alliance won a majority of seats in the National Assembly, paving the way for possible reforms of two crucial laws: the Law of Telecommunications and Resorte-ME.[120] However, the Constitutional Chamber of the Supreme Court, whose members were selected by the outgoing pro-government National Assembly, has been able to rule against new legislation promoted by the opposition as unconstitutional.[121]

Prosecutions and Detentions for Online Activities

Several individuals were arrested for their online activities during the coverage period.

One of the most prominent incidents was the trial and conviction of opposition leader Leopoldo López. Held since February 2014 in a military prison, he was sentenced to nearly 14 years on charges of conspiracy, public incitement, and responsibility for property damage and fi e in September 2015.[122] The central argument of the prosecution was a speech he gave on February 12, calling for people to join the movement #LaSalida, which, according to the judge, sparked protests that sought to topple the government and caused the death of 43 people. The interpretation of his speech was based on the analysis of his tweets,[123] as well as a video that circulated on YouTube.[124] Although López had called for nonviolence, the prosecution asserted that he had used "subliminal" messages to incite others to commit crimes.[125] After the sentencing, prosecutor Franklin Nieves fled the cou - try claiming that he had been pressured to accept false evidence, and sought political asylum in the United States.[126] The trial, which by rule should have been public, was virtually inaccessible for Venezuelans who used social networks to stay informed, while international news outlets faced difficulties in covering the trial.[127]

Journalists also faced arrests and questioning for reporting on sensitive stories or while covering protests during the year (see also Intimidation and Violence). On March 18, radio journalist Pedro Luis Montilla, who reported on the disappearance of 28 gold miners near the town of Tumeremo on

118 Official Gazet e, Nr. 40.787, November 12, 2015, http://bit.ly/2d48FiR.

119 D. Bracho, "Arreaza: Hay 15 detenidos por venta de productos con sobreprecio en internet" [Arreaza: 15 arrested for selling overpriced products online], *Panorama*, November 9, 2015, http://bit.ly/2dUQvRG.

120 "AN aprueba Proyecto de Reforma de la Ley de Telecomunicaciones," [National Assembly approves bill to reform the Telecommunications Law], *El Universal,* April 28, 2016, http://bit.ly/2dzDkFK.

121 "En los primeros 100 días la AN aprobó cinco leyes, negadas luego por Maduro y el TSJ," [National Assembly approved fi e laws in fi st 100 days, later rejected by Madoro and Supreme Court], *Efecto Cocuyo,* April 14, 2016, http://bit.ly/2dFadCE.

122 Cristina Marcano, "Un juicio para la historia" [A trial for history], *Letras Libres,* November 5, 2015, http://bit.ly/2d5esGj.

123 Priselen Martínez Haullier, "Así fue el análisis a los tuits de Leopoldo López" [This is how the analysis of tweets from Leopoldo Lopez went] *Panorama,* March 17, 2015, http://bit.ly/2dNOp4O.

124 Daniel Lozano, "Leopoldo López seguirá en prisión por emitir mensajes subliminales," [Leopoldo Lopez will remain in prison for sending subliminal messages] *El Mundo*, June 5, 2014, http://bit.ly/1NXqPy9.

125 Human Rights Watch, "The Shattered Case Against Leopoldo López," December 2, 2015, http://bit.ly/1PyIb78.

126 "Venezuela prosecutor who accused Lopez flees count y," *Reuters*, October 24, 2015, http://reut.rs/2e3d0V3.

127 Javier La Fuente, "Apagón informativo sobre el caso de Leopoldo López en Venezuela" [News blackout on the case of Leopoldo Lopez in Venezuela], *El País,* September 11, 2015, http://bit.ly/2d5suaY.

his blog, was arrested and questioned by security agents, and had his computer seized.[128] On April 26, Reinaldo Mozo, a reporter for the online outlet "Efecto Cocuyo" was arrested and briefly detained while covering street protests over food shortages in Vargas State.[129]

As the economic crisis deteriorated, arrests also occurred under new provisions of the Law of Fair Prices implemented in November 2015. Within the same month, according to the Vice President, 23 detentions took place, 15 of them for unscrupulous sales on social networks and speculation on the internet, which he called "electronic crimes."[130] Those arrested include Julio César Hernández Sánchez, who was arrested for reselling birth control pills,[131] Reinaldo Tatoli for selling tires,[132] and Omar Vicente Machado Evia for selling household appliances.[133]

Several other social media users were also arrested, including Carlos Alberto Rocha de las Salas, a Colombian who allegedly defamed and discredited the governor of Aragua state,[134] and Carlos Ferreira Rincón, who was accused of writing threatening tweets against President Maduro.[135]

Meanwhile, six out of nine individuals arrested in the fall of 2014 for their social media activities were released in April 2016.[136] Many of them had disseminated photographs and information, or simply joked, about the death of Robert Serra, a member of parliament in the ruling party, who was murdered in 2014. However, three of these users remained in detention:

- Victor Ugas was arrested on October 13, 2014, after publishing photos of the corpse of Robert Serra. He was charged with improper disclosure of data or personal information and digital espionage.[137]
- Leonel Sánchez Camero was detained on August 22, 2014, accused of promoting hatred, conspiring, defamation, and unlawful access to electronic channels. He remained detained at the headquarters of the Bolivarian Intelligence Service (SEBIN).[138]
- Another user called Skarlyn Duarte, from whom there is no further information except for

128 "Sebin detiene a periodista por informar sobre caso Tumeremo" [SEBIN detains journalist for reporting on Tumeremo case], *Espacio Público*, March 18, 2016, http://bit.ly/2diDFvw.

129 "Detienen a periodista de Efecto Cocuyo mientras cubría protesta por comida en Vargas" [Efecto Cocuyo journalist arrested while covering protest for food in Vargas], *Efecto Cocuyo*, April 26, 2016, http://bit.ly/2dOkedW.

130 "Detenidas 23 personas por vender con sobreprecio en Internet" [23 people arrested for selling overpriced items via Internet] *La Patilla*, November 9, 2015, http://bit.ly/2dZk0iy.

131 "Detienen a hombre por revender anticonceptivos en Internet" [Man detained for reselling contraception on internet], *Panorama,* November 10, 2016, http://bit.ly/2dHuKoh.

132 "Preso por vender cauchos con sobreprecio por internet" [Arrested for selling tires via Internet], *Entorno Inteligente,* November 2, 2016, http://bit.ly/2dTw1ab.

133 "Imputan a hombre que revendía productos de Mi Casa Bien Equipada por internet" [Man accused of selling regulated products online], *Entorno Inteligente,* November 5, 2015, http://bit.ly/2e7ex9W.

134 "Detienen a un hombre por difamar y desprestigiar a políticos del oficialism " [Man detained for defaming and discrediting ruling party politicians], *La Patilla,* June 22, 2015, http://bit.ly/2d5TtS1.

135 "Detienen a twittero tras amenazar a Maduro" [Twitter user detained after threatening Maduro], *El Nacional*, January 28, 2015, http://bit.ly/1VunxUs.

136 Personal consultation via email with lawyers of Foro Penal on April 14, 2016. Those arrested and subsequently released include: Lessi Marcano, Ginette Hernández, Daniely Benítez, Inés Margarita González Árraga, Abraham David Muñoz Marchán, María Magaly Contreras. See: Julett Pineda, "Tres tuiteros han sido liberados en las últimas dos semanas," [Three Twitter users released in the past two weeks], *Efecto Cocuyo,* November 27, 2015, http://bit.ly/2dOBwup.

137 Foro Penal, "Victor Andrés Ugas," accessed October 6, 2016, http://bit.ly/2duXItL.

138 Foro Penal, "Leonel Sánchez Camero," accessed October 6, 2016, http://bit.ly/2dOwWfE; See also: "Trasladan del Helicoide al Ortopédico infantil a tuitero preso" [Detained Twitter user transferred from Helicoide to Children's Orthopaedics clinic], *Efecto Cocuyo*, January 15, 2016, http://bit.ly/2dUT5Vm.

that provided by Foro Penal, was arrested on August 26, 2014 and remained detained on charges related to Twitter messages against government officials [139]

Appearing before the Inter-American Commission on Human Rights (IACHR) at a hearing on the situation of freedom of expression in Venezuela in October 2015, a group of NGOs reported that from 2002 to 2015, 36 people had faced legal action. Of these, 29 were for defamation and libel and more than half corresponded to the group of media executives denounced for defamation in April 2015 by then President of the National Assembly, Diosdado Cabello.[140] Cabello accused these media executives of reproducing information from the Spanish daily *ABC*, which mentions Cabello's alleged links to drug trafficking [141] The accused included Alberto Federico Ravell, the founder of digital outlet *La Patilla*. The digital outlet was served with a multi-million lawsuit for "moral damages" in August 2015.[142]

In October 2015, the Venezuelan Central Bank filed a lawsuit in the Uni ed States against three Venezuelan citizens whom the government believes to be responsible for the website Dólar Today. The suspected website admins were accused of using cyber terrorism tools to cause economic havoc in the country.[143] In a press release, the Venezuelan Central Bank claimed that Dólar Today distorts the exchange rate with the aim of deteriorating the acquisition power of Venezuelans.[144] President Maduro later insisted in February 2016 that the country's economic downturn was caused by "that webpage directed from the United States." [145]

Surveillance, Privacy, and Anonymity

Government surveillance and counterintelligence activities have increased since 2013, when the government released its 2013-2019 Plan for the Homeland, which emphasized the strengthening of national defense among its priorities.[146] Although it is difficult o confi m and determine the full scale of surveillance, activists have denounced targeted tracking and spying by the government. The lack of independent oversight has raised concerns about the ease with which systematic content fil ering and surveillance could be implemented.

139 Foro Penal, "Skarlyn Duarte," accessed October 6, 2016, http://bit.ly/2dUSjLB.

140 Silvia Higuera, "Denuncian múltiples ataques a la libertad de expresión en Venezuela ante Comisión de Derechos Humanos de la OEA," [Multiple attacks on freedom of expression in Venezuela Reported to Commission on Human Rights of the OAS] *Knight Center (blog),* October 20, 2015, http://bit.ly/1MTu6Pf.

141 Ramón Castro, "CIDH acordó medidas cautelares de protección a Petkoff, Otero y Ravell" [IACHR agreed precautionary measures to protect Petkoff, Otero and Ravell], November 9, 2015, http://bit.ly/1kI8zOg.

142 "La demanda mil millonaria del ciudadano Diosdado Cabello en contra de LaPatilla" [The billion dollar lawsuit by Diosdado Cabello against La Patilla], *La Patilla*, August 14, 2015, http://bit.ly/1JYpSoi; "Tribunal admite demanda contra tres medios de comunicación" [Court accepts lawsuit against three media], *El Universal*, August 13, 2015 http://bit.ly/2dIUOhk; "Tribunal ordena buscar, por solicitud de Cabello, a directivos de La Patilla, El Nacional y Tal Cual con el SIPOL" [Court orders SIPOL, upon request of Cabello, to search for the executives of La Patilla, El Nacional and Tal Cual], *La Patilla,* October 6, 2015, http://bit.ly/2dISBCx; "Comisión del Cicpc acudió a LaPatilla en busca de Alberto Federico Ravell" [Cicpc Commission went to La Patilla looking for Alberto Federico Ravell] *La Patilla*, October 8, 2015, http://bit.ly/2e75kOU.

143 Airam Fernandez, "Banco Central de Venezuela demanda a dueños de Dolar Today en EEUU por "conspiradores"" [Central Bank of Venezuela demand owners of Dolartoday in the US for "conspirators], *Efecto Cocuyo,* October 23, 2015, http://bit.ly/2dHkV9y; See also: Hannah Dreier, "Venezuela sues black market currency tracker for terrorism," *Associated Press,* October 23, 2015, http://apne.ws/2e67iBA.

144 "Precio en web de DolarToday "es falso"" [Price on DolarToday website is false], *Últimas Noticias*, October 24, 2015, http://bit.ly/2dSsr1r.

145 Margioni Bermúdez, "Maduro: "A Dolar Today los desmontamos o ellos desmontan al país" [Maduro: We dismantle Dolartoday or they dismantle the country], *Panorama*, February 17, 2016. http://bit.ly/2dHjIyW.

146 Plan de la Patria: Segundo plan socialista de desarrollo económico y social de la nación, 2013-2019 [Plan for the Homeland, 2013-2019], September 28, 2013, http://bit.ly/1ii5WKR.

A decree issued in October 2013 created the Strategic Center for the Security and Protection of the Fatherland (CESPPA), a special body charged with monitoring and tracking of social media and other online information.[147] Agents of the National Guard have also reportedly been trained by the Ministry of Information and Communication in the management of social networks for the "implementation of early warnings" that can "keep the Venezuelan people truthfully informed, and detect any threat in order to defend our national sovereignty."[148]

Complaints about the government's purchase and use of surveillance software have progressively surfaced. Leaked emails posted on Wikileaks in July 2015 revealed that the Ministry of Interior, Justice and Peace had shown interest in buying spyware from the company Hacking Team,[149] a transaction that was allegedly never completed.[150] However, Citizen Lab reported that it had detected the existence of a server of the spyware FinFisher in Lithuania, which would serve as an "intermediary" for another master server in Venezuela.[151]

In early April 2016, Venezuelan journalist Casto Ocando, based in Miami, published a report on the existence of an organization, under the direction of President Maduro, dedicated to electronic spying on opponents of his regime. The journalist asserted that the operations are coordinated by civilian and military personnel grouped within CESPPA, using "a combination of advanced electronic equipment and malware designed by Chinese and Russian specialists."[152]

On the sidelines, a group of anonymous users operating under the name of "patriotas cooperantes" (cooperating patriots) has also emerged in the country, allegedly responsible for providing illegally collected private information from citizens and activists to authorities. Evidence from these anonymous informers has in turn been used in at least 20 court cases since 2014, according to Reuters.[153] Public attacks against dissenting voices have also used supposed accusations made by "cooperating patriots," notably during the televised show hosted by the former President of the National Assembly, Diosdado Cabello. In May 2015, advocacy groups requested that the Attorney General investigate Diosdado Cabello, after he released information on his television show that seemingly could have only been obtained through the interception of electronic communications.[154]

There are no known government restrictions on encryption technologies or other digital privacy

147 IPYS Venezuela, "Reglamento del CESPPA contiene disposiciones contrarias a la libertad de expresión," [CESPPA Regulation contains provisions contrary to freedom of expression], February 25, 2014, http://bit.ly/1exVnBa ; See also Danny O'Brien, "Venezuela's Internet Crackdown Escalates into Regional Blackout," Deeplinks Blog, Electronic Frontier Foundation, February 20, 2014, http://bit.ly/1ffcDB4.

148 IPYS Venezuela, "MINCI instruyó a agentes de seguridad del estado en la supervisión de redes sociales [MINCI instructed state security agents in monitoring social networks], April 23, 2015, http://bit.ly/2dvBK9I.

149 Jeanfreddy Gutiérrez, "Funcionario del Ministerio de Interior y Justicia solicitó oferta a fabricante de software espía" [Ministry of Interior official equested offer to spyware manufacturer], *El Cambur,* July 13, 2015, http://bit.ly/2dJDiNM.

150 Katherine Pennacchio, "Hacking Team casi corona en Venezuela" [Hacking Team almost "crowns" in Venezuela], Armando. Info, July 18, 2015, http://bit.ly/2dZnfGQ.

151 "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation," CitizenLab, October 15, 2015, http://bit.ly/1GfcZ9n; See also: "Gobierno venezolano sospechoso de usar el software espía FinFisher" [Venezuelan government suspected of using the FinFisher spyware], *La Patilla*, November 7, 2015, http://bit.ly/2dOopq6.

152 Casto Ocando, "Una invasión a la privacidad sin precedentes" [An unprecedented invasion of privacy], *Vértice*, April 3, 2016, http://bit.ly/2dueDXY.

153 Diego Oré, "Venezuela's state informers: patriots or snitches?" *Reuters,* January 29, 2015, http://tmsnrt.rs/2e7gZ08; See also: Jesus Yajure, "Se buscan sapos: así operan los "patriotas cooperantes" [Looking for "frogs": this is how the "cooperating patriots" operate], *Runrunes*, July 24, 2015, http://bit.ly/1MOt4RS.

154 Provea, "Provea y Espacio Público denunciaron ante el MP la intervención ilegal de sus comunicaciones por parte de Diosdado Cabello" [Provea and Espacio Público denounced illegal intervention of their communications by Diosdado Cabello], May 27, 2015, http://bit.ly/1h3ybmE.

tools. Furthermore, Venezuelan laws, such as the Law against Cybercrime and the Law to Protect Communication Privacy, guarantee the privacy of communications.[155] In practice, however, authorities have failed to apply these laws evenly in cases where activists have sued for protection under the law.[156]

The constitution expressly prohibits anonymity. In order to buy a cellphone, a SIM card, or a USB modem to access mobile broadband, Venezuelan law requires customers to register using their personal ID number, address, signature, and fingerprints [157] The Law against Kidnapping and Extortion also contains a provision that requires telecommunications companies and banking entities to provide the Public Ministry with information it requests.[158]

In October 2015, the Superintendence of Banking Sector Institutions (SUDEBAN) issued regulations requiring banks to deliver the IP addresses from which customers make electronic transactions between financial institutions, as ell as other private data. While the measure claims to track trading related to foreign exchange,[159] the collection of significant amounts f personal data raised concerns about the lack of privacy safeguards and the risk of political interference. IP identification and other data had already been used to pursue dissenting opinions online: a leaked report revealed how, in the midst of protests in 2014, the telecoms regulator (CONATEL) helped to track and locate critical Twitter users who were later detained by the National Bolivarian Intelligence Service (Sebin) (see Prosecutions and Detentions).[160]

During the 2015 election campaign, the ruling party also developed a system designed to monitor citizens, drawing on the participation of its supporters and its relationship to the Voter Information System, a structure that works within voting precincts based on the capture of voter's finge tips. By knowing this data, the party was in theory able to identify the supporters previously registered in their network who did not vote.[161] Activists also worried that the government could use data collected through the Biometric System for Food Security, [162] as well as personal data collected through social welfare programs, to exert pressure on voters.[163] In the midst of demands for a referendum to recall President Maduro, senior officials th eatened to retaliate against petition signers, warning that "there is no private data."[164]

155 Ley contra los Delitos Informáticos [Law Against Cybercrime], accessed October 20, 2016, http://bit.ly/2daEjI9; Ley Sobre Protección a la Privacidad de las Comunicaciones [Law on Protection of Communications Privacy], December 16, 1991, http://bit.ly/2d5EqJV.

156 Internet Society Venezuela, "Libro blanco sobre libertad en Internet" [The white paper on internet freedom], June 2014, http://bit.ly/1O4ZL1m; see also: EsLaRed, "Venezuela," in *Global Information Society Watch 2014: Communication surveillance in the digital age*, APC and HIVOS, 2014, http://bit.ly/1sjkimX.

157 Gaceta Oficial, No. 38.157, P ovidencia Administrativa Contentiva de las normas Relativas al Requerimiento de Información en el Servicio de Telefonía Móvil, [Administrative ruling on norms relating to information requirements for mobile services], April 1, 2005, http://bit.ly/1MBmTBx.

158 Asamblea Nacional de Venezuela, Ley contra el secuestro y la extorsión [Law against kidnapping and extortion], June 5, 2009, http://bit.ly/1RbJINP.

159 "Gobierno exige a los bancos revelar hasta el alma de sus clientes" [Government requires banks to disclose the soul of its customers], *El Estímulo*, November 5, 2015, http://bit.ly/2ed0FyA.

160 Alberto Yajure, "Conatel elaboró informes para el @SEBIN_OFICIAL sobre tuiteros detenidos" [Conatel reported Twitter users to Sebin], *Runrunes,* July 3, 2005, http://bit.ly/1GXrDwA.

161 Carlos Crespo, "PSUV enfrentará descontento con su maquinaria electoral" [PSUV will face discontent with electoral machinery], *Crónica Uno*, November 25, 2015, http://bit.ly/2dujx7h.

162 Marianne Díaz, "Tu huella digital por un kilo de harina: biométrica y privacidad en Venezuela" [Your fingerprint for a kilo of flou : biometrics and privacy in Venezuela], Digital Rights, December 16, 2015, http://bit.ly/1PL5Sa1.

163 Venezuela does not have a Data Protection Act and there is not clarity regarding the use that could give the government to the increasing and more accurate information obtained from citizens through the use of biometric devices.

164 "Si Jorge Rodríguez mostró planillas con fi mas fue porque se las robó" [If Jorge Rodriguez showed forms with signatures is it is because he stole them], *El periódico venezolano*, May 13, 2016, http://bit.ly/2e7leZG.

Intimidation and Violence

Reporters covering political events, protests, or queues to buy food or medicine continued to suffer arbitrary arrests, confiscation f cellphones, and the deletion of images by security forces.[165] Physical attacks against journalists and citizens by progovernment groups have also been reported, in some instances under the watch of security agents.[166] In May 2016, photojournalist Harold Escalona of the digital outlet *El Estímulo* was attacked by a group of government militants after photographing members of the Bolivarian National Police evicting the deputies who protested at the headquarters of the Electoral Council.[167] Also in May, the reporter of *El Pitazo*, Maria Virginia Velázquez, was attacked by government supporters while covering the visit of the leader of the political party Vente Venezuela, Maria Corina Machado, at the University Hospital of Mérida city.[168]

Harassment and intimidation of journalists critical of the government remained prolific on social ne - works, with many reporting insults and threats via Twitter after covering politically sensitive events.[169] In early 2016, state and progovernment media launched a number of smear campaigns against dig- ital media journalists critical of the government. CONATEL's director, William Castillo, often posted negative messages against critical journalists and human rights defenders through his personal ac- count on Twitter.[170] The website of the former president of the National Assembly, Diosdado Cabello, was also used to discredit and attack both new digital media and human rights defenders.[171]

Meanwhile, journalists who participated in the Panama Papers project received insults and attacks online, and progovernment portals also discredited them.[172]

165 Edison Lanza, Special Rapporteur for Freedom of Expression, Annual Report of the Inter-American Commission on Human Rights, IACHR-OEA 2015. For examples of cases, see: Ipys Venezuela, "Militares despojaron a corresponsal de IPYS Venezuela de su celular a las afueras de centro electoral y borraron su material" [Military agent took cellphone from IPYS Venezuela correspondent just outside electoral center and erased its material], December 4, 2015, http://bit.ly/2dSA1pT; "Detienen a periodista en Yaracuy mientras hacía cobertura en una cola" [Journalist detained in Yaracuy while reporting on a queue], *Espacio Público*, September 11, 2015, http://bit.ly/2e5tQUH; Ipys Venezuela, "Caracas: Funcionarios de inteligencia obligaron a equipo reporteril a borrar imágenes en cobertura" [Caracas: Intelligence officials fo ced journalists to delete images], July 13, 2015, http://bit.ly/2dkm1Yd.

166 "Nuevo informe detalla interminables violaciones a la libertad de expresión en Venezuela" [New report details endless violations of freedom of expression in Venezuela], *La Patilla,* July 6, 2015, http://bit.ly/2dHrOYn.

167 "Golpean y roban a fotoperiodista en el CNE" [Photojournalist beaten and robbed at the CNE], *El Estímulo*, April 21, 2016, http://bit.ly/2dZtb2z.

168 "Oficialistas ag eden a reporteras en Hospital Universitario de Mérida" [Government supporters harass reporters at University Hospital of Merida], *Espacio Público*, May 4, 2016, http://bit.ly/2epkG4a.

169 Ipys Venezuela, "Amedrentaron a periodista Thabata Molina a través de Twitter" [Journalist Molina Thabata intimidated via Twitter], July 8, 2015, http://bit.ly/2eHdzl7; Ipys Venezuela, "Periodista Clavel Rangel fue víctima de ciberamenazas" [Journalist Clavel Rangel was victim of cyber threats], September 21, 2015, http://bit.ly/2dLJCnT; Ipys Venezuela, "Periodista recibió mensaje intimidatorio a través de Twitter" [Journalist received threatening message via Twitter], September 24, 2015 http://bit.ly/2erwEtZ; Ipys Venezuela, "Amenazan a periodista a través de Twitter" [Journalist threatened via Twitter], October 22, 2015, http://bit.ly/2dRmaCc; Lorena Bornacelly, "Corresponsal de El Pitazo en Táchira denunció ante el Ministerio Público acoso por Twitter" [El Pitazo correspondent in Tachira complained about harassment via Twitter before the Public Ministry], *El Pitazo*, April 4, 2016, http://bit.ly/2ed5g3U.

170 IPYS Venezuela, "Director de CONATEL emitió mensajes agraviantes contra periodistas y defensores de DDHH" [Director of CONATEL sends offensive messages against journalists and human rights defenders], September 17, 2015, http://bit.ly/2e79Snc.

171 "El brazo mediático de las bandas armadas" [The media arm of the armed gangs], *Con el mazo dando*, May 4, 2016, http://bit.ly/1NWF49h.

172 "Periodistas venezolanos tras #PanamaPapers sufren ataques y despidos por sus investigaciones" [Venezuelan journalists suffer attacks and dismissals for their research after #PanamaPapers], *Efecto Cocuyo,* April 12, 2016, http://bit.ly/2a9WyNB.

Technical Attacks

Hacking and falsification of social media profiles belonging to journalists, writers and TV figures remains common.[173] After the December 2015 parliamentary elections, some messages urging the privatization of CANTV were disseminated using a Twitter account attributed to the former president of CANTV, Gustavo Roosen (@roosengustavo).[174] On December 13, IESA, the institution headed by Roosen clarified that the account did not belong to Roosen, and that his actual account (@gustavoroosen) had been inactive since 2011.[175] Nevertheless, in response to these messages, on December 15, the government promoted protests and demonstrations against the alleged plan to privatize telecommunications.[176] According to Professor Rosa Amelia González and other digital media analysts, this was a deliberate lie used to justify a protest on false assumptions.[177] Unidentified persons also hacked CANTV's webpage after the elections.[178]

Established and new media outlets that criticize the government have also reported targeted cyberattacks. On April 3, when the stories related to the Panama Papers showed evidence of corruption and money laundering by officials and people close to the regime were published, the site *Armando.Info* was hacked and went offline for approximately 12 hours.[179]

A study by Citizen Lab also reported evidence of an extensive campaign of contamination using malware, phishing and active disinformation.[180]

173 "Hackean cuenta en Twitter de Nelson Bocaranda" [Twitter account of Nelson Bocaranda is hacked], *RunRunes,* May 6, 2016, http://bit.ly/2eryBXs; See also: http://bit.ly/2e1aBH2.

174 Gustavo Roosen, Twitter post, December 11, 2015, 10:46am, http://bit.ly/2e2W9QB.

175 IESA, Letter to CONATEL, December 14, 2015, http://bit.ly/2diViIe.

176 Jesús Rivas, "Trabajadores de Cantv rechazan mensajes de Roosen" [Cantv's employees reject Roosen's messages], *Diario de Los Andes*, December 16, 2015, http://bit.ly/2dW3W1B.

177 Rosa Amelia González, "Fábrica de mentiras" [Factory of lies], IESA, December 27, 2015, http://bit.ly/2erCGed.

178 Juan Carlos Figueroa, Twitter post, December 30, 2015, 6:38pm, http://bit.ly/2dkpOou.

179 "El portal armando.info sufre ataque DoS justo cuando publicaba los #PanamaPapers" [The website armando.info suffers DDoS attack just after publishing the #PanamaPapers], *La Patilla*, April 3, 2016, http://bit.ly/2dvYtxr.

180 Nathaniel Janowitz, "The Hackers Targeting Dissidents throughout Latin America May Be State Sponsored," *Vice,* December 17, 2015, http://bit.ly/2dcfBXP.

Freedom House

Vietnam

	2015	2016
Internet Freedom Status	Not Free	Not Free
Obstacles to Access (0-25)	13	14
Limits on Content (0-35)	29	28
Violations of User Rights (0-40)	34	34
TOTAL* (0-100)	**76**	**76**

* 0=most free, 100=least free

Population:	**91.7 million**
Internet Penetration 2015 (ITU):	**53 percent**
Social Media/ICT Apps Blocked:	**Yes**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- Prosecutions of ICT users fell during Trans-Pacifi Partnership negotiations, but three bloggers were sentenced the month after the agreement was signed (see **Prosecutions and Detentions for Online Activities**).
- Facebook and Instagram were sporadically blocked in May 2016 to curb environmental protests organized online (see **Blocking and Filtering**).
- Authorities administered fine and disciplinary warnings for critical content online (see **Media, Diversity, and Content Manipulation**).
- A cybersecurity law passed in November 2015 could undermine privacy and encryption (see **Surveillance, Privacy, and Anonymity**).

Introduction

The internet freedom environment saw no overall change in 2016. In January, the 12th Vietnamese Communist Party (VCP) congress took place in an atmosphere that appeared unsettled in contrast to previous, more carefully choreographed congresses. Rumours and manipulated information spread on social media for weeks in advance, leading observers to anticipate a power reshuffle In the end, 71-year-old Nguyen Phu Trong, a leader of the party's old guard, was re-elected as party chief and leader of the country.[1]

The Trans-Pacifi Partnership (TPP), a trade agreement among twelve Pacifi Rim countries, including Vietnam, went through intensive negotiations during the coverage period of this report, and was finall signed in February. Vietnam, which has successfully negotiated trade deals with the European Union and South Korea in the past, expects that the deal will open access to developed markets for its goods and boost ties with the United States to balance its relationship with China.

The government may have tried to keep the number of political arrests and trials to a minimum while it faced heightened scrutiny during TPP negotiations. Arrests for online activity declined in comparison to past years, and high profil bloggers like Nguyen Quang Lap and Ta Phong Tan were released from prison, reducing the number of jailed internet users from 29 in December 2014 to 15 a year later.[2] Yet repression of critical netizens remained severe. In March 2016, the month after the TPP agreement was finalized three bloggers who had been detained without trial since 2014 were sentenced to between three and fi e years in prison each.

Obstacles to Access

Although internet is widely available in cities, access can be sporadic in rural areas. The quality of access is improving, yet remains poor by global standards. Investment is needed to improve access speeds, and the infrastructure is vulnerable to physical damage. The telecom market is dominated by a few players, most of them state or military-owned, lacking fairness and autonomy by international standards.

Availability and Ease of Access

Internet penetration grew from 48 to 53 percent in 2015, according to an International Telecommunication Union estimate.[3]

Despite incremental improvement, the quality of access remains poor. Internet speeds were among the lowest in the Asia Pacific ranking 17th in the region, according to one study, and 102nd in the world.[4] Akamai reported average connection speeds of 5 Mbps in early 2016.[5]

1 Nguyen Manh Hung, "A Post-Mortem of Vietnam's Communist Party Congress" Cogitasia, February 2, 2016 http://bit.ly/21z0peU.

2 "Đình chỉ điều tra đối với nhà văn Nguyễn Quang Lập" <Stop investigation against writer Nguyen Quang Lap>, Nguoi Do Thi, October 20 2015, http://bit.ly/1XXoqqA."Well-known blogger freed but 15 other citizen-journalists still held", Reporters Without Borders, September 22 2015, http://bit.ly/1OOGmkD

3 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1cblxxY.

4 "Vietnam's Internet speed ranks 102nd in the world", VietnamNet, December 12, 2015, http://bit.ly/1QjnSsn

5 https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-state-of-the-internet-report-q1-2016.pdf?mkt_tok=eyJpIjoiTldJek0yVTNPVEV6T0RZeiIsInQiOiJiOHFGMVdoMExqb1wvRDNMbW1HdUFxOTRpRFN5NmxDUGxUTERuM2puK0xrWk5kbUNoXC9yTkJ1R0hEUWE1QUZnU0hzMW5FbkRscGJEU2FHdnh3bVwvYjdnK3VYMGJTZkc3bk9ZcmRLd0J1Y3lVYz0ifQ%3D%3D

While there has been a surge in the number of subscribers, fi ed broadband remains a relatively small market segment. Fixed broadband services have been largely based on DSL technology; more recently, faster fibe -based broadband services are starting to replace it, with FttH subscriptions overtaking DSL subscriptions for the fi st time in November 2015.[6]

Mobile broadband has been a more significan factor in increasing access to faster internet service. Mobile broadband penetration was more than four times that of fi ed broadband by 2015 (34 percent compared to 8 percent). [7] Mobile penetration was reported at 130 percent in 2015.[8] By March 2015, 52 percent of Vietnamese mobile subscribers used smartphones. [9]

The 3G network operating since 2009 is growing fast. As of March 2015, Vietnam had 29.3 million 3G users, up from 15.7 million in 2012.[10] In 2015 the Ministry of Information and Communication was preparing for the introduction of the faster 4G network. The regulator authorized operators to launch trial 4G LTE networks, though its use has not been commercialized, and spectrum has yet to be licensed.[11]

Restrictions on Connectivity

While several companies have licenses to build infrastructure, the state-owned Viet Nam Post and Telecommunications Corporation (VNPT) and military-owned Viettel dominate the country's telecommunications sector.

Three out of four providers servicing Internet Exchange Points (IXP), which allocate bandwidth to service providers, are state- or military-owned (VNPT, Viettel, and SPT; the fourth, FPT, is private).[12] Although this suggests a concerning degree of state influenc over the internet architecture, authorities in Vietnam did not employ noticeable throttling or restrict access to the internet for political reasons during the coverage period of this report. Research published in 2014 indicated that mobile operators may throttle over-the-top communications applications which represent a threat to their own, paid services,[13] though this is difficul to confi m, and the services were accessible and popular in 2015 and 2016.

In early 2015, the Asia-America Gateway (AAG) submarine cable, one of several which carry international traffic was damaged twice, significantl impairing the speed and quality of access.[14] No similar incident was reported during the coverage period of this report.

6 https://www.vietnambreakingnews.com/2016/10/telecom-agency-still-room-for-new-ftth-service-providers/

7 "Vietnam - Telecoms Infrastructure, Operators, Regulations - Statistics and Analyses", Buddle, August 2015, http://bit.ly/1Lt7kPq

8 International Telecommunication Union, "Mobile-cellular subscriptions," http://bit.ly/1cblxxY.

9 Ibid

10 Ibid

11 "Tại sao iPhone, iPad ở Việt Nam chưa dùng được 4G?" <Why 4G still has not been used on iPhone, iPad in Vietnam", Thanh Nien Online, December 20, 2015, http://bit.ly/1QjohL.

12 MIC http://bit.ly/1oVnHuy

13 Open Technology Fund, Radio Free Asia, "Internet Access and Openness: Vietnam 2013," June 2014, https://www.opentech.fund/sites/default/files/attachments/otf_vietnam_ eport_final.pd .

14 "Tại sao cáp quang biển AAG tại Việt Nam hay bị đứt?" <Why submarine cable AAG in Vietnam was often damaged>, Thanh Nien Online, June 07, 2015, http://bit.ly/1TNUhcK.

ICT Market

The three biggest internet service providers (ISPs) are VNPT, which controls 51 percent of the market; Viettel (40 percent); and the private FPT (6 percent).[15] Though any fi m is allowed to operate an ISP, informal barriers prevent new companies without political ties or economic clout from disrupting the market. In the mobile sector, Viettel commands 40 percent of mobile subscriptions; MobiFone and Vinaphone rank second and third with 21 percent and 20 percent, respectively.[16] Smaller players which lack infrastructure to provide quality service and coverage, like Vietnamobile and Gmobile, struggle to compete.[17]

Regulatory Bodies

The Vietnam Internet Network Information Center (VNNIC), an affilia e of the Ministry of Information and Communications, is responsible for managing, allocating, supervising, and promoting the use of internet domain names, IP addresses, and autonomous system numbers (ASN). Three additional ministries—information and culture (MIC), public security (MPS), and culture, sport, and tourism (MCST)—manage the provision and usage of internet services. On paper, the MCST regulates sexually explicit and violent content, while the MPS oversees political censorship. In practice, however, guidelines are issued by the Vietnamese Communist Party (VCP) in a largely non-transparent manner.

Limits on Content

Political content on a range of sensitive topics is restricted online, especially in Vietnamese. Blogging and social media platforms are widely available, though Facebook was apparently briefly blocked in May 2016 in response to protests. Decree 174 has been widely used to levy harsh fines for government criticism online since it was introduced in 2015. Additionally, Circular 09, issued in October 2014, requires website owners to immediately take down content at the request of authorities, resulting in increased self-censorship. In 2013, the government officially acknowledged using paid commentators, who have since grown in number and continue to manipulate online content.

Blocking and Filtering

Access to Facebook and Instagram appears to have been interrupted for a couple of days after hundreds of people protested against an environmental disaster in Hanoi and Ho Chi Minh City in May 2016. Demonstrators criticized a Taiwanese steel plant they held responsible for millions of fis washing up dead along the central coast, and the government for failing to respond to the crisis. The mainstream media failed to cover the rallies, adding to Facebook's importance as a means of sharing information and organizing public events (see Digital Activism). Operators of at least three tools used to circumvent blocking reported a dramatic spike in the number of their Vietnamese users on May 15, coinciding with reports that social media platforms were inaccessible and indicat-

15 Viettel dẫn đầu về di động, VNPT chiếm lĩnh thị phần Internet băng rộng," [Viettel leads in mobile, VNPT gains in broadband market] ICT News, October 27, 2014 http://bit.ly/1YYnsfA.

16 "VNPT, Viettel rule telecoms market", VietnamNews, September 2013, http://bit.ly/1oLDStB.

17 "Viettel dominates Vietnam's mobile market with $2bn profi in 2015", Tuoi Tre, December 30, 2015, http://bit.ly/1ID8qHk.

ing that the platforms had been blocked.[18] Some mobile users also reported that they were unable to send SMS messages about the rallies. Facebook has been blocked for long periods in the past, but this was one example of temporary, more targeted blocking that suggests censorship is becoming more agile. At the end of the coverage period, both platforms were available with no reports of interruption.

With fewer resources devoted to online content control than in China, the Vietnamese authorities have nevertheless established an effective content fil ering system. Censorship is implemented by ISPs rather than at the backbone or international gateway level. Specifi URLs are generally identifie for censorship and placed on blacklists. Censorship targets high-profil blogs or websites with many followers, as well as content considered threatening to Communist Party rule, including political dissent, human rights and democracy, as well as websites criticizing the government's reaction to border and sea disputes with China.

Content promoting organized religion such as Buddhism, Roman Catholicism, and the Cao Dai group, which the state considers a potential threat, is blocked to a lesser but still significan degree. Websites critical of the government are generally inaccessible, whether they are hosted overseas, such as Human Rights Watch, Talawas, Dan Luan, U.S.-funded Radio Free Asia's Vietnamese-language site, and Dan Chim Viet, or domestically, like Dan Lam Bao, Dien Dan Xa Hoi Dan Su, or Bauxite Vietnam.

ISPs use different techniques to inform customers of their compliance with blocking orders. While some notify users when an inaccessible site has been deliberately blocked, others post an apparently benign error message.

Content Removal

The party's Department for Culture and Ideology and the Ministry of Information and Culture (MIC) regularly instruct online outlets to remove content they perceive as problematic, through nontransparent, often verbal orders. Their instructions cover social as well as political content. On November 25, 2015, MIC official ordered local media production company Monday Morning Ltd. Co. to stop producing episodes of the YouTube celebrity gossip series "Bitches in Town," for using offensive language and causing public outrage.[19] After the producers sent an explanation to the MIC, the show restarted.

Other entities with financia and political influenc may exert control over online content or discourage free expression. In February 2016, online reports of inadequate animal welfare at a safari on Phu Quoc island in southern Vietnam, led to a Facebook campaign questioning the importation and treatment of wild animals. The Vinpearl safari is operated by Vingroup, one of the country's biggest conglomerates. Shortly afterward, Facebook users who had previously discussed the issue temporarily deactivated their accounts, and a Facebook page administrator posted that they had to stop reporting on the case "for security reasons," according to the BBC Vietnamese service, leading

18 Sarah Perez "Facebook blocked in Vietnam over the weekend due to citizen protests" , TechCrunch, May 17, 2016 http://tcrn.ch/28KKrG2.

19 "'Những kẻ lắm lời' bị yêu cầu tạm ngừng vì xúc phạm người khác" < "Bitches in Town" was required to stop for offending others>, Tuoi Tre, November 25, 2015 http://bit.ly/1MhXdgL;

observers to believe that they feared reprisals from Vingroup or its supporters.[20] Vingroup denied reports that thousands of animals had died at the park and workers had quit in protest.[21]

Intermediary liability has long been implied in Vietnam, but was formalized in 2013 with Decree 72 on the Management, Provision, Use of Internet Services and Internet Content Online. It requires intermediaries—including those based overseas—to regulate third-party contributors in cooperation with the state, and to "eliminate or prevent information" prohibited under Article 5. It holds cybercafe owners responsible if their customers are caught surfin "bad" websites. This process was articulated in Circular 09/2014/TT-BTTTT, issued in October 2014, which requires website owners to eliminate "incorrect" content "within three hours" of its detection or receipt of a request from a competent authority in the form of email, text message, or phone call. The circular also tightened procedures for registering and licensing new social media sites. Among other requirements, the person responsible for the platform should have a university or higher degree. It also requires Vietnamese companies who operate general websites and social networks, including blogging platforms, to locate a server system in Vietnam and to store posted information for 90 days and certain metadata for up to two years.[22] It is not clear how much service providers removed content for fear of possible reprisals before the decree was introduced, so its immediate impact was not possible to gauge. Further, it did not outline penalties for non-compliance or enforcement measures.

Media, Diversity, and Content Manipulation

Internet content producers face a range of pressures that affect the quality of online information. All content needs to pass through in-house censorship before publication. In weekly meetings, guidelines handed out by a Party Committee to editors dictate areas and themes to report on or suppress, as well as the allowed depth of coverage. Editors and journalists also risk post-publication sanctions including imprisonment, fines disciplinary warnings, and job loss (see Intimidation and Violence).

Decree 174, effective since January 2014, introduced administrative fine of up to VND 100 million (US$4,700) for anyone who "criticizes the government, the Party or national heroes" or "spreads propaganda and reactionary ideology against the state" on social media. These fine can be applied for offenses not serious enough to merit criminal prosecution. The decree outlined additional fine for violations related to online commerce.

In 2015, the Ministry of Information and Communications reported imposing a total of over VND 1.5 billion ($70,000) in fine in 33 cases of administrative violations committed by press agencies, and VND 777 million ($38,000) in 18 cases involving violations of rules governing the provision and use of information on the internet.[23]

The practice of issuing administrative fine for online content was not without controversy. In November 2015, the local government in southwestern An Giang province fine a secondary school teacher VND 5 million ($220) for describing the provincial chairman as "arrogant" on Facebook.

20 "Safari Phú Quốc 'chưa nhập tê giác'" <Phu Quoc Safari "not imported rhinos yet">, BBC Vietnamese, February 27, 2016, http://bbc.in/1Tkwnaw
"Safari Phú Quốc 'nên minh bạch'" <Phu Quoc Safari 'should be transparent"> BBC Vietnamese February 26, 2016, http://bbc.in/1LL7koS.

21 "Reports of mass animal deaths at Vietnam safari zoo are false: authorities," Tuoi Tre News, February 24, 2016, http://tuoitrenews.vn/society/33384/reports-of-mass-animal-deaths-at-vietnam-safari-zoo-are-false-authorities.

22 Mong Palatino, "Corporate Critics Say Vietnam's New Tech Regulations Are Bad for Business," Global Voice Advocacy, November 3, 2014, http://bit.ly/1LtKLK4.

23 "VND1.5 billion fine imposed on press agencies in 2015", VietnamNet, December 31, 2015, http://bit.ly/1Tk2JCf.

Two other individuals were fine and received disciplinary warnings from the Party for "liking" and sharing the post. The incident became a national event, attracting dozens of media representatives to press conferences. Finally, the People's Committee of An Giang ordered its Department of Information and Communication to withdraw the fines [24] Following the case, Minister of Information and Communication Nguyen Bac Son reminded internet users that social media posts speaking ill of, or spreading false information about another person, would be subject to fine or prosecution.[25] The same month, Prime Minister Nguyen Tan Dung said the internet should be "clean and pure" and called on internet users in Vietnam to be more "responsible."[26]

These economic and social penalties, in addition to the risk of criminal prosecution, foster self-censorship. The unpredictable and nontransparent ways in which topics become prohibited make it difficul for users to know what might be off-limits, and bloggers and forum administrators routinely disable commenting functions to prevent controversial discussions.

The government has also taken steps to manipulate public opinion online. In 2013, Hanoi's head of propaganda Ho Quang Loi was the fi st officia who admitted that the communist regime employs a Chinese-style system of Internet moderators to control news and manipulate opinion. He revealed the city has a 900-strong team of "internet polemicists" or "public opinion shapers" who are tasked with spreading the party line. The "teams of experts" had set up some 18 websites and 400 online accounts to monitor and direct online discussions on everything from foreign policy to land rights, he said at the time. [27]

Organized campaigns involving political content appeared to be ongoing in 2015 and 2016. In one case Mai Khoi, a singer who ran for the National Assembly as an independent member, said her Facebook account had been disabled twice during her campaign. She suspected that individuals aligned with the security forces reported her account to Facebook for violating security guidelines in order to silence her.[28]

In the past, some blogs have published anonymous criticism of high-profil party members. These include Quan Lam Bao in 2013, or Chan Dung Quyen Luc ("Portrait of Power") in 2014. The identity of the authors has never been verified but their use of documents, audio, and video footage caused observers to speculate they were published by politicians using inside information to try to damage rivals. As such, critics say, they contribute little to the cause of freedom of expression.

Although government-run media continue to dominate, new domestic online outlets and social media sites are expanding the traditional media landscape. Young educated Vietnamese are increasingly turning to blogs, social media, and other online news sources over state TV and radio. [29] While some important alternative blogs have stopped operating following the prosecution of their owners, like Que Choa in 2014, new Facebook pages and other sites continue to emerge. In August 2015, independent broadcaster Conscience TV began producing YouTube videos on human rights issues in

24 "Chê Chủ tịch tỉnh 'kênh kiệu' trên Facebook: 'Chúng tôi xử phạt không sai" <Criticising Provincial Chairman "cocky" on Facebook: 'Our fin was not wrong," Thanh Nien online,. http://bit.ly/1MtVdwN.

25 "Social media abuse unlawful: Minister", VietnamNet, November 11, 2015, http://bit.ly/1XXJe1k.

26 "Vietnam promises 'favorable conditions' for Internet fi ms like Google, Facebook", Thanh Nien News, November 21, 2015, http://bit.ly/1SSD92V.

27 "Vietnam's propaganda agents battle bloggers online", Bangkok Post, January 19, 2013, http://bit.ly/1L21XH8

28 Matthew Clayfield "Vietnam's National Assembly elections plagued by biased vetting, intimidation," ABC News, May 20, 2016, http://www.abc.net.au/news/2016-05-20/vietnam-national-assembly-elections-plagued-by-bias/7430010.

29 Paul Rothman, "Media Use in Vietnam: Findings from BBG and GALLUP", Cima June 10, 2015, http://www.cima.ned.org/blog/media-use-vietnam/.

Vietnam. Police in Hanoi interrogated seven people for several hours about the content in September, and a dissident lawyer involved in the project was arrested in December (See Prosecutions and Detentions for Online Activities).[30]

In October 2015, the government opened an officia Facebook page to provide timely information about the government and the prime minister.[31] Other government agencies, such as the Ministry of Health or the Hanoi People's Committee have also started to reach out to citizens on Facebook, apparently signaling a shift away from the perception of such platforms as oppositional, towards more digital engagement for propaganda purposes.

Tools for circumventing censorship are well known among younger, technology-savvy internet users in Vietnam, and many can be found with a simple Google search.[32]

Digital Activism

Digital mobilization is local rather than national in scale, compared to some other countries in Asia. In May 2016, the mass deaths of fis in central coastal provinces sparked a wave of protest on Facebook, which led to street rallies in Hanoi and Ho Chi Minh City demanding more transparency from the government. The protest proved to be a challenge to the government on how to deal with crisis. Since mainstream media failed to cover the protests, Facebook became the platform for news, petitions, rallies, and other forms of social activism,[33] so much so that it was apparently blocked when the protests were at their peak (see Blocking and Filtering).

In March 2015, a Hanoi government plan to remove thousands of trees lining the city's thoroughfares spawned outrage on Facebook in a campaign which gathered 20,000 supporters in 24 hours, some of whom speculated that official were motivated by the chance of selling the valuable timber. Authorities reversed the plan later that month, after a rare protest where residents took to the streets following several online campaigns by different social groups.[34] The previous year, a plan to build a cable car near the UN-recognized world-heritage site Phong Nha-Ke Bang was also stalled by Facebook critics whose page amassed over 33,000 likes, and a petition of over 71,000 signatures.[35]

Violations of User Rights

The interrogation, imprisonment, and physical abuse of bloggers and online activists continued during the coverage period, with 15 behind bars, even though the government may have been trying to keep the number of political arrests and trials to a minimum in 2015 in the context of the Trans-Pacific Partnership negotiations. New revisions to the penal code passed in November 2015 included several harsh provisions penalizing legitimate online activity, though have yet to be implemented.

30 Bita Eghbali and Lakshna Mehta, "Vietnam Police Detain Six Over Web Videos," Global Journalist, September 29, 2015, http://globaljournalist.org/2015/09/vietnam-police-detain-six-over-web-videos/; Reporters Without Borders, "Citizen-journalist Nguyen Van Dai badly beaten," via IFEX, December 11, 2015, https://www.ifex.org/vietnam/2015/12/11/citizen_journalist_attacked/; Radio Free Asia, "Authorities in Vietnam Crack Down on New Independent Broadcast Service," September 25, 2015, http://www.rfa.org/english/news/vietnam/authorities-in-vietnam-crack-down-on-new-independent-broadcast-service-09252015152145.html.

31 "Vietnam sets up its own Facebook page to reach its young," AP, October 22, 2015, http://apne.ws/1Tkz6AH.

32 The Sec Dev Foundation, "Circum-what? Circumvention Widely Employed, Poorly Understood in Vietnam," February 1, 2016, https://secdev-foundation.org/circum-what-circumvention-widely-employed-poorly-understood-in-vietnam/.

33 "Rare rallies in Vietnam over mysterious mass fis deaths", Reuters May 1, 2016, http://reut.rs/23gFOI7.

34 "If a tree falls… online, will the Communist Party hear anything?" The Economist, April 18, 2015, http://econ.st/1DqEUy2.

35 "Son Doong Saved From Cable Car: No Development Until 2030", Caving News, February 13, 2015, http://bit.ly/1OLzzDY.

Legal Environment

The constitution, amended in 2013, affi ms the right to freedom of expression, but in practice the VCP has strict control over the media. Legislation, including internet-related decrees, the penal code, the Publishing Law, and the State Secrets Protection Ordinance, can be used to fin and imprison journalists and netizens. The judiciary is not independent, and trials related to free expression are often brief, and apparently predetermined. Police routinely flou due process, arresting bloggers and online activists without a warrant or retaining them in custody beyond the maximum period allowed by law.

Articles 79, 88, and 258 of the penal code are commonly used to prosecute and imprison bloggers and online activists for subversion, antistate propaganda, and abusing democratic freedoms. Though the law was in effect for the duration of the coverage period, Vietnam's National Assembly amended the penal code on November 27, 2015.[36] Under the amended law, Article 79, "carrying out activities aimed at overthrowing the people's administration," became Article 109, and Article 88, "making, storing, disseminating or propagandizing materials and products that aim to oppose the State of the Socialist Republic of Vietnam," became Article 117.[37] The clauses newly criminalized preparing to commit those crimes with penalties of one to fi e years in prison. Article 258, which punishes "abuse of democratic rights to infringe upon the interests of the State, the legitimate rights and interests of organizations and citizens," became Article 330. The amendments were supposed to become effective on July 1, 2016 butt it was postponed for further revision.[38]

Since 2008, a series of regulations have extended controls on traditional media content to the online sphere. Decree 97 ordered blogs to refrain from political or social commentary and barred them from disseminating press articles, literary works, or other publications prohibited by the Press Law. In 2011, Decree 02 gave authorities power to penalize journalists and bloggers for a series of infractions, including publishing under a pseudonym.[39] Decree 72 on the Management, Provision, Use of Internet Services and Internet Content Online replaced Decree 97 in 2013, expanding regulation from blogs to all social media networks. Article 5 prohibits broad categories of online activity including "opposing the Socialist Republic of Vietnam," inciting violence, revealing state secrets, and providing false information.

A cybersecurity law passed in November 2015 and came into effect on July 1, 2016 (see Surveillance, Privacy and Anonymity).[40]

36 "HRW Submission to EU on Bilateral Dialogue with Vietnam", Human Rights Watch, December 13, 2015 http://bit.ly/1WTky8Q.

37 Human Rights Watch, "Vietnam's Proposed Revisions to National Security Laws," November 19, 2015, https://www.hrw.org/news/2015/11/19/vietnams-proposed-revisions-national-security-laws.

38 "Vietnam legislature to postpone revised penal code as implementation day nears," Tuoi Tre News, June 28, 2016, http://tuoitre-news.vn/society/35591/legislature-to-postpone-revised-penal-code-as-implementation-day-nears.

39 OpenNet Initiative, "Vietnam," August 7, 2012, http://bit.ly/1Z4zX9m; The Ministry of Information and Communication, Decree No 97/2008/ND-CP of August 28, 2008, Officia Gazette, August 11-12, 2008, http://bit.ly/1j9Ejf5; Ministry of Information and Communications, Circular No. 07/2008/TT-BTTTT of December 18, 2008, Officia Gazette, January 6-7, 2009,http://bit.ly/1FSWgs7
Article 19, "Comment on the Decree No. 02 of 2011 on Administrative Responsibility for Press and Publication Activities of the Prime Minister of the Socialist Republic of Vietnam," June 2011, http://bit.ly/1JPbb1x; Decree 02/2011/ND-CP, [in Vietnamese] January 6, 2011, available at Committee to Protect Journalists, http://cpj.org/Vietnam%20media%20decree.pdf.

40 Tilleke and Gibbons, "Legal Update: New Regulations in the ICT Sector in Vietnam, March 2016, http://www.tilleke.com/sites/default/files/2016_Mar_New__egulations_ICT_Sector_Vietnam.pdf; Rouse, "New Law On Cyber Information Security And Its Impact On Data Privacy In Vietnam," March 30, 2016, http://www.rouse.com/magazine/news/new-law-on-cyber-information-security-and-its-impact-on-data-privacy-in-vietnam/.

Prosecutions and Detentions for Online Activities

Vietnam released 14 bloggers and activists under pressure from the US in 2014 and 2015, in the midst of negotiations over the Trans-Pacifi Partnership (TPP), according to Human Rights Watch.[41] Bloggers released from prison were not pardoned. In one case, a fin was still outstanding.[42] Another was escorted to the airport, and will serve her full sentence if she returns from exile.[43]

Although this significantl reduced the number of individuals detained in Vietnam for online activity, which Reporters Without Borders documented as 29 in December 2014,[44] there was no improvement in the overall environment for freedom of expression online. General Tran Dai Quang, the public security minister, told the National Assembly in November 2015 that his forces had "received, arrested, and dealt with" 1,410 cases involving 2,680 people who violated national security since June 2012, a category that includes critics of the government, according to Human Rights Watch.[45] He did not provide details of individual cases, so the number of cases involving online activity remains unknown.

At least 15 bloggers and activists were still jailed at the end of 2015.[46] Some were tried and sentenced during the coverage period, though long after the legal time limit for detention without trial had expired. Nguyen Huu Vinh, who ran the well-known independent blog Anh Ba Sam, was arrested along with his assistant Nguyen Thi Minh Thuy in May 2014 under Article 258 of the penal code. Suspects charged under Article 258 (2) can initially be held in pre-trial detention for up to six months, and for a further 90 days following indictment.[47] Yet both were held for more than 22 months before a court in Hanoi sentenced them to fi e and three years in prison, respectively, in March 2016.[48] Anh Ba Sam was blocked in Vietnam in 2016, but still accessible for users of circumvention tools, though it no longer posts original content.

In a separate trial in March, blogger Nguyen Dinh Ngoc, also known under the pen name Nguyen Ngoc Gia, was sentenced by a court in Ho Chi Minh City to four years in prison for publishing anti-state propaganda online. He was fi st arrested in December 2014.[49]

During the coverage period, several prominent activists were jailed for peaceful dissent, though not directly for their digital activity. In December, the police arrested prominent rights campaigner Nguyen Van Dai and charged him with "conducting propaganda against the state" under Article 88

41 "Vietnam: Widespread 'National Security' Arrests", Human Rights Watch, November 19, 2015, http://bit.ly/1OVc8y0.

42 Article 19, "Interview: Activist Le Quoc Quan, one day after his release from prison," via IFEX, June 30, 2015, https://www.ifex.org/vietnam/2015/06/30/interview_le_quoc_quan/.

43 Human Rights Watch, "Vietnam: Events of 2015," World Report, https://www.hrw.org/world-report/2016/country-chapters/vietnam; Reuters, "Vietnam frees anti-state blogger, U.S. calls for more releases," September 20, 2015, http://www.reuters.com/article/us-vietnam-dissident-idUSKCN0RK0D320150920.

44 Reporters Without Borders, "Another blogger held, RWB calls for immediate release," December 31, 2014, http://bit.ly/1410Xhx.

45 "Vietnam: Widespread 'National Security' Arrests", Human Rights Watch, November 19, 2015, http://bit.ly/1OVc8y0.

46 "Vietnam: Widespread 'National Security' Arrests", Human Rights Watch, November 19, 2015, http://bit.ly/1OVc8y0.

47 "Demand release of blogger and his assistant", Amnesty International, December 2015 http://bit.ly/21z4qQA

48 Committee to Protect Journalists, "Vietnamese bloggers imprisoned for 'abusing democratic freedoms,'" March 23, 2016, https://cpj.org/2016/03/vietnamese-bloggers-imprisoned-for-abusing-democra.php.

49 Committee to Protect Journalists, "Blogger sentenced amid clampdown in Vietnam," March 31, 2016, https://cpj.org/2016/03/blogger-sentenced-amid-clampdown-in-vietnam.php.

of the penal code.[50] The lawyer and activist was involved with YouTube broadcaster Conscience TV,[51] although the charges against him involved organizing meetings.[52]

Separately, in December 2015 two men aged 21 and 23 were sentenced to six months' imprisonment each by a court in the northern city of Hai Phong, four months after they were detained; they had publicized how to avoid traffi checkpoints on Facebook, according to Voice of America.[53]

Surveillance, Privacy, and Anonymity

Limited information is available about advanced surveillance technology available to Vietnamese authorities. In 2013, Citizen Lab, a research group based in Canada, identifie FinFisher software on servers in 25 countries worldwide, including Vietnam. Promoted by United Kingdom-based distributor Gamma International as a suite for lawful intrusion and surveillance, FinFisher offers the power to monitor communications and extract information from other computers without permission, such as contacts, text messages, and emails. Citizen Lab noted that the presence of such a server did not prove who was running it, though it is marketed to governments.

Decree 72 requires providers like social networks to "provide personal information of the users related to terrorism, crimes, and violations of law" to "competent authorities" on request, but lacks procedures or oversight to discourage intrusive registration or data collection. It also mandates that companies maintain at least one domestic server "serving the inspection, storage, and provision of information at the request of competent authorities." The decree gave users themselves the ambiguous right to "have their personal information kept confidentia in accordance with law." Implementation is at the discretion of ministers, heads of ministerial agencies and governmental agencies, the provincial People's Committees, and "relevant organizations and individuals," leaving anonymous and private communication subject to invasion from almost any authority in Vietnam. During the coverage period, "correspondence from the Saigon Post and Telecommunications Service Corporation" was the basis of Nguyen Dinh Ngoc's indictment for disseminating antigovernment propaganda; he was charged under Article 88 of the penal code.[54]

The Law on Information Security passed in November 2015 and came into effect on July 1, 2016, introducing some cybersecurity protections.[55] In more troubling provisions, the law allows the sharing of users' personal information without consent at the request of competent state agencies (Article 17.1.c), mandates that authorities be given decryption keys on request, and introduces licensing

50 "Vietnam: End Thuggish Repression of Activists", Human Rights Watch, January 27, 2016, http://bit.ly/1KbQ9RY

51 Reporters Without Borders, "Vietnam continues crackdown on citizen-journalism," December 10, 2015, https://rsf.org/en/news/vietnam-continues-crackdown-citizen-journalism; Radio Free Asia, "Authorities in Vietnam Crack Down on New Independent Broadcast Service," September 25, 2015, http://www.rfa.org/english/news/vietnam/authorities-in-vietnam-crack-down-on-new-independent-broadcast-service-09252015152145.html

52 FIDH, "Arrest and arbitrary detention of Mr. Nguyen Van Dai, a human rights lawyer and well-known defender of religious freedom," December 18, 2015, https://www.fidh.o g/en/issues/human-rights-defenders/arrest-and-arbitrary-detention-of-mr-nguyen-van-dai-a-human-rights.

53 Trung Nguyen, "Vietnamese Student Jailed for Facebook Posts," Voice of America, December 3, 2015, http://www.voanews.com/content/vietnamese-student-jailed-for-facebook-posts/3086505.html.

54 Human Rights Watch, "Vietnam: 7 Convicted in One Week," April 4, 2016, https://www.hrw.org/news/2016/04/04/vietnam-7-convicted-one-week.

55 Tilleke and Gibbons, "Legal Update: New Regulations in the ICT Sector in Vietnam, March 2016, http://www.tilleke.com/sites/default/files/2016_Mar_New__egulations_ICT_Sector_Vietnam.pdf; Rouse, "New Law On Cyber Information Security And Its Impact On Data Privacy In Vietnam," March 30, 2016, http://www.rouse.com/magazine/news/new-law-on-cyber-information-security-and-its-impact-on-data-privacy-in-vietnam/.

requirements for tools that offer encryption as a primary function, threatening anonymity.[56]

Real-name registration is not required to blog or post online comments, and many Vietnamese do so anonymously. However, Vietnamese authorities do monitor online communication and dissident activity. Cybercafe owners are required to install software to track and store information about their clients' online activities, and citizens must also provide ISPs with government-issued documents when purchasing a home internet connection.[57] In late 2009, the MIC requested all prepaid mobile phone subscribers to register their ID details with the operator and limited each to three numbers per carrier. As of 2016, however, the registration process is not linked to any central database and could be circumvented using a fake ID. Pay-per-use, SIM cards, can be easily purchased without IDs.

Intimidation and Violence

In addition to imprisonment, bloggers and online activists have been subjected to physical attacks, job loss, severed internet access, travel restrictions, and other rights violations. In 2015, at least 40 bloggers and rights activists were beaten by plain-clothes agents, according to Human Rights Watch.[58]

Not all of those assaults were in direct reprisal for online activity, though many targets of violence were known to the authorities because of their blogging and digital activism. In July 2015, Nguyễn Ngọc Như Quỳnh, a blogger who writes under the name "Mẹ Nấm," said police in the southern city of Nha Trang hit her in the face and detained her during a public demonstration in support of political prisoners.[59] She was released without charge.

In September 2015, police in Hanoi detained seven staff members of Conscience TV for several hours as part of a sustained campaign of harassment that included home searches and traffi stops (see Media, Diversity, and Content Manipulation). Other activists, including blogger Doan Trang, reported being harassed outside the police station when they demanded their release.[60]

Journalists for traditional media outlets faced reprisals for Facebook posts in 2015 and 2016. On June 20, 2016, just outside the coverage period of this report, an announcement on the MIC website said the ministry had revoked press credentials for Mai Phan Loi, head of Hanoi bureau of the HCMC Law Newspaper, on grounds he had insulted the military. Loi had discussed the crash of a Vietnamese maritime patrol aircraft in a journalists' group on Facebook the previous week. The post asked why the plane had "exploded into pieces."[61] On June 21, Minister of Information and Communication

56 Michael L. Gray, "The Trouble with Vietnam's Cyber Security Law," The Diplomat, October 21, 2016, http://thediplomat.com/2016/10/the-trouble-with-vietnams-cyber-security-law/; "Vietnamese Cyber Security Law Threatens Privacy Rights and Encryption," September 8, 2016, https://www.tiasangvietnam.org/vietnams-cyber-security-law-threatens-privacy-rights-and-encryption/.

57 "Internet Censorship tightening in Vietnam," Asia News, June 22, 2010, http://bit.ly/1yJgoHk.

58 Human Rights Watch, "Vietnam: End Thuggish Repression of Activists," January 27, 2016, https://www.hrw.org/news/2016/01/27/vietnam-end-thuggish-repression-activists.
Human Rights Watch, "Vietnam: Events of 2015," World Report, https://www.hrw.org/world-report/2016/country-chapters/vietnam

59 "Vietnam's rising repression". New Mandala September 22, 2015 http://bit.ly/1ScnMmJ;
Vietnam Right Now, "Blogger "beaten and arrested" at Nha Trang vigil," July 25, 2015, http://vietnamrightnow.com/2015/07/blogger-beaten-and-arrested-at-nha-trang-vigil/

60 Radio Free Asia, "Authorities in Vietnam Crack Down on New Independent Broadcast Service," September 9, 2015, http://www.rfa.org/english/news/vietnam/authorities-in-vietnam-crack-down-on-new-independent-broadcast-service-09252015152145.html; BBC Vietnamese, "Xô xát vì vụ 'bắt người Lương tâm TV'," September 23, 2015, http://www.bbc.com/vietnamese/vietnam/2015/09/150923_xo_xat_o_quan_hai_ba.

61 "Vietnam reporter's press card revoked for insulting military", AP June 20th 2016 http://apne.ws/28OXZRg.

Truong Minh Tuan warned that journalists should be considerate when using social networks. [62]

In a separate incident, in September 2015, journalist Do Van Hung from the state-run Thanh Nien newspaper was dismissed from his post as the editorial office s deputy general secretary and later had his press card revoked by the Ministry of Information and Communications. Though the media did not publicize the officia reason behind this decision, it was widely reported online that Hung was punished for a September 2 Facebook post coinciding with Vietnam's national day celebrations. The post satirized the August revolution which preceded Vietnam's 1945 declaration of independence from France, and leaders such as Ho Chi Minh and Vo Nguyen Giap.[63]

Technical Attacks

Activists in Vietnam and abroad have been the target of systematic cyberattacks. When activity was fi st documented in 2009, the attackers used Vietnamese-language programs to infect computers with malicious software to carry out distributed denial-of-service (DDoS) attacks on blogs and websites perceived as critical of the government. Google estimated that "potentially tens of thousands of computers" were affected, but Vietnamese authorities took no steps to fin or punish the attackers.

Activists today are subject to account takeovers, where spear-phishing emails disguised as legitimate content carry malware which can breach the recipient's digital security to access private account information. In 2013, attackers seized control of a handful of important alternative blogs, including websites Anh Ba Sam, Que Choa, and blogs written by activists Xuan Dien, Huynh Ngoc Chenh, and others. It is common for sites to post a list of alternative URLs in case the current one is hacked.

Starting in 2013, attacks using malware to spy on journalists, activists and dissidents became more personal. California-based Electronic Frontier Foundation (EFF) and Associated Press journalists reported receiving infected emails inviting them to human rights conferences or offering academic papers on the topic, indicating that the senders are familiar with the activities and interests of the recipients. According to EFF's analysis, the detection rate for the malware is very low - only one anti-virus vendor out of a possible 47 could detect it as of January 2014. In 2015, targeted, personalized attacks were reported by several internet professionals in Vietnam. While they did not receive the same publicity in 2016, they are believed to continue at the same rate.

62 Nhà báo phải cân nhắc khi sử dụng mạng xã hội < journalists should consider when using social networks>, Vietnamnet, June 21, 2016 http://bit.ly/28KtOKa.

63 "Thu hồi Thẻ nhà báo của nhà báo Đỗ Văn Hùng, báo Thanh Niên", (Withdraw the Press card of journalist Do Van Hung, Thanh Nien newspaper), Tuoi Tre, September 4, 2015, http://bit.ly/1LxgTgy.

Freedom House

Zambia

	2015	2016
Internet Freedom Status	Partly Free	Partly Free
Obstacles to Access (0-25)	11	11
Limits on Content (0-35)	12	10
Violations of User Rights (0-40)	17	17
TOTAL* (0-100)	**40**	**38**

* 0=most free, 100=least free

Population:	**16.2 million**
Internet Penetration 2015 (ITU):	**21 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2016 Status:	**Not Free**

Key Developments: June 2015 – May 2016

- There were no reports of blocking, fil ering, or content removals compared to previous years when critical online news outlets were restricted under the preceding president (see **Limits on Content**).
- In January 2016, President Lungu signed into law the much-anticipated Constitution of Zambia (Amendment) Act of 2016, though the amendments lacked many of the provisions sought by citizens, including the protection of fundamental rights and freedoms (see **Legal Environment**).
- Digital activism was vibrant, helping rollback a government shutdown of two universities, while a video shared on WhatsApp and social media helped bring critical attention to the assault of a woman, leading police to seek out the perpetrators (see **Digital Activism**).
- The popular singer Pilato was arrested for a song widely shared on social media and WhatsApp that allegedly defamed President Edgar Lungu in June 2015. Charged with incitement, his case was dismissed in July 2015 (see **Prosecutions and Detentions for Online Activities**)

Introduction

Internet freedom in Zambia improved marginally during the coverage period due to less blocking incidents under the current administration of Edgar Lungu compared to the late and former President Michael Sata, who died in October 2014.

Sata's record on internet freedom was poor, characterized by the blocking of news websites from July 2013 to April 2014 and arrest of several journalists suspected of having an affiliation with the blocked news outlets. In contrast, there have been no websites blocked under President Lungu. Nonetheless, the current government started showing signs of intolerance towards criticism in the past year, arresting the popular singer Pilato for a song widely shared on social media and WhatsApp that allegedly defamed President Lungu in June 2015.

Despite some improvements due to less problematic issues compared to previous years, backsliding occurred in the aftermath of the contentious presidential elections in August 2016 (after this report's coverage period for FOTN scores), which saw the reelection of Edgar Lungu. Following protests that erupted among opposition supporters who accused the electoral commission of voter fraud, there were reports of mobile broadband network disruptions for 48 to 72 hours in opposition held regions of the country, leading to strong suspicions of deliberate government interference. The critical online news outlet *Zambian Watchdog* and its Facebook page were later shut down in September, reportedly after the authorities raided the offices f a local web hosting company in search of *Zambian Watchdog*'s servers.

The August 2016 elections also sought voter approval of constitutional amendments that would enshrine fundamental rights, including protections for print, broadcast, and electronic media freedom. The referendum was initiated in response to the highly anticipated Constitution of Zambia (Amendment) Act of 2016 that was enacted by President Lungu in January 2016 but excluded many of the provisions sought by citizens such as the protection of fundamental rights and freedoms. Though the referendum was approved by 71 percent of voters, the vote failed to garner the minimum voter turnout threshold of 50 percent to validate the results.

Despite Zambia's middling internet freedom environment, citizens continued to be empowered by digital media, using it to pushback against government abuses and call for justice. Digital activism was vibrant in the past year, helping rollback a government shutdown of two universities, while a video shared on WhatsApp and social media helped bring critical attention to the assault of a woman, leading police to seek out the perpetrators.

Obstacles to Access

Internet and mobile access rose steadily but remained low compared to other countries in the region. Increased electricity load shedding, high mobile and Internet purchase costs, poor infrastructure, and a large urban-rural divide are considered as major obstacles to access.

Availability and Ease of Access

Zambia was among the early adopters of the Internet in sub-Saharan Africa with the installation of dial-up and satellite technology at the University of Zambia in the early 1990s, though access has

grown slowly ever since. Internet penetration increased incrementally the past year, growing from a rate of 17 percent in 2014 to 21 percent in 2015, according to the International Telecommunication Union (ITU).[1] Mobile phone usage is expanding more rapidly, reaching a penetration of nearly 75 percent in 2015, up from 67 percent the previous year,[2] as most Zambian internet users access the internet via their mobile devices. Despite increasing access, internet connection speeds remain slow, averaging 2.0 Mbps compared to a global average of 6.2 Mbps, according to Akamai's *State of the Internet* report.[3]

The costs of ICT ownership and access are very expensive and out of reach for the majority of citizens in Zambia, where the average minimum wage is approximately US$47 per month.[4] Blackberry devices still remain the most popular internet-enabled mobile phones in Zambia due to cheap subscription fees, which cost as low as US$5 per month for access. Nevertheless, high costs hinder most Zambians from accessing other the top Internet applications, with a standard smart phone costing about US$200 while broadband subscriptions cost an average of US$26 for 10 GB of data. Only 13.5 percent of people that own mobile phones have a smart phone. Further, less than 1 percent of Zambians access the internet from their homes via fi ed-line broadband subscriptions, which cost an average of US$26 as of February 2016.[5] Zambians also access the internet at cybercafes, which cost slightly less than US$1 per hour. In recent years, however, cybercafes have become less popular as people increasingly access the internet via mobile devices.

While access to ICTs is steadily increasing, it is only widespread in urban areas. Access in rural areas has lagged behind due to the high costs of hardware and software, poor network coverage, and high levels of illiteracy. Erratic and expensive electricity also hinders access for rural areas, where less than 6 percent of residents have access to electricity,[6] and the government has lacked the resources needed to prioritize the development of ICT infrastructure in rural areas. Consequently, the urban-rural divide remains high, with 68 percent of the urban population having access to mobile phones, compared to 39 percent of the rural population.

Restrictions on Connectivity

During the June 2015 to May 2016 coverage period, there were no reports of the Zambian government restricting access to the internet or mobile phone services. However, during presidential elections in August 2016, mobile broadband networks were reportedly disrupted for 48 to 72 hours in opposition held regions of the country, leading to strong suspicions of deliberate government interference.[7] The outage followed protests that erupted among opposition supporters who accused the electoral commission of voter fraud. Two mobile providers—MTN and Airtel—confi med the disruptions but did not provide a reason, leaving it unclear whether the outage was ordered by the

1 International Telecommunication Union, "Percentage of Individuals Using the Internet," 2000-2015, http://bit.ly/1cblxxY.

2 International Telecommunication Union, "Mobile-Cellular Subscriptions," 2000-2015, http://bit.ly/1cblxxY.

3 Akamai, "Broadband Adoption," map visualization, *State of the Internet Report,* http://akamai.me/1LiS6KD.

4 There has been a significant d op in the dollar equivalent to last year's report of $75 due to the loss of value of the kwacha against the dollar. It must be noted that the minimum wage still stands at K540 equivalent to $49 as of 20th February 2016.

5 ZICTA, "ICT survey report 2015 – Households and individuals," https://www.zicta.zm/Views/Publications/2015ICTSURVEYREPORT.pdf.

6 ZICTA, "ICT survey report 2015 – Households and individuals."

7 Nigel Gambanga, "Zambian government suspected of causing internet shutdown following outage in opposition strongholds," TechZim, August 18, 2016, http://www.techzim.co.zw/2016/08/zambian-government-suspected-causing-internet-slowdown-shutdown-following-outage-opposition-strongholds/

government.[8] Nonetheless, the subsequent banning of independent broadcast and radio outlets further strengthened suspicions that the disruptions were part of an overall strategy to crackdown on press freedom and freedom of expression during the election period.[9]

Partial state ownership over the country's fiber ackbone and control over connections to the international internet may enable the government to restrict connectivity at will.[10] As a landlocked country, Zambia's national fiber ackbone is provided by three operators: state-owned Zambia Telecommunications Ltd (Zamtel), state-owned Zambia Electricity Supply Corporation Ltd (ZESCO),[11] and privately-owned Copper belt Energy Corporation (CEC). Zamtel operates the fibe -optic connection to two international submarine cables: the WACS and Sat-3.[12] MTN and Airtel lease access to the undersea cables from Zamtel, while MTN also connects directly to the EASSy.[13] According to a July 2013 *Zambian Watchdog* report, the government may also control the country's internet exchange point (IXP), which is reportedly housed in the same building as state-owned Zamtel in Lusaka.[14]

ICT Market

The Zambian market for ISPs is very competitive and characterized by a lack of a significant dom nant player.[15] As of 2016, there are 23 registered ISPs, three of which are also the country's mobile phone providers: MTN, Airtel, and state-owned Zamtel.[16] All Internet and mobile service providers are privately owned, with the exception of Zamtel, which was renationalized in January 2012 under the directive of the late President Michael Sata.[17] Sata's predecessor had sold the 75 percent share of Zamtel to Lap Green in 2010 for US$257 million.[18] While Zamtel has the smallest share in the mobile phone market,[19] it commands the largest share of Internet subscriptions, with over 60 percent of the market.[20]

Regulatory Bodies

The Zambia Information and Communications Authority (ZICTA) is the regulatory body for the country's ICT sector. Established under the Information and Communication Technologies Act of 2009,

8 Moses Karanja, Twitter post, August 19, 2016, https://twitter.com/Mose_Karanja/status/766684089613185025

9 Conor Gaffey, "Zambia: Three broadcasters shut down as opposition alleges media crackdown," Newsweek, August 23, 2016, http://www.newsweek.com/zambia-three-independent-broadcasters-shut-down-opposition-alleges-media-492764

10 According to the ITU, the gateway to the international internet in Zambia is fully liberalized and competitive. See, ITU, "Zambia Profile (La est data available: 2013)," *ICT-Eye*, accessed August 1, 2016, http://bit.ly/1NEnLHk.

11 Michael Malakata, "ZESCO begins leasing fiber communication ackbone," Network World, September 24, 2008, http://bit.ly/1LcyRkN.

12 Michael Malakata, "Zambia's Zamtel connects to WACS, Sat-3 undersea cables," PC Advisor, July 26, 2012, http://bit.ly/1OxJLFC.

13 "MTN Zambia to invest USD3 million on connection to EASSy," Tele Geography, March 29, 2012, http://bit.ly/1k89kjF.

14 "In bid to spy on citizens, Sata gives Chinese complete access to Zambia's military, OP files" Zambian Watchdog, "July 23, 2013, http://bit.ly/1LczMlf.

15 Shuller Habeenzu, "Zambia ICT Sector Performance Review 2009/2010," (policy paper, Research ICT Africa, 2010) http://bit.ly/1NK9LgU.

16 ZICTA "Internet Service Provider," accessed February 10, 2015, http://bit.ly/1MsuzmW.

17 Sata "deemed it desirable to acquire back the 75 percent shareholding of Libya's Lap Green Network in Zamtel." George Chellah "Press Statement: ZAMTEL Nationalization," press release, January 24, 2012, http://on.fb.me/1OxKlmP.

18 Matthew Saltmarsh, "Privatization of Zambian Phone Company Degenerates into a Feud," *New York Times*, October 3, 2010, http://nyti.ms/1VURg8z.

19 "MTN Zambia is the country's largest mobile operator – ZICA," Lusaka Voice, March 2, 2015, http://bit.ly/1KbWlT2.

20 Deloitte, *Doing Business in Zambia – A unique flavour*, March 2013, http://bit.ly/1NeSJUU.

ZICTA is known to be generally autonomous in its decision-making, although the government has some ability to influence ZIC A's activities.[21] The Minister of Information and Broadcasting Services is mandated to oversee ZICTA's activities and appoint the members and chairperson of the ZICTA board.[22] The minister is also entitled to issue general directives, which the regulator is obligated to carry out.[23]

Some internet content is also regulated by the Independent Broadcasting Authority, which oversees the enforcement and compliance of regulations in broadcast programming. This includes programming that is streamed and published online by TV and radio stations.[24]

Limits on Content

There were no reports of blocking, filtering, or content removals during the coverage period. Digital activism helped rollback a government shutdown of two universities, while a video shared on WhatsApp and social media helped bring critical attention to the assault of a woman, leading police to seek out the perpetrators.

Blocking and Filtering

No websites were blocked during the June 2015 to May 2016 coverage period, and social media and communications platforms such as YouTube, Twitter, Facebook, WhatsApp, and international blog hosting services were freely available. Nevertheless, government officials and po erful business people often issued threats to shut down select websites and blogs.[25] In August 2015, for example, a wealthy banking magnate unsuccessfully sought legal action against the website hosting company GoDaddy to shut down the critical online news outlet *Zambia Reports*, which had been publishing allegedly defamatory reports about the businessman.[26]

Tests conducted by the Open Observatory of Network Interference (OONI) and Strathmore University's Centre for Intellectual Property and Information Technology Law (CIPIT) during the August 2016 election's period (after this report's coverage period for FOTN scores) found that 10 different websites were consistently inaccessible, though it was inconclusive whether the websites were blocked.[27] The sites affected included a forum on drugs, a pornography hub, and a dating website for LGBTI communities, which may be linked to the prohibition of homosexuality under Zambia's Penal Code.[28]

In 1996, Zambia became the fi st country in sub-Saharan Africa to censor online content when the government demanded the removal of a banned edition of *The Post* from the newspaper's website by threatening to hold the Internet service provider (ISP), Zamnet, criminally liable for the content.

21 International Telecommunication Union, "Zambia Profile (La est data available: 2013)."

22 First Schedule (Section 4), The Information and Communication Technologies, Act [No. 15 of 2009], http://bit.ly/1KbWEx7.

23 Information and Communication Technologies Act, No. 15 of 2009, Part XI, art 91, http://bit.ly/1KbWEx7; See also, Shuller Habeenzu, "Zambia ICT Sector Performance Review 2009/2010," (policy paper, Research ICT Africa, 2010) http://bit.ly/1NK9LgU.

24 Independent Broadcasting Authority, "About Us," accessed August 1, 2016, http://www.iba.org.zm/about-us.html

25 Gershom Ndhlovu, "Rahjani Mathani petitions Zambia reports to shut down," Lusaka Voice, August 8, 2015, http://lusakavoice.com/2015/08/08/rajan-mahtani-petitions-zambia-reports-to-be-shutdown/

26 "Zambia Reports may be shut down permanently, Dr. Rajan Mahtani takes action!" Newswire, press release, August 11, 2015, https://www.newswire.com/press-release/zambia-reports-may-be-shut-down-permanently-dr-rajan-mahtani

27 Maria Xynou et al., "Zambia. Internet censorship during the 2016 general elections?" October 11, 2016, https://ooni.torproject.org/post/zambia-election-monitoring/#finding

28 Sections 155 through 157, http://www.parliament.gov.zm/sites/default/files/documents/acts/ enal%20Code%20Act.pdf.

There were no other reported incidents of internet censorship until July 2013, when four independent online news outlets—*Zambia Watchdog*, *Zambia Reports, Barotse Post*, and *Radio Barotse*—were blocked until April 2014, purportedly by the government for their critical coverage of the Patriotic Front ruling party under President Michael Sata.[29] The government had previously tried to ban *Zambian Watchdog* in 2012.

Content Removal

The government has been known to censor content by directing online media editors to remove material considered problematic or offensive upon request. However, the extent of this practice is unknown given the predominance of state-owned and progovernment news outlets in the country. Instances of takedown requests are likely unreported, while self-censorship may limit the volume of critical content that could be targeted.

In September 2016 (after this report's coverage period for FOTN scores), the critical online news outlet *Zambian Watchdog* and its Facebook page became completely inaccessible to all users, including outside Zambia, reportedly after the authorities raided the offices f a local web hosting company in search of *Zambian Watchdog*'s servers.[30] Though the government has not released an official sta e-ment about the issue, the shutdown followed weeks of post-election criticism by the news outlet, which had been blocked in the past (see "Blocking and Filtering"). It is uncertain whether the outlet's Facebook page was taken down by the company or its administrators. Both pages remain inaccessible as of October 2016.

Prior to this incident, the only other known case of content removal comes from *Zambia Reports*, who publicly admitted to complying with a government takedown request in its July 2013 open letter to the government, though the outlet did not reveal the nature of the content that was taken down or when it occurred.[31] Otherwise, intermediaries are not held liable for content under the 2009 Electronic Communications and Transactions Act.[32]

Media, Diversity, and Content Manipulation

Online content producers have continued to face considerably less government pressure compared to their traditional media counterparts, though the majority of online news sources in Zambia are merely web versions of pro-government mainstream outlets. As a result, social media platforms and citizen journalists have emerged as important sources of information, and Zambians now recognize the parallel existence of official media and al ernative voices from online sources. The Zambian blogosphere is vibrant, representing diverse viewpoints and opposition voices, and many mainstream journalists have turned to blogs to express themselves more freely. With the start of the digital migration process in June 2015, local content from mainstream media is now available online, greatly improving local media productions both online and off.

29 Peter Adamu, "Zambia Reports, Watchdog 'Unblocked'," *Zambia Reports*, April 4, 2014, http://bit.ly/1KbWYfu; "The Watchdog has been released," *Zambia Weekly*, March 27, 2014, http://bit.ly/1X7wVPP; "Zambia blocks third website: Barotse Post," *Zambian Watchdog*, September 10, 2013, http://bit.ly/1MFdqLs.

30 "The Plight of the Zambian Watchdog: Embattled Opposition News Site Goes Down," Global Voices (blog), October 11, 2016, http://bit.ly/2eG86wc

31 Editor, "Zambia Requested to Stop Blocking Access to Websites," *Zambia Reports*, July 25, 2013, http://bit.ly/1Rdpkve.

32 Electronic Communications and Transaction Act No. 21 of 2009, Part X, Limitation of Liability of Service Providers, http://bit.ly/1Pk92TO.

While blogs hosted on international platforms have proliferated in recent years, online publications face economic constraints that compromise their ability to remain financially sustainable. The government is the largest source of advertising revenue for traditional media outlets and has been known to withhold advertisements from critical outlets.[33] Moreover, private companies often do not advertise in news outlets that seem antagonistic to government policies out of fear of the potential repercussions.[34] These trends are likely mirrored online, though in general, online news platforms are much less developed than print and broadcast media. The two most popular independent online news outlets in Zambia—*Zambian Watchdog* and *Zambia Reports*—are both hosted abroad and receive advertising revenue from international businesses.

Growing government pressure on the media in recent years has created a climate of self-censorship among journalists, both on and offline. Online jou nalists and bloggers are increasingly choosing to write anonymously due to harassment, the threat of legal action, or both,[35] particularly on issues regarding politics and corruption involving government officials. Social media use s tend to express themselves more freely online, but a growing belief that the government monitors social media activity has made users more cautious in recent years.[36] Meanwhile, pro-government trolls are becoming increasingly common on social media platforms such as Facebook, typically flooding posts that are critical of the government with insults and comments on unrelated issues.[37] Some observers suspect that the government may be paying the trolls to disseminate pro-government propaganda.[38]

Digital Activism

Social media and communications platforms, particularly Facebook and WhatsApp, have played an important role mobilizing Zambian citizens around a variety of social and economic issues, such as land reform, the mining industry, education, social economic injustices and taxes.

In response to the shutdown of the University of Zambia and the Copperbelt University by the government due to student protests in February 2016, one of Zambia's musicians popularly known as Pilato produced and released a song in support of the student protesters.[39] Pilato announced the release of the song on his Facebook page and disseminated the song through WhatsApp, urging people to forward the song. The digital activism inspired by Pilato's song ultimately compelled the government to reopen the universities in April 2016.

In June 2016, WhatsApp and social media helped bring critical attention to the assault of a woman by a group of men. The video was shot on a mobile phone and widely circulated on WhatsApp and social media platforms, eventually attracting the attention of police who arrested the perpetrators.[40]

33 Freedom House, "Zambia," *Freedom of the Press 2014*, http://www.freedomhouse.org/report/freedom-press/2014/zambia.

34 "Zambia 2013," African Media Barometer (Friedrich-Ebert-Stiftung: fesmedia Africa, 2013).

35 "Zambia 2013," African Media Barometer (Friedrich-Ebert-Stiftung: fesmedia Africa, 2013).

36 Catherine de Lange, "Journalism in Zambia: Self-Censorship, Blocked Websites, and Social Media Monitoring," International Reporting Project, Johns Hopkins University, July 26, 2013, http://bit.ly/1MFfQJQ.

37 Zambian Economist, Facebook Post, July 12, 2014, http://on.fb.me/1GIYKED.

38 Evans Mulenga, "Zambia's Growing Censorship Problem," *Zambia Reports*, May 6, 2014, http://bit.ly/1jriYOu.

39 Government on 3rd February closed down CBU and UNZA after student protests for meal and book allowances. See, "Kaingu closes UNZA, CBU indefini ely," Lusaka Times, February 3, 2016, http://bit.ly/2frgvTA

40 The video of the incident was circulated on WhatsApp and shared on social media platforms. See: "Brutal assault, sexual abuse video goes viral," Lusaka Times, July 2, 2016, http://lusakavoice.com/2016/07/02/brutal-assault-sexual-abuse-video-goes-viral/; YouTube video: https://www.youtube.com/watch?v=lDYRjgdudBs

Violations of User Rights

In January 2016, President Lungu signed into law the much-anticipated Constitution of Zambia (Amendment) Act of 2016, though the amendments lacked many of the provisions sought by citizens, including the protection of fundamental rights and freedoms. The Zambian government was less restrictive on online journalists during this report's coverage period but started showing signs of intolerance towards criticism, arresting the popular singer Pilato for a song widely shared on social media and WhatsApp that allegedly defamed President Lungu in June 2015.

Legal Environment

President Lungu enacted the Constitution of Zambia (Amendment) Act of 2016 in January, implementing a new constitution that had been in the works since the early 2000s.[41] The new amendments stemmed from a process that started in 2011 under then President Michael Sata. While many drafts emerged from local conferences that sought multi-stakeholder engagement from citizens and civil society organizations, the January amendments approved by parliament and the president lacked many of the provisions sought by citizens, including the protection of fundamental rights and freedoms.[42] A constitutional referendum was subsequently held in August 2016 alongside general elections to seek voter approval of new amendments to the constitution's "Bill of Rights," which provides specific p otections for print, broadcast, and electronic media freedom, and explicitly prohibits the government from exercising control or interfering with media activities.[43] Though approved by 71 percent of voters, the referendum vote failed to garner the minimum voter turnout threshold of 50 percent to validate the results.[44]

Without constitutional protections, freedom of expression and the media are limited by clauses in the penal code that criminalize defamation of the president[45] and give the president "absolute discretion" to ban publications regarded as "contrary to the public interest."[46] In July 2016, the Minister of Information and Broadcasting was reportedly put on the record stating in reference to coverage of the political opposition that "it was important to censor the information that would be disseminated to the public to avoid raising alarm."[47] Concerned observers took the minister's statement to mean that public media must only cover the ruling party and ignore opposition political parties because the information they present is not important.[48]

Compared to specific restrictions on the traditional media, there are no restrictive laws related to the regulation of ICTs and online activities, though government officials often state their intentions to introduce legislation regulating online media, citing the problems of "internet abuse" and cybercrime.

41 "President Lungu ushers news constitution, calls for new approach to politics," Lusaka Times, January 5, 2016, https://www.lusakatimes.com/2016/01/05/president-lungu-ushers-in-a-new-constitution-calls-for-a-new-approach-to-politics/

42 "Zambia constitutional amendments do not protect basic rights," Freedom House, press release, January 6, 2016, https://freedomhouse.org/article/zambia-constitutional-amendments-do-not-protect-basic-rights

43 Constitution of Zambia Amendment Bill of Rights, June 2016, http://bit.ly/2eAonTu

44 "Referendum vote flops, fails o meet threshold," Lusaka Times, August 19, 2016, http://bit.ly/2fGW1K1

45 The Penal Code Act, Chapter 7, art. 69, http://bit.ly/2fcA9ln

46 The Penal Code Act, Chapter 7, art. 53.

47 Michael Malakata, "Zambia rejects new constitution permitting online news freedom," PC Advisor, April 11, 2014, http://bit.ly/1MFhETh.

48 "Censorship is crucial in giving the readers the correct information-Kambwili," Lusaka Times, August 4, 2016, https://www.lusakatimes.com/2016/08/04/censorship-crucial-giving-readers-correct-information-kambwili/

Judicial independence is guaranteed in the new amended constitution but is not respected in practice; it is also undermined by other laws that allow for executive interference in Zambia's justice system. Notably, the Service Commissions Act, which establishes a Judicial Service Commission to advise the president on judicial appointments, provides the president with the power to give the commission "general directions as the President may consider, necessary" and obliges the commission to comply with the directions.[49]

Prosecutions and Detentions for Online Activities

The Zambian authorities periodically arrest and/or prosecute citizens for their online activities. In June 2015, the singer Chama Fumba popularly known as "Pilato" was arrested for a song criticizing the president that went viral on Facebook and WhatsApp. Officials accused Pila o of defaming President Edgar Lungu through lyrics that depicted a man named Lungu as incompetent and an alcoholic.[50] He was charged with provoking public unrest, which would have carried a prison sentence of up to six months and fine if convic ed.[51] Prosecutors dropped the case in July 2015.[52]

Surveillance, Privacy, and Anonymity

Little is known about the Zambian government's surveillance practices and capabilities. In July 2015, email leaks from the Italian surveillance fi m Hacking Team revealed that the company may have sold sophisticated spyware known as Remote Control System (RCS) to the Zambian authorities.[53] While the leaked emails did not confi m the sale, they point to the government's intent to acquire such technologies that can monitor and intercept user communications.

The Electronic Communications and Transaction Act of 2009 details conditions for the lawful interception of communications,[54] though several provisions give the government sweeping surveillance powers with little to no oversight. Article 77 requires service providers to install both hardware and software that enable communications to be intercepted in "real-time" and "full-time" upon request by law enforcement agencies *or* under a court order. Service providers are also required to transmit all intercepted communications to a Central Monitoring and Coordination Centre managed by the communications ministry.[55] Service providers that fail to comply with the requirements could be held liable to a fine, imprisonment f up to fi e years, or both.

While surveillance abuse has not been reported under the current government, the late President Michael Sata's previous administration was often accused of conducting extensive illegal surveillance

49 Service Commissions Act, Cap 259, Part II, Service Commissions, http://bit.ly/1hHnYwq; See also: Richard Lee, "Executive interference undermines judiciary in Zambia," Open Society Initiative for Southern Africa (blog), August 27, 2013, http://bit.ly/1KbYIoY.

50 "Singer Pilato detained and prosecuted for song about president," Free Muse, June 11, 2015, http://freemuse.org/archives/10228

51 "Zambian police arrest musician mocking president," Reuters, June 8, 2015, http://reut.rs/2epYkLk

52 "Zambian singer accused of lampooning president as drunk incompetent walks free," Mail & Guardian, July 13, 2015, http://mgafrica.com/article/2015-07-13-zambian-singer-accused-of-lampooning-president-as-drunk-incompetent-walks-free

53 Ryan Gallagher, Twitter Post, July 6, 2015, 1:10 PM, http://bit.ly/1OGeQoW

54 Electronic Communications and Transaction Act No. 21 of 2009, Part XI, Interception of Communication, http://www.zicta.zm/Downloads/The%20Acts%20and%20SIs/ect_act_2009.pdf

55 Articles 7, Electronic Communications and Transaction Act No. 21 of 2009, Part XI, Interception of Communication.

of citizens' ICT activities, such as the phone tapping of senior government officials who fell out f the ruling party's favor,[56] civil society leaders,[57] and journalists.[58]

The ability for Zambians to communicate anonymously through digital media is compromised by SIM card registration requirements instituted in September 2012.[59] Registration requires an original and valid identity card such as a national registration card presented in person to a registration agent at a mobile service provider.[60] While the government stated that the registration requirements were for the purposes of combatting crime,[61] investigative reports from 2012 have alleged that subscriber details may be passed directly to the secret service for the creation of a mobile phone user database.[62]

Registration for the .zm country code top-level domain (ccTLD) is managed by ZICTA as provided for under the 2009 Electronic Communications and Transaction Act, which may compromise the anonymity of .zm website owners given the murky independence of the regulatory authority.[63] The act also provides a government minister the authority to create statutory agreements that determine further requirements for domain name registration, in addition to "the circumstances and manner in which registrations may be assigned, registered, renewed, refused, or revoked."[64] Such direct oversight of local web domains may allow the government to access user data belonging to local content creators and hosts.

Intimidation and Violence

Online journalists are periodically targeted for harassment and intimidation, while media workers in general face a climate of intimidation for their independent reporting, though there have been no reported incidents under current President Lungu who took office in anuary 2015. The last reported incidents of harassment occurred between June and September 2013, when the previous government targeted individuals suspected of writing anonymously for the critical online news outlets, *Zambian Watchdog* and *Zambia Reports*, including Thomas Zyambo, Clayson Hamasaka, and Wilson Pondamali who were all harassed and subsequently arrested. Zyambo was reportedly threatened and physically assaulted by President Sata's son for unknown reasons in March 2014.[65] Pondamali was attacked in April 2014 at a public event, allegedly by government "thugs" who took off with his digital equipment.[66]

56 Evans Mulenga, "Sata Is Listening to Your Conversation," *Zambia Reports*, October 9, 2013, http://bit.ly/1X7BJVc; Rebecca Chao, "Zambian President Admits to Spying on Fellow Officials" *TechPresident* (blog), October 16, 2013, http://bit.ly/1GJ08ak.

57 Peter Adamu, "Sata is Tapping Phones, says Fr Bwalya," *Zambia Reports*, January 23, 2014, http://bit.ly/1VViJfq.

58 "Airtel Zambia Facing Phone Tapping Allegations," *AfricaMetro*, June 18, 2015, http://bit.ly/1VUX2Hh.

59 "Zambia switches off 2.4 million unregistered SIMs," *Lusaka Voice*, February 6, 2014, http://bit.ly/1k8g15g.

60 MTN Zambia, "SIM Registration," accessed September 25, 2014, http://bit.ly/1NKgCXx.

61 Gershom Ndhlovu, "Zambia: SIM Registration is For Security Reasons," Global Voices (blog), November 30, 2012, http://bit.ly/1ZGFOC9.

62 "OP compiling Database from simcard registration exercise," Zambian Watchdog, November 13, 2012, http://bit.ly/1VUY9GZ. An official f om ZICTA also publicly stated in November 2012 that registration would "enable law enforcement agencies [to] create a database to help identify the mobile SIM card owners," according to a news report in *Lusaka Times*. See, "SIM card registration is not a political issue-ZICTA," *Lusaka Times*, November 25, 2012, http://bit.ly/1LcFfZ8.

63 Electronic Communications and Transaction Act No. 21 of 2009, Part IX, Domain Name Regulation.

64 Electronic Communications and Transaction Act No. 21 of 2009, Part IX, Domain Name Regulation, art. 52.

65 Gershom Ndhlovu, "Zambia: President's Son Warns Journalist, 'We Will Kill You,'" Global Voices (blog), March 12, 2014, http://bit.ly/1GgGBTH.

66 "PF thugs beat up Journalist Wilson Pondamali," Zambian Watchdog, April 11, 2014, http://bit.ly/1NKh8oB.

Technical Attacks

Government-sponsored technical attacks against opposition activists, ordinary users, or online journalists are not common in Zambia and were not reported during the coverage period. The last reported technical attack was reported in April 2014 when the website of the Media Institute for Southern Africa (MISA) was hacked alongside a number of government websites by hackers from the Middle East.[67] *Zambian Watchdog* was last attacked with a DDoS attach in May 2012 that brought the site down for about eight hours.[68]

67 Limbikani Makani, "100+ Zambian websites hacked & defaced: Spar, Postdotnet, SEC, Home Affairs, Ministry of Finance," *Tech Trends*, April 15, 2014, http://bit.ly/1MFmY9c.

68 Gershom Ndhlovu, "Zambia: Citizen News Website Hacked," *Global Voices*, May 13, 2012, http://bit.ly/1VUYw45.

Freedom House

Zimbabwe

	2015	2016
Internet Freedom Status	**Partly Free**	**Partly Free**
Obstacles to Access (0-25)	15	15
Limits on Content (0-35)	16	16
Violations of User Rights (0-40)	25	25
TOTAL* (0-100)	**56**	**56**

* 0=most free, 100=least free

Population:	**15.6 million**
Internet Penetration 2015 (ITU):	**16 percent**
Social Media/ICT Apps Blocked:	**Yes^**
Political/Social Content Blocked:	**No**
Bloggers/ICT Users Arrested:	**Yes^**
Press Freedom 2016 Status:	**Not Free**

^Occurred after coverage period until September 2016

Key Developments: June 2015 – May 2016

- The government increased its share of the ICT market in its acquisition of mobile provider Telecel, while infighting bet een the regulator and telecoms on various policy issues led to decreasing industry confidence in the egulatory environment (see **ICT Market**).
- The draft National Policy for Information and Communications Technology (ICT) introduced in late 2015 provides a framework for centralizing control over the country's internet, which critics worry will establish a Chinese-style "Great Firewall" on Zimbabwe's internet (see **Restrictions on Connectivity**).
- A YouTube video featuring a spoken word lament about Zimbabwe's current state of affairs by Pastor Evan Mawarire in April 2016 sparked the largescale #ThisFlag social media movement (see **Digital Activism**).
- In a landmark positive step, criminal defamation was ruled unconstitutional in February 2016 (see **Legal Environment**).
- Several individuals were arrested for their online activities during the coverage period, reflecting a mar ed increase compared to previous years (see **Prosecutions and Detentions for Online Activities**).

Introduction

Internet freedom in Zimbabwe remained tenuous over the past year, beleaguered by declining conditions for access, government efforts to exert greater control over the country's ICT market and internet infrastructure, threats to shutdown social media, and increasing arrests for online activities.

In the midst of political infighting, economic instabilit , and uncertainty over who will eventually succeed President Robert Mugabe—the 92-year old authoritarian in power since 1987—Zimbabweans increasingly floc ed to social media and communications apps to share critical news and information and to express discontent with the government's failing policies. In May 2016, citizens were captivated by a YouTube video created by Pastor Evan Mawarire in which he criticized Zimbabwe's current state of affairs in a spoken word piece titled, "This Flag – A Lament."[1] The video launched the #ThisFlag social media movement which helped inspire anti-government protests in July.

Catching onto citizens' increasing online engagement, government officials egularly decried the destabilizing effects of social media and reportedly blocked access to WhatsApp for several hours during the July protests. Meanwhile, several individuals were arrested for online activities throughout the year, including Pastor Evan Mawarire for his videos on social media that the authorities perceived as inciting public violence,[2] as well as several ordinary users for their WhatsApp messages that criticized aging President Mugabe.[3]

In the past year, the government took concrete steps to increase its control over the internet, though the efforts have yet to manifest. In January 2016, for example, the president announced that his government would engage the Chinese to help fil er the internet and block social media.[4] His announcement came shortly after the draft National Policy for Information and Communications Technology (ICT) was introduced that provides a framework for centralizing control over the country's internet, which critics worry will establish a Chinese-style "Great Firewall" on Zimbabwe's internet. The Computer Crime and Cybercrime Bill was also introduced in August 2016, which threatens to penalize social media criticism.

In a positive step, the Constitutional Court struck down criminal defamation under the Criminal Law Codification and eform Act (CODE) in February 2016,[5] while another court spoke up in defense of the constitutional right to privacy in October, indicating that legislation impeding privacy and other rights may be challenged by Zimbabwe's judiciary.[6]

1 YouTube video, "This Flag – A Lament," posted April 19, 2016, https://www.youtube.com/watch?v=LubMilbHiPg

2 "Zimbabwe protest pastor Evan Mawarire charged with 'inciting violence,'" Times Live, July 12, 2016, http://www.timeslive.co.za/africa/2016/07/12/Zimbabwe-protest-pastor-Evan-Mawarire-charged-with-inciting-violence

3 "WhatsApp slur against Mugabe gets Zim man arrested – report," News24, October 4, 2015, http://www.news24.com/Africa/Zimbabwe/WhatsApp-slur-against-Mugabe-gets-Zim-man-arrested-report-20151004

4 L.S.M. Kabweza, "Chinese style internet censorship coming to Zimbabwe – President Mugabe," TechZim, April 4, 2016, http://www.techzim.co.zw/2016/04/china-style-internet-censorship-coming-to-zimbabwe-president-mugabe/

5 "Zimbabwe Constitutional Court Strikes Criminal Defamation Laws," Committee to Project Journalists, press release, February 3, 2016, https://cpj.org/2016/02/zimbabwe-constitutional-court-strikes-criminal-def.php

6 Tawanda Korondo, "Hands off private communications warns Zim court," ITWeb Africa, October 18, 2016, http://www.itwebafrica.com/ict-and-governance/273-zimbabwe/236953-hands-off-private-communications-warns-zim-court

Obstacles to Access

The draft National Policy for Information and Communications Technology (ICT) was introduced in late 2015 aims to centralize the country's internet, raising deep concerns over the government's desire to restrict access. The government increased its share of the ICT market in its acquisition of mobile provider Telecel, while infighting between the regulator and telecoms on various policy issues led to decreasing industry confidence in the regulatory environment.

Availability and Ease of Access

Access to the internet in Zimbabwe stood at 50 percent in March 2016, according to official go ernment data from the telecoms regulator, which incorporates mobile broadband access.[7] The International Telecommunications Union (ITU) reported a much lower rate of 16 percent, decreasing from 20 percent in 2014.[8] Mobile phone penetration was much higher at 85 percent as of December 2015 per ITU data,[9] or 97 percent as of March 2016 per official go ernment data,[10] though millions of Zimbabweans remain virtually disconnected due to poor network coverage in remote areas or the lack of affordable services.[11] According to the 2015/16 Affordability Report, the Alliance for Affordable Internet estimated that 500MB of mobile broadband costs nearly 30 percent of the country's GNI per capita of US$840, which is well above the target of 5 percent or less set by the UN Broadband Commission in 2011 as a goal for broadband affordability.[12]

A significant ur an-rural divide exists among Zimbabwean internet users, as most base stations that facilitate access to the internet via mobile phones are in urban areas.[13] Network quality and coverage are still poor, with only 88 percent and 54 percent of Zimbabwe's population covered by 2G and 3G enabled base stations, respectively. Average broadband speeds improved incrementally from 3.1 Mbps in 2015 to 4.7 Mbps in 2016, though Zimbabwe still performs below the global average of 6.3 Mbps, according to Akamai.[14]

Flagging internet access rates in the past year could be attributed to the country's economic crisis and falling household incomes,[15] which have decreased the profits f telecommunications companies, resulting in reduced investments in the ICT sector. In October 2015, Zimbabwe's leading telecoms provider Econet announced a 17.7 percent drop in profit as com ared to the past year's revenue, which the company blamed on a floundering economy and new egulations, such as a

7 POTRAZ, Postal and Telecommunications Sector Performance Report, First Quarter 2016, https://www.potraz.gov.zw/images/documents/Sector_Perfomance_report_1st_Quarter_2016.pdf

8 International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2015," http://bit.ly/1cblxxY

9 International Telecommunication Union, "Mobile-Cellular Telephone Subscriptions, 2000-2015," http://bit.ly/1cblxxY

10 POTRAZ, Postal and Telecommunications Sector Performance Report, First Quarter 2016.

11 Majaka, N. "Zim Mobile penetration rate misleading," The Daily News, December 21, 2014, http://www.dailynews.co.zw/articles/2014/12/21/zim-mobile-penetration-rate-misleading-potraz.

12 Alliance for Affordable Internet, The Affordability Report, 2015, http://a4ai.org/affordability-report/data/?_year=2015&indicator=INDEX&country=ZWE

13 According to the fi st quarter 2016 report from Potraz: "The total number of base stations in rural areas was 1,940 versus 4,780 base stations in urban areas. A comparison with the fourth quarter shows that base stations in rural areas increased by 11% from 1,748 to reach 1,940 base stations. However the increase was mostly in 2G technology." See, POTRAZ, Postal and Telecommunications Sector Performance Report, First Quarter 2016.

14 Akamai, "Average Connection Speed," map visualization, *The State of the Internet*, Q1 2016, accessed August 1, 2016, http://akamai.me/1LiS6KD

15 Fidelity Mhlanga, "Firms repackage products as economy sinks deeper," Zimbabwe Independent, November 4, 2016, https://www.theindependent.co.zw/2016/11/04/fi ms-repackage-products-economy-sinks-deeper/

35 percent reduction on the costs of voice calls in 2014.[16] Other adverse regulations included a 5 percent tax on airtime and a 40 percent duty on imported mobile phone handsets, computers, and laptops, which were introduced by the government in 2014. This unfavorable operating environment has forced telecom companies to reduce investments in infrastructure.[17]

In January 2016, the Zimbabwe Revenue Authority reduced a traveler rebate for the value of goods that individuals can import without paying duties from US$300 to $200,[18] which may have a negative impact on small IT businesses that use this duty-free rebate to import ICT gadgets for resale.

Restrictions on Connectivity

No cases of deliberate disruptions in mobile phone or broadband internet networks were recorded during the June 2015 to May 2016 coverage period, though WhatsApp was inaccessible for several hours during widespread anti-government protests in July (see Blocking and Filtering). Separately, the internet research fi m Renesys documented outages on 31 percent of the country's networks on the same day.[19] Observers have noted that private ownership of the majority of the country's international gateways makes it difficult for the go ernment to shutdown the entire internet.[20] Two of Zimbabwe's fi e international gateways for internet and voice traffic a e operated by the state-owned fi ed network, TelOne, and mobile network, NetOne. The private mobile operators—Econet, TeleCel, and Africom—operate the other three international gateways.[21]

In late 2015, the Ministry of ICT introduced the draft National Policy for Information and Communications Technology (ICT), which put forth an ambitious set of policies that, if implemented, would dramatically change Zimbabwean's internet freedom landscape through centralized control over the country's internet. Section 5 of the document on "ICT Infrastructure" details plans to establish a single national ICT backbone to be owned by various public and private shareholders but ultimately controlled by the government.[22] The section also mandates infrastructure sharing among telecoms, which private telecoms who have invested heavily in their own infrastructure have decried as a form of "backdoor nationalization."[23] Most troublingly, Section 21.3 creates "The National Backbone Company," defined by the document as "one Super Ga eway which shall be the entry and exit point for all international traffic "[24] The policy had not been implemented as of October 2016.

16 Gambanga, N., "Econet announces 17.7% drop in revenue, 52% decline in profit in 2015 Half ear Results," TechZim, October 14, 2015, http://www.techzim.co.zw/2015/10/econet-announces-17-7-drop-in-revenue-52-decline-in-profi -in-2015-half-year-results/; L.S.M. Kabweza, "Zim government introduces 5% tax on mobile airtime," TechZim, September 11, 2014, http://www.techzim.co.zw/2014/09/zim-government-introduces-5-tax-mobile-airtime/

17 POTRAZ, Postal and Telecommunications Sector Performance Report, First Quarter 2016.

18 Thupeyo Muleya, "Govt slashes travellers' rebate," The Herald, January 5, 2016, http://bit.ly/2eGbXcA

19 "60 networks out in Zimbabwe," Dyn Events, July 6, 2016, http://bit.ly/2fUFDF4

20 Munya Bloggo, "'We really believe social media will drive change in Mugabe's Zimbabwe,'" Quartz Africa, August 2, 2016, http://qz.com/748132/we-really-believe-social-media-will-drive-change-in-mugabes-zimbabwe/

21 POTRAZ, Postal and Telecommunications Sector Performance Report, First Quarter 2016.

22 Zimbabwe National Policy for Information and Communications Technology (ICT), 2015, Section 5.1, http://www.techzim.co.zw/wp-content/uploads/2015/12/Zimbabwe-Draft-National-ICT-Policy-2015-.pdf?x97092

23 POTRAZ, "POTRAZ Embarks on Infrastructure Sharing Drive," accessed October 1, 2016, http://www.potraz.gov.zw/index.php/categorylinks/103-potraz-embarks-on-an-infrastructure-sharing-drive

24 Zimbabwe National Policy for Information and Communications Technology (ICT), 2015, Section 21.3.

ICT Market

The ICT market in Zimbabwe is diverse, with 15 licensed internet service providers (ISPs) registered with the Zimbabwe Internet Service Providers Association (ZISPA) in 2016,[25] one of which is the government-owned Zarnet, which provides IT products and services as well as internet service.[26] As set by the regulator, license fees for ISPs range from US$2-4 million, depending on the type of service, and must be vetted and approved by the regulator prior to installation.[27] Providers must also pay 3.5 percent of their annual gross income to the regulator.

There are fi e mobile service providers in the country: state-owned TelOne and NetOne, partially state-owned Telecel, and privately owned Econet and Africom. License fees for operating mobile phone services in Zimbabwe are steep, increasing from US$100 million to $137.5 million in 2013.[28] Only one mobile service provider, privately-owned Econet, had paid this fee in full by 2016, while the second largest network, Telecel, had paid a deposit. Telecel's future also hangs in the balance after a hostile government takeover in late 2015. The Zimbabwean government reportedly forced Dutch company VimpelCom to sell 60 percent of its shares in Telecel to government-owned Zarnet for US$40 million in November 2015,[29] forcing VimpelCom out of the Zimbabwe market and increasing the government's share. Telecel lost clients as a result of the takeover, forcing the company to cut down on staff and salaries.[30]

The state-owned telecom companies NetOne and TelOne were embroiled in accusations of mismanagement and corruption in the past year, with NetOne reportedly losing millions of USD through misappropriation and saddled with a US$330 million debt that the government has taken over.[31] Observers believe the proposed centralization of the country's internet backbone and gateway in the draft National Policy for ICT (see Restrictions on Connectivity) is partially motivated by the government's desire to bolster the flagging p ofits f its telecom providers.

Regulatory Bodies

ISPs and mobile phone companies are regulated by the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), whose leaders are appointed by the president in consultation with the minister of transport and communication.[32] POTRAZ is expected to operate independently but has increasingly become subsumed by the ICT Ministry in recent years; it previously fell under the

25 Zimbabwe Internet Service Providers Association: http://www.zispa.org.zw/

26 ZARNet: http://www.zarnet.ac.zw/index.php/about/

27 L.S.M Kabweza, "Zimbabwe Raises Telecoms License Fees, Migrates to Converged Licensing," TechZim, March 12, 2013, http://www.techzim.co.zw/2013/03/zimbabwe-raises-telecoms-licence-fees-migrates-to-converged-licencing/.

28 Tawanda Karombo, "Zimbabwe sets telecom license fees at $137.5mn," IT Web Africa, June 3, 2013, http://www.itwebafrica.com/telecommunications/154-zimbabwe/231106-zimbabwe-sets-telecom-license-fees-at-1375mn.

29 Majaka,N. "Telecel Sold for a song," Daily News, November 19, 2015, https://www.dailynews.co.zw/articles/2015/11/19/telecel-sold-for-a-song

30 Makoshori, S. "Subscribers ditch Telecel," The Financial Gazette, February 4, 2016, http://nehandaradio.com/2016/02/05/94361/.

31 Gumbo,L. "NetOne scandal deepens," The Herald, February 17, 2016, http://www.herald.co.zw/netone-scandal-deepens/; Muronzi,C. "Government t to inherit USD 322, Telone debt," Zimbabwe Independent, October 2, 2015, http://www.theindependent.co.zw/2015/10/02/govt-to-inherit-us322-million-telone-debt/

32 L.S.M. Kabweza, "POTRAZ now under Office f President & Cabinet. To improve regulatory independence," TechZim, October 15, 2013, http://bit.ly/1Ga8Wv8

President's Office [33] In July 2015, ICT Minister Supa Mandiwanzira dismissed the POTRAZ board over alleged corruption in what observers believe was a politically motivated move.[34]

Industry confidence in the egulator is low, resulting in public spats between POTRAZ and telecoms on various policy issues,[35] as exemplified by Econet s legal suit launched against POTRAZ in January 2016, which seeks USD 132 million in damages from POTRAZ for revenue losses incurred after the fi m was ordered to reduce its tariffs in 2014.[36] The privately-owned telecom alleges that the playing field was made une en by the directive to reduce tariffs, as well as a demand that Econet pay USD 137.5 million in license renewal fees while allowing its competitors Telecel and NetOne to continue operating without paying.[37] In its court papers, Econet is seeking the High Court to compel both Telecel and NetOne to pay license fees as well as POTRAZ to restore tariffs set out in Econet's license issued in 2013.

Limits on Content

WhatsApp was inaccessible for several hours during anti-government protests in July 2016 (outside the coverage period for FOTN scores), which were inspired by the #ThisFlag social media movement launched by Pastor Evan Mawawire's YouTube video in May. The draft National Policy for Information and Communications Technology (ICT) introduced in late 2015, if implemented, will seek to expand the government's reach on social media and potentially manipulate the online information landscape.

Blocking and Filtering

During this report's coverage period, no websites were blocked or fil ered in Zimbabwe and access to social media platforms such as Facebook, Twitter, and YouTube and international blog-hosting platforms were all freely available. However, on July 6, 2016, WhatsApp was reportedly inaccessible for nearly 5 hours during anti-government protests, leading to strong suspicions of government interference given the platform's widespread use by citizens to organize the protests.[38] While the government denied that it had blocked the service, sources in the telecoms sector confi med that they had received instructions from the government to shut down WhatsApp.[39]

The WhatsApp outage followed months of threats made by government officials o restrict social media, including President Mugabe who stated in early 2016 that his government would engage the

33 L.S.M. Kabweza, "POTRAZ now under Office f President & Cabinet. To improve regulatory independence," TechZim, October 15, 2013, http://www.techzim.co.zw/2013/10/telecoms-regulator-potraz-now-falls-under-office- f-president-and-cabinet/#.WBXjyOF946g

34 Munyoro, F., "POTRAZ Board fi ed over graft," The Herald, July 3, 2015, http://bit.ly/2fw4U7A

35 Nigel Gambanga, "POTRAZ hits back at Econet, dismisses allegations of unfair play," TechZim, June 7, 2016, http://www.techzim.co.zw/2016/06/potraz-hits-back-econet-dismisses-allegations-unfair-play/#.WBXocuF946g

36 Laiton,C., "Econet sues POTRAZ for 132 million," Newsday, January 14, 2016, https://www.newsday.co.zw/2016/01/14/econet-sues-potraz-for-132m/

37 Laiton,C., "Econet sues POTRAZ for 132 million," Newsday, January 14, 2016.

38 "Totalitarian Regime blocks WhatsApp," New Zimbabwe, July 6, 2016, http://www.newzimbabwe.com/news-30060-Totalitarian+regime+blocks+WhatsApp/news.aspx

39 Freedom House consultant interviews, May 2016.

Chinese government for assistance with fil ering the internet and blocking social media.[40] The ICT minister later stated in July 2016 that social media would not be regulated unless the need arose.[41]

Meanwhile, bulk text messages with political content are subject to censorship. Originally implemented in the lead-up to the 2013 elections,[42] a ban on bulk SMS services continues to obstruct the ability of civil society groups to send SMS messages on important issues or to mobilize,[43] and there are no mechanisms in place for appeal.[44]

Content Removal

There were no reported incidents of forced content removal of online content during the coverage period, though Zimbabwean government authorities have been known to pressure users and content producers to delete content from social media platforms. Most notably, the government is suspected of being behind the removal of the anonymous whistleblower Baba Jukwa's Facebook page in July 2014, but the manner in which it was removed remains shrouded in mystery.

Media, Diversity, and Content Manipulation

Zimbabwe's online landscape is vibrant, with Facebook, Google, Yahoo, and YouTube among the most popular websites with Zimbabwean internet users. Citizen journalism outlets such as @263 have become popular in informing citizen about important public affairs.[45] Youth activism groups include Magamba Network that fuses online activism with artistic expression and an online political satire show, Zambezi News.[46] Zambezi News broadcasts on YouTube and distributes its news content on compact discs (CDs).

The growth in social media use has prompted newspapers to work on integrating online platforms and developing social media strategies. For example, ALPHA media group publisher of *The Standard*, *Newsday*, *Southern Times* and *Zimbabwe Independent* have partnered with the telecom Econet to provide Mobinews, a mobile based news service for US$0.80 per week. A source in ALPHA media noted the platform has brought more revenue to the fi m than print advertisements, indicating a shift in the media model.

40 L.S.M. Kabweza, "Chinese style internet censorship coming to Zimbabwe – President Mugabe," TechZim, April 4, 2016, http://www.techzim.co.zw/2016/04/china-style-internet-censorship-coming-to-zimbabwe-president-mugabe/

41 Nigel Gambanga, "Minister of ICT says Zimbabwean government will consult citizens if need to regulate social media arises," TechZim, July 20, 2016, http://www.techzim.co.zw/2016/07/minister-ict-says-zimbabwean-government-will-consult-citizens-need-regulate-social-media-arises/#.WB-l6dzAVv5

42 Ephraim Batambuze III, "Bulk Text Messaging Service banded in Zimbabwe," PC Tech Magazine, July 29, 2013, http://bit.ly/1jISrvx; Gareth van Zyl, "Zimbabwean regulator 'blocks' bulk SMS as election nears," IT Web Africa, July 29, 2013, http://bit.ly/1RN8UdN; Kubatana, "POTRAZ bans bulk SMS," July 26, 2013, http://bit.ly/1QBgwzb.

43 According to Freedom House consultant interviews, May 2016.

44 One such ICT based Civic network Kubatana.net issued a statement stating that, "….in the run-up to Zimbabwe's 2013 election, our ability to send bulk text messages has been blocked. We have been informed by Econet that their regulator, Potraz, has issued a directive blocking the delivery of bulk messages from international gateways. "Potraz Bans Bulk SMSs," News Day, July 26, 2013, http://bit.ly/1Ga9G3k. See also, Brandon Gregory, "Zimbabwe Authorities Block Award Winning SMS Service for 'Political Reasons,'" Humanipo, July 30, 2013, http://www.humanipo.com/news/7611/Zimbabwe-authorities-block-award-winning-SMS-service-for-political-reasons/; Gareth van Zyl, "Zimbabwean regulator 'blocks' bulk SMS as election nears," ITWeb Africa, July 29, 2013, http://www.itwebafrica.com/ict-and-governance/273-zimbabwe/231381-zimbabwean-regulator-blocks-bulk-sms-as-election-nears#sthash.IwjQp075.dpuf

45 @263Chat's Twitter page: https://twitter.com/263Chat.

46 Magamba Network blog: http://www.povo.co.zw/blogs/magamba-network and YouTube page: https://www.youtube.com/watch?v=wvbQNWTu5yw

Despite the increasing diversity of local content, independent news websites and other digital media outlets based outside Zimbabwe continue to provide the most critical news and information, especially on sensitive topics that local media groups are afraid of covering. By contrast, local media outlets reporting on controversial issues are often met with attacks from state officials who th eaten to arrest or further legislate media operations. Popular online news sites include Newzimbabwe.com and NehandaRadio.com, which are used by local journalists and citizens to report on sensitive issues, often under the cover of pseudonyms.

Online self-censorship among Zimbabwean internet users remains high. Users even began to censor themselves on private messaging platforms such as WhatsApp following the arrest of several individuals for messages and images shared on the WhatsApp platform (see Prosecutions and Detentions for Online Activities).[47]

The draft National Policy for Information and Communications Technology (ICT) introduced in late 2015, if implemented, will seek to expand the government's reach on social media and potentially manipulate the online information landscape. In particular, section 18 of the draft on social networks includes a policy to "ensure availability of local capacity to snuff out undesirable social content."[48]

Digital Activism

Social media tools became a new political battle ground in Zimbabwe in the past year due to their wide availability and relative low cost of use on internet-enabled smart phones, which has allowed citizens to express themselves and criticize poor governance freely and easily. In particular, the communications platform WhatsApp became citizens' platform of choice for organizing and sharing information during the #ShutDownZim protests beginning in July 2016, leading the government to reportedly restrict access to WhatsApp for several hours and ramp up its threats to restrict social media in general. The protests were inspired by the #ThisFlag social media movement launched by Pastor Evan Mawarire[49] through his spoken word commentary that criticized Zimbabwe's current state of affairs in a YouTube video posted in April 2016.[50]

WhatsApp has also served as an important tool enabling organized civic activism, giving space for political activists and citizen journalists through private encrypted WhatsApp groups to share community information and strategies to influence local go ernment decisions. Residents' associations have also adopted WhatsApp as their key mobilizing platform on service delivery issues.

Violations of User Rights

Several individuals were arrested for online activities, particularly for WhatsApp messages that criticized aging President Mugabe. Intimidation and harassment was also prevalent. A draft cybercrime law introduced in August 2016 threatens to impede citizens' privacy and increase government surveillance.

47 "20 cops detained over WhatsApp chat," Chronicle, January 11, 2016, http://www.chronicle.co.zw/20-cops-detained-over-whatsapp-chat/

48 Zimbabwe National Policy for Information and Communications Technology (ICT), 2015, Section 18.1.

49 #ThisFlag E Mawarire Twitter page, https://twitter.com/PastorEvanLive

50 Dominic Mhiripiri, "Joining #ThisFlag? Use this App to Overlay Your FB Profile Pictu e," TechZim, May 13, 2016, http://www.techzim.co.zw/2016/05/thisflag- b-profile/#.V4Qff6I_Vdx

Legal Environment

Zimbabwe's existing media laws remain undemocratic, contradicting constitutional protections for the media, free expression, and access to information. In a landmark positive step, however, criminal defamation under the Criminal Law Codification and eform Act (CODE) was ruled unconstitutional on February 3, 2016,[51] indicating a judiciary with some level of independence and willingness to balance executive overreach.

A draft Computer Crime and Cybercrime Bill introduced in August 2016 raised alarms about potential new restrictions on Zimbabwe's internet freedom, particularly given its timing following widespread anti-government protests that were largely mobilized via social media and communications platforms in July. The current draft prohibits the publication and dissemination of pornography as well as racist and xenophobic material and penalizes the use of "electronic communication, with intent to coerce, intimidate, harass, or cause substantial emotional distress to a person" with a fine, prison of up to fi e years, or both,[52] which observers believe will be used to penalize government criticism on social media.[53] Provisions in the draft also intrude on citizens' right to privacy by authorizing interception, search, and seizure of electronic gadgets without sufficient o ersight to prevent abuse, which would further strengthen the government's surveillance capabilities (see Surveillance, Privacy, and Anonymity).[54]

Prosecutions and Detentions for Online Activities

Several individuals were arrested for their online activities during the coverage period, reflecting a marked increase compared to previous years. In October 2015, opposition party councilor in rural Bubi, Nduna Matshazi, was arrested for allegedly demeaning President Mugabe in a WhatsApp message to a private chat group with other regional councilors. One of the councilors belonging to the ruling ZANU-PF party reported his message to the police.[55] His case remains open as of October 2016.

In April 2016, Ernest Matsapa, a government employee in Nyanga, was also arrested for his WhatsApp messages, in particular audio and images that allegedly depicted President Mugabe as too old and a burden to the people in a private chat group called "Nyanga Free Range." Matsapa was accused of denigrating Mugabe and charged with "criminal nuisance" under the Criminal Codification Act [56] If convicted, he faces up to six months in prison; his trial is ongoing as of October 2016.[57]

On April 7, 2016 Media Centre Director Earnest Mudzengi was detained for 8 hours and questioned

51 "Con-Court outlaws criminal defamation," The Herald, February 4, 2016, http://www.herald.co.zw/concourt-outlaws-criminal-defamation/

52 Computer Crime and Cybercrime Bill (July 2013 draft), Sections 15, 17, 18, 23.

53 Paul Kaseke, "Zim's cyber laws – Going nowhere quickly," Newsday, August 25, 2016, https://www.newsday.co.zw/2016/08/25/zims-cyber-laws-going-nowhere-quickly/

54 Paul Kaseke, "Zim's cyber laws – Going nowhere quickly," Newsday, August 25, 2016.

55 Masara,W. "MDC-T official nabbed for WhatsApp P esident slur," The Chronicle, October 3, 2015, http://www.chronicle.co.zw/mdc-t-official-nabbed-fo -whatsapp-president-slur/

56 Blessing Zulu, "Zimbabwe Intensifies Crac down on Facebook, WhatsApp Messages 'Insulting' Mugabe," Voice of America, April 4, 2016, http://www.voazimbabwe.com/a/zimbabwe-mugabe-insult/3268562.html

57 "Zimbabwe social media surveillance's latest victim," The Zimbabwe Mail, April 6, 2016, http://thezimbabwemail.com/scie-tech-21317-zimbabwe-social-media-surveillances-latest-victim.html

over an online story published by *Zimbabwe Sentinel* news website run by the Media Centre that reported about a plot to bomb President Robert Mugabe's dairy farm and factory.[58] The following day, *Zimbabwe Sentinel* writers Malvern Mkudu and Mlondolozi Ndlovu were also questioned for hours about the same story, though no charges were pressed on the three journalists.

During the July 2016 anti-government protests, the government became more brazen and open about its disdain for social media activities. On July 6, the telecoms regulator POTRAZ issued a statement threatening to arrest individuals for "social media abuse," indicating that since mobile phone cards are registered with the regulator, security agents could easily track those sharing protest messages.[59]

Shortly after, police arrested Pastor Evan Mawarire on July 12, whose #ThisFlag social media movement inspired the widespread protests, on allegations of inciting public violence, but his charge was amended to subversion when he appeared before the courts.[60] The courts dismissed his case on July 13 over a technicality, though widespread international attention and the popular #FreePastorEvan social media campaign may have played a role.[61] At the time of writing, the police were reportedly still interested in arresting and charging Mawarire, though he had left the country shortly after his release, reportedly out of concerns for his safety.[62]

Meanwhile, in June 2015, the government withdrew charges against University of Zimbabwe student Romeo Musemburi who was arrested in June 2014 based on accusations of running the Facebook page of the anonymous whistleblower Baba Jukwa and charged with "attempting acts of insurgency, banditry, and sabotage."[63] The withdrawal put an end to the saga surrounding Baba Jukwa, who had captivated Zimbabwe in 2013-2014 and marked the government's fi st confrontation with social media activism, though the affair left a chilling effect on critical speech online.

An interesting/positive development saw a perpetrator of sexual crimes in Zimbabwe arrested after the images had gone viral on WhatApp[64].

Surveillance, Privacy, and Anonymity

Unchecked government surveillance has been a persistent concern in Zimbabwe, and several legal provisions may allow the government to conduct surveillance without respect for the Necessary

58 Kandemiri, J. "Zimbabwean in Trouble over Gushungo Dairy bombing story," Voice of America, April 7, 2016, http://www.voazimbabwe.com/a/zimbabwe-politics-police-media-centre-mudzendi-zimbabwe-sentinel/3275013.html

59 "We are therefore warning members of the public that from the date of this notice, any person caught in possession of, generating, sharing or passing on abusive, threatening, subversive or offensive telecommunication messages, including WhatsApp or any other social media messages that may be deemed to cause despondency, incite violence, threaten citizens and cause unrest, will be arrested and dealt with accordingly in the national interest," read the POTRAZ statement. See, Gambanga, N. "Zimbabwe Government warning on social media," TechZim, July 6, 2016, http://www.techzim.co.zw/2016/07/heres-zimbabwean-governments-warning-social-media-abuse/#.V4ezvFR97IU

60 MacDonald Dzirutwe, "#ThisFlag: Zimbabwean pastor Evan Mawarire released from police custody," Mail & Guardian, July 13, 2016, http://mg.co.za/article/2016-07-12-thisflag- astor-evan-mawarire-summoned-by-zimbabwean-police

61 Columbus Mavhunga et al., "Mugabe speaks out against #ThisFlag pastor Evan Mawarire," CNN, July 19, 2016, http://www.cnn.com/2016/07/06/africa/zimbabwe-shut-down/

62 Patricia Mudadigwa, "Has Pastor Evan Mawarire of #ThisFlag Abandoned Zimbabweans?" Voice of America, August 16, 2016, http://www.voazimbabwe.com/a/zimbabwe-evan-mawarire-exile/3467647.html

63 The state did not give reasons for withdrawing charges. See, Machakaire, T. "Student freed in Baba Jukwa saga," Nehanda Radio, June 28, 2015, http://bit.ly/2fw5yC5

64 Arron Nyamayaro, "WhatsApp sexual abuse suspect arrested," H-Metro, June 22, 2016, http://hmetro.co.zw/whatsapp-sexual-abuse-suspect-arrested/

and Proportionate Principles—international guidelines that apply human rights law to monitoring technologies.[65]

The Post and Telecommunications Act of 2000 allows the government to intercept suspicious communications and requires a telecommunications licensee, such as an ISP, to supply information to government officials upon equest.[66] The act also obligates telecoms to report any communications with "offensive" or "threatening" content.

The Interception of Communications Act of 2007 established a Monitoring of Interception of Communications Center that has the power to oversee traffic in all elecommunications services and to intercept phone calls, emails, and faxes under the pretext of national security, though it is uncertain whether the center is operating.[67] Section 9 of the act requires telecommunications operators and ISPs to install necessary surveillance technology at their own expense and to intercept information on the state's behalf.[68] Failure to comply is punishable with a fine and sen ence of up to three years in prison. Warrants allowing the monitoring and interception of communications are issued by the minister of information at his/her discretion; consequently, there is no adequate judicial oversight or other independent safeguard against abuse,[69] and the extent and frequency of monitoring remains unknown.

The draft National Policy for Information and Communications Technology (ICT) introduced in late 2015 put forth an ambitious set of policies that, if implemented, would provide the government with the ability to shut down networks or block websites as well as strengthen its surveillance capabilities through centralized control over the country's internet (see Restrictions on Connectivity). In October 2015, Portnet Software—an IT company that provides security solutions for various sectors and in which the government has a 51 percent share—reportedly upgraded its capacity to help the government intercept and analyze ICT communications.[70] IT experts saw the move as part of efforts to facilitate the implementation of the draft National Policy.[71]

Anonymous communication and user data are compromised by SIM card registration regulations implemented in 2011, which require mobile phone users to submit personal identity details to mobile operators, ostensibly to combat crime and curtail threatening or obscene communications.[72] Under the 2013 Postal and Telecommunications (Subscriber Registration) Regulations, subscribers are required to register with all telecommunications service providers with details including a full name, permanent residential address, nationality, gender, subscriber ID number, and national ID or

65 Necessary and Proportionate principles: https://necessaryandproportionate.org/about

66 Postal and Telecommunications Act 2000, Part XII, Section 98, "Interception of communications," http://www.potraz.gov.zw/files/_ostal_Act.pdf

67 Reporters Without Borders, "All Communications Can Now be Intercepted Under New Law Signed by Mugabe," news release, August 6, 2007, http://en.rsf.org/zimbabwe-all-communications-can-now-be-06-08-2007,17623.html. The law is available at http://www.vertic.org/media/National%20Legislation/Zimbabwe/ZW_Interception_of_Communications_Act.pdf

68 Interception of Communications Act, No. 6/2007, Section 9, "Assistance by service providers."

69 Interception of Communications Act, No. 6/2007, Section 6, "Issue of warrant."

70 Ndebele. H. "Gvt hones spying tools," Zimbabwe Independent, October 9, 2015, http://www.theindependent.co.zw/2015/10/09/govt-hones-spying-tools/

71 Ndebele, H. "Gvt sharpens spying tools," Zimbabwe Independent, January 8, 2016, http://www.theindependent.co.zw/2016/01/08/govt-sharpens-spying-tools/

72 "POTRAZ Issues Mobile Phone Registration Reminder," Technology Zimbabwe, January 31, 2011, http://www.techzim.co.zw/2011/01/potraz-registration-reminder/

passport number.[73] Network operators are then required to retain such personal information for fi e years *after* either the subscriber or operator, has discontinued service. The subscriber registration regulations also require ISPs to provide POTRAZ with copies of their subscriber registers to be stored in a Central Subscriber Information Database to enable POTRAZ to "assist law enforcement agencies on safeguarding national security," among other aims.[74]

A 2014 amendment to the regulations requires law enforcement agents to obtain a court order or a warrant to request information from the central database,[75] which some analysts worry falls short of judicial oversight since a warrant "can be issued by police office s who have been designated as justices of the peace."[76] Following the law's enactment in April 2015, the Zimbabwe Internet Services Providers Association released a statement stating that none of its members would participate in email surveillance, though penalties for breaching the new law include both fines and imprisonment.

To comply with the SIM card registration requirements, Econet disconnected one million of its subscribers in November 2015.[77] During the registration process, the telecom was reportedly pressured to verify subscriber details with the government Registrar General's offic .[78]

Intimidation and Violence

Online journalists and ICT users often faced harassment, intimidation, and violence for their online activities in the past year. During the July 2016 anti-government protests, journalists were reportedly arrested and forced to delete images covering the demonstrations as part of an effort to suppress reporting and sharing of information via social media.[79]

WhatsApp group conversations became the subject of increasing scrutiny for critical content. In January 2016, 20 junior police office s were questioned and suspended over a WhatsApp group they had created to discuss concerns over the delayed payment of their salaries and end of year bonuses,[80] which was reportedly leaked to the police authorities. Alongside increasing arrests for WhatsApp messages (see Prosecutions and Detentions for Online Activities), the suspension resulted in a chilling effect among users of the platform.

In an unfortunate case, journalist/cum activist Itai Dzamara, who was abducted in March 2015 near his home in Harare,[81] remains missing as of October 2016.[82] Dzamara was known for his leadership

73 Garikai Dzoma, "Zimbabwe's new online spying law," TechZim, October 9, 2013, http://www.techzim.co.zw/2013/10/zimbabwes-new-online-spying-law/; Postal and Telecommunications (Subscriber Registration) Regulations, 2013, (Statutory Instrument 142/2013), https://docs.google.com/file/d/0B006T_7m0f19NTR2b1BsZjZza2s/edi

74 Postal and Telecommunications (Subscriber Registration) Regulations, 2013, (Statutory Instrument 142/2013), Section 8 (1) and (2).

75 Postal and Telecommunications (Subscriber Registration) Regulations, 2014, http://www.cfuzim.org/images/si9514.pdf.

76 "Bill Watch 29/2014 of 21st July," The Zimbabwean, July 22, 2014, http://bit.ly/1Gae1nc

77 Lovemore Meya, "Econet disconnects 1 million subscribers," The Herald, November 16, 2015, http://www.herald.co.zw/econet-disconnects-1-million-subscribers/

78 Meya,L. "Econet disconnects 1 Million subscribers," The Herald, November 16, 2015, http://www.herald.co.zw/econet-disconnects-1-million-subscribers/

79 Privilege Musvanhiri, Twitter post, July 6, 2016, https://twitter.com/Musvanhiri/status/750673802716119040

80 "20 Cops detained over WhatsApp chat." The Chronicle, January 11, 2016.

81 "Human Rights Watch: 61 Days: Police doing nothing about Dzamara," Nehanda Radio, May 9, 2015, http://nehandaradio.com/2015/05/09/61-days-police-doing-nothing-about-dzamara/

82 About Itai Dzamara, Pindula, http://www.pindula.co.zw/Itai_Dzamara

of the anti-government "Occupy Africa Unity Square" protest group organized on Facebook and had received numerous threats from state security agents for his activism prior to his disappearance.[83]

Technical Attacks

There were no technical attacks against government critics, online news outlets, or human rights organizations reported during the coverage period. In February 2016, a hacktivist group identifying itself as Anon hacked Zimbabwe's parliament website.[84] The ruling party ZANU PF also had its website hacked and pulled down twice in 2016,[85] while the state broadcaster Zimbabwe Broadcast Corporation (ZBC) and the regulator POTRAZ had their websites shutdown by hackers in July 2016, apparently as retribution for the government's alleged blocking of WhatsApp amid antigovernment protests (see Blocking and Filtering).[86]

83 Occupy Africa Unity Square, Facebook Page, http://on.fb.me/1OznpUe

84 "Hackers attack parliament website," Newsday, February 8, 2016, https://www.newsday.co.zw/2016/02/08/hackers-attack-parliament-website/

85 Abdur Rahman Alfa Shaban, "Anonymous Africa hacks websites of 'racist' EFF and ZANU PF," Africa News, June 14, 2016, http://www.africanews.com/2016/06/14/anonymous-africa-hacks-websites-of-racist-eff-and-zanu-pf/

86 "Mugabe Party & Govt Websites Shut Down By Hackers As Punishment For Whatsapp Ban," The Southern Daily, July 6, 2016, http://thesoutherndaily.co.zw/2016/07/06/zanu-zim-govt-hacked/

Methodology

Freedom on the Net provides analytical reports and numerical scores for 65 countries worldwide. Assigning scores allows for comparative analysis among the countries surveyed and facilitates an examination of trends over time. The accompanying country reports provide narrative detail to support the scores.

The countries were chosen to provide a representative sample with regards to geographical diversity and economic development, as well as varying levels of political and media freedom. The numerical ratings and reports included in this study particularly focus on developments that took place between June 1, 2015 and May 31, 2016, although the analysis in the Key Internet Controls graph and the Topics Censored table covers developments through the end of September, when this year's edition was sent to press.

Freedom on the Net is a collaborative effort between a small team of Freedom House staff and an extensive network of local researchers and advisors in 65 countries. Our in-country researchers have diverse backgrounds—academia, blogging, traditional journalism, and tech— and track developments from their country of expertise. In the most repressive environments, Freedom House takes care to ensure researchers' anonymity or, in exceptional cases, works with individuals living outside their home country.

What We Measure

The *Freedom on the Net* index measures each country's level of internet and digital media freedom based on a set of methodology questions developed in consultation with international experts to capture the vast array of relevant issues that enable internet freedom (see "Checklist of Questions"). Given increasing technological convergence, the index also measures access and openness of other digital means of transmitting information, particularly mobile phones and text messaging services.

Freedom House does not maintain a culture-bound view of freedom. The project methodology is grounded in basic standards of free expression, derived in large measure from Article 19 of the Universal Declaration of Human Rights:

> "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media regardless of frontiers."

This standard applies to all countries and territories, irrespective of geographical location, ethnic or religious composition, or level of economic development.

The project particularly focuses on the transmission and exchange of news and other politically relevant communications, as well as the protection of users' rights to privacy and freedom from both legal and extralegal repercussions arising from their online activities. At the same time, the index acknowledges that in some instances freedom of expression and access to information may be legitimately restricted. The standard for such restrictions applied in this index is that they be implemented only in narrowly defined circumstances and in line with international human rights standards, the rule of law, and the principles of necessity and proportionality. As much as possible, censorship and surveillance policies and procedures should be transparent and include avenues for appeal available to those affected.

The index does not rate governments or government performance per se, but rather the real-world rights and freedoms enjoyed by individuals within each country.

While digital media freedom may be primarily affected by state actions, pressures and attacks by nonstate actors, including the criminal underworld, are also considered. Thus, the index ratings generally reflect the interplay of a variety of actors, both governmental and nongovernmental, including private corporations.

The Scoring Process

The methodology includes 21 questions and nearly 100 subquestions, divided into three categories:

- **Obstacles to Access** details infrastructural and economic barriers to access, legal and ownership control over internet service providers , and independence of regulatory bodies;
- **Limits on Content** analyzes legal regulations on content, technical filtering and blocking of websites, self-censorship, the vibrancy and diversity of online news media, and the use of digital tools for civic mobilization;
- **Violations of User Rights** tackles surveillance, privacy, and repercussions for online speech and activities, such as imprisonment, extralegal harassment, or cyberattacks.

Each question is scored on a varying range of points. The subquestions guide researchers regarding factors they should consider while evaluating and assigning points, though not all apply to every country. Under each question, a lower number of points is allotted for a more free situation, while a higher number of points is allotted for a less free environment. Points add up to produce a score for each of the subcategories, and a country's total points for all three represent its final score (0-100). Based on the score, Freedom House assigns the following internet freedom ratings:

- Scores 0-30 = Free
- Scores 31-60 = Partly Free
- Scores 61-100 = Not Free

After researchers submitted their draft scores in 2016, Freedom House convened five regional review meetings and numerous international conference calls, attended by Freedom House staff and over 70 local experts, scholars, and civil society representatives from the countries under study. During the meetings, participants reviewed, critiqued, and adjusted the draft scores—based on set coding guidelines—through careful consideration of events, laws, and practices relevant to each item. After completing the regional and country consultations, Freedom House staff did a final review of all scores to ensure their comparative reliability and integrity.

Key Internet Controls Explained

In the Key Internet Controls Table (page 15), Freedom House documented how governments censor and control the digital sphere. Each colored cell represents at least one occurrence of the cited control during the report's coverage period of June 2015 to May 2016; colored cells with an asterisk (*) represent events that occurred from June until the time of writing (September 2016). Incidents are based on *Freedom on the Net* research and verified by in-country researchers. The Key Internet Controls reflect restrictions on content of political, social, or religious nature.

- **Social media or communications apps blocked:** Entire apps or key functions of social media, messaging, and calling platforms temporarily or permanently blocked to prevent communication and information sharing.
- **Political, social, or religious content blocked:** Blocking or filtering of domains, URLs, or keywords, to limit access to specific political, social, or religious content.
- **Localized or nationwide ICT shutdown:** Intentional disruption of internet or cellphone networks in

response to political or social events, whether temporary or long term, localized or nationwide.

- **Progovernment commentators manipulate online discussions:** Strong indications that individuals are paid to distort the digital information landscape in the government's favor, without acknowledging sponsorship.
- **New law or directive increasing censorship or punishment passed:** Any legislation adopted or amended during the coverage period, or any directive issued, to censor or punish legitimate online activity.
- **New law or directive increasing surveillance or restricting anonymity passed:** Any legislation adopted or amended during the coverage period, or any directive issued, to surveil or expose the identity of citizens using the internet with legitimate intent.
- **Blogger or ICT user arrested, imprisoned, or in prolonged detention for political or social content:** Any arrest, prosecution, detention that is credibly perceived to be in reprisal for digital expression, including trumped up charges. Brief detentions for interrogation are not reflected.
- **Blogger or ICT user physically attacked or killed (including in custody):** Any physical attack, kidnapping, or killing that is credibly perceived to be in reprisal for digital expression. This includes attacks while in custody, such as torture.
- **Technical attacks against government critics or human rights organizations:** Cyberattacks against human rights organizations, news websites, and individuals sharing information perceived as critical, with the clear intent of disabling content or exposing user data, and motives that align with those of agencies that censor and surveil the internet. Targets of attacks considered here may include critics in exile, but not transnational cyberattacks, even with political motives.

Censored Topics by Country Explained

In the Censored Topics by Country graphic (page 10), Freedom House staff documented a selection of topics that were subject to censorship in the 65 countries covered. Countries were included if state authorities blocked or ordered the removal of content, or detained or fined users for posting content on the topics considered. The chart does not consider extralegal pressures like violence, self-censorship, or cyberattacks, even where the state is believed to be responsible. To capture a comprehensive data set, the chart includes incidents over a two-year span, between June 2014 and September 2016, and distinguishes between pervasive and sporadic censorship. All data is based on *Freedom on the Net* research and verified by in-country researchers.

- **Criticism of the Authorities:** Content perceived as criticism of the state or its representatives, including the government, military, ruling family, police, judiciary, or other officials.
- **Political Opposition:** Content affiliated with political groups or opponents, including in the diaspora.
- **Corruption:** Accusations or exposés of corruption or misuse of public funds.
- **Blasphemy:** Content perceived as insulting or offending religion.
- **Mobilization for Public Causes:** Calls to protest or campaigns on political, social, or human rights issues.
- **Satire:** Humorous or ironic commentary on political or social issues.
- **Ethnic and Religious Minorities:** Content related to marginalized groups, including ethnic and religious minorities.
- **LGBTI Issues:** Content related to lesbian, gay, bisexual, transgender, or intersex individuals.
- **Conflict:** Discussion or reporting on local or international instances of violence, conflict, or terrorism.
- **Social Commentary:** Content that is not overtly political, including on economic, environmental, cultural, or educational issues.

Checklist of Questions

- Each country is ranked on a scale of 0 to 100, with 0 being the best and 100 being the worst.
- A combined score of 0-30=Free, 31-60=Partly Free, 61-100=Not Free.

A. OBSTACLES TO ACCESS (0-25 POINTS)

1. To what extent do infrastructural limitations restrict access to the internet and other ICTs? (0-6 points)

- Does poor infrastructure (electricity, telecommunications, etc.) limit citizens' ability to receive internet in their homes and businesses?
- To what extent is there widespread public access to the internet through internet cafes, libraries, schools and other venues?
- To what extent is there internet and mobile phone access, including data connections or satellite?
- Is there a significant difference between internet and mobile phone penetration and access in rural versus urban areas or across other geographical divisions?
- To what extent are broadband services widely available in addition to dial-up?

2. Is access to the internet and other ICTs prohibitively expensive or beyond the reach of certain segments of the population? (0-3 points)

- In countries where the state sets the price of internet access, is it prohibitively high?
- Do financial constraints, such as high costs of telephone/internet services or excessive taxes imposed on such services, make internet access prohibitively expensive for large segments of the population?
- Do low literacy rates (linguistic and "digital literacy") limit citizens' ability to use the internet?
- Is there a significant difference between internet penetration and access across ethnic or socioeconomic societal divisions?
- To what extent are online software, news, and other information available in the main local languages spoken in the country?

3. Does the government impose restrictions on ICT connectivity and access to particular social media and communication apps permanently or during specific events? (0-6 points)

- Does the government place limits on the amount of bandwidth that access providers can supply?
- Does the government use control over internet infrastructure (routers, switches, etc.) to limit connectivity, permanently or during specific events?
- Does the government centralize telecommunications infrastructure in a manner that could facilitate control of content and surveillance?
- Does the government block protocols and tools that allow for instant, person-to-person communication (VOIP, instant messaging, text messaging, etc.), particularly those based outside the country (e.g. Skype, WhatsApp, etc)?
- Does the government block protocols, social media, and/or communication apps that allow for information sharing or building online communities (video-sharing, social-networking sites, comment features, blogging platforms, etc.) permanently or during specific events?
- Is there blocking of certain tools that enable circumvention of online filters and censors?

4. Are there legal, regulatory, or economic obstacles that prevent the existence of diverse business entities providing access to digital technologies? (0-6 points)

Note: Each of the following access providers are scored separately:

1a. Internet service providers (ISPs) and other backbone internet providers (0-2 points)

1b. Cybercafes and other businesses entities that allow public internet access (0-2 points)

1c. Mobile phone companies (0-2 points)

- Is there a legal or de facto monopoly over access providers or do users have a choice of access provider, including ones privately owned?
- Is it legally possible to establish a private access

provider or does the state place extensive legal or regulatory controls over the establishment of providers?
- Are registration requirements (i.e. bureaucratic "red tape") for establishing an access provider unduly onerous or are they approved/rejected on partisan or prejudicial grounds?
- Does the state place prohibitively high fees on the establishment and operation of access providers?

5. To what extent do national regulatory bodies overseeing digital technology operate in a free, fair, and independent manner? (0-4 points)
- Are there explicit legal guarantees protecting the independence and autonomy of any regulatory body overseeing internet and other ICTs (exclusively or as part of a broader mandate) from political or commercial interference?
- Is the process for appointing members of regulatory bodies transparent and representative of different stakeholders' interests?
- Are decisions taken by the regulatory body, particularly those relating to ICTs, seen to be fair and apolitical and to take meaningful notice of comments from stakeholders in society?
- Are efforts by access providers and other internet-related organizations to establish self-regulatory mechanisms permitted and encouraged?
- Does the allocation of digital resources, such as domain names or IP addresses, on a national level by a government-controlled body create an obstacle to access or are they allocated in a discriminatory manner?

B. LIMITS ON CONTENT (0-35 POINTS)

1. To what extent does the state or other actors block or filter internet and other ICT content, particularly on political and social issues? (0-6 points)
- Is there significant blocking or filtering of internet sites, web pages, blogs, or data centers, particularly those related to political and social topics?
- Is there significant filtering of text messages or other content transmitted via mobile phones?
- Do state authorities block or filter information and views from inside the country—particularly concerning human rights abuses, government corruption, and poor standards of living—from reaching the outside world through interception of email or text messages, etc?
- Are methods such as deep-packet inspection used for the purposes of preventing users from accessing certain content or for altering the content of communications en route to the recipient, particularly with regards to political and social topics?

2. To what extent does the state employ legal, administrative, or other means to force deletion of particular content, including requiring private access providers to do so? (0-4 points)
- To what extent are non-technical measures—judicial or extra-legal—used to order the deletion of content from the internet, either prior to or after its publication?
- To what degree do government officials or other powerful political actors pressure or coerce online news outlets to exclude certain information from their reporting?
- Are access providers and content hosts legally responsible for the information transmitted via the technology they supply or required to censor the content accessed or transmitted by their users?
- Are access providers or content hosts prosecuted for opinions expressed by third parties via the technology they supply?

3. To what extent are restrictions on internet and ICT content transparent, proportional to the stated aims, and accompanied by an independent appeals process? (0-4 points)
- Are there national laws, independent oversight bodies, and other democratically accountable procedures in place to ensure that decisions to restrict access to certain content are proportional to their stated aim?
- Are state authorities transparent about what content is blocked or deleted (both at the level of public policy and at the moment the censorship occurs)?
- Do state authorities block more types of content than they publicly declare?
- Do independent avenues of appeal exist for those

who find content they produced to have been subjected to censorship?

4. Do online journalists, commentators, and ordinary users practice self-censorship? (0-4 points)

- Is there widespread self-censorship by online journalists, commentators, and ordinary users in state-run online media, privately run websites, or social media applications?
- Are there unspoken "rules" that prevent an online journalist or user from expressing certain opinions in ICT communication?
- Is there avoidance of subjects that can clearly lead to harm to the author or result in almost certain censorship?

5. To what extent is the content of online sources of information determined or manipulated by the government or a particular partisan interest? (0-4 points)

- To what degree do government officials or other powerful actors pressure or coerce online news outlets to follow a particular editorial direction in their reporting?
- Do authorities issue official guidelines or directives on coverage to online media outlets, blogs, etc., including instructions to marginalize or amplify certain comments or topics for discussion?
- Do government officials or other actors bribe or use close economic ties with online journalists, bloggers, website owners, or service providers in order to influence the online content they produce or host?
- Does the government employ, or encourage content providers to employ, individuals to post pro-government remarks in online bulletin boards and chat rooms?
- Do online versions of state-run or partisan traditional media outlets dominate the online news landscape?

6. Are there economic constraints that negatively impact users' ability to publish content online or online media outlets' ability to remain financially sustainable? (0-3 points)

- Are favorable connections with government officials necessary for online media outlets or service providers (e.g. search engines, email applications, blog hosting platforms, etc.) to be economically viable?
- Are service providers who refuse to follow state-imposed directives to restrict content subject to sanctions that negatively impact their financial viability?
- Does the state limit the ability of online media to accept advertising or investment, particularly from foreign sources, or does it limit advertisers from conducting business with disfavored online media or service providers?
- To what extent do ISPs manage network traffic and bandwidth availability to users in a manner that is transparent, evenly applied, and does not discriminate against users or producers of content based on the content/source of the communication itself (i.e. respect "net neutrality" with regard to content)?
- To what extent do users have access to free or low-cost blogging services, webhosts, etc. to allow them to make use of the internet to express their own views?

7. To what extent are sources of information that are robust and reflect a diversity of viewpoints readily available to citizens, despite government efforts to limit access to certain content? (0-4 points)

- Are people able to access a range of local and international news sources via the internet or text messages, despite efforts to restrict the flow of information?
- Does the public have ready access to media outlets or websites that express independent, balanced views?
- Does the public have ready access to sources of information that represent a range of political and social viewpoints?
- To what extent do online media outlets and blogs represent diverse interests within society, for example through websites run by community organizations or religious, ethnic and other minorities?
- To what extent do users employ proxy servers and other methods to circumvent state censorship efforts?

8. To what extent have individuals successfully used the internet and other ICTs as sources of informa-

tion and tools for mobilization, particularly regarding political and social issues? To what extent are such mobilization tools available without government restriction? (0-6 points)

- To what extent does the online community cover political developments and provide scrutiny of government policies, official corruption, or the behavior of other powerful societal actors?
- To what extent are online communication tools or social networking sites (e.g. Twitter, Facebook) used as a means to organize politically, including for "real-life" activities?
- Are mobile phones and other ICTs used as a medium of news dissemination and political organization, including on otherwise banned topics?

C. VIOLATIONS OF USER RIGHTS (0-40 POINTS)

1. To what extent does the constitution or other laws contain provisions designed to protect freedom of expression, including on the internet, and are they enforced? (0-6 points)

- Does the constitution contain language that provides for freedom of speech and of the press generally?
- Are there laws or legal decisions that specifically protect online modes of expression?
- Are online journalists and bloggers accorded the same rights and protections given to print and broadcast journalists?
- Is the judiciary independent and do the Supreme Court, Attorney General, and other representatives of the higher judiciary support free expression?
- Is there implicit impunity for private and/or state actors who commit crimes against online journalists, bloggers, or other citizens targeted for their online activities?

2. Are there laws which call for criminal penalties or civil liability for online and ICT activities? (0-4 points)

- Are there specific laws criminalizing online expression and activity such as posting or downloading information, sending an email, or text message, etc.? (Note: this excludes legislation addressing harmful content such as child pornography or activities such as malicious hacking)
- Do laws restrict the type of material that can be communicated in online expression or via text messages, such as communications about ethnic or religious issues, national security, or other sensitive topics?
- Are restrictions of internet freedom closely defined, narrowly circumscribed, and proportional to the legitimate aim?
- Are vaguely worded penal codes or security laws applied to internet-related or ICT activities?
- Are there penalties for libeling officials or the state in online content?
- Can an online outlet based in another country be sued if its content can be accessed from within the country (i.e. "libel tourism")?

3. Are individuals detained, prosecuted or sanctioned by law enforcement agencies for disseminating or accessing information on the internet or via other ICTs, particularly on political and social issues? (0-6 points)

- Are writers, commentators, or bloggers subject to imprisonment or other legal sanction as a result of posting material on the internet?
- Are citizens subject to imprisonment, civil liability, or other legal sanction as a result of accessing or downloading material from the internet or for transmitting information via email or text messages?
- Does the lack of an independent judiciary or other limitations on adherence to the rule of law hinder fair proceedings in ICT-related cases?
- Are individuals subject to abduction or arbitrary detention as a result of online activities, including membership in certain online communities?
- Are penalties for "irresponsible journalism" or "rumor mongering" applied widely?
- Are online journalists, bloggers, or others regularly prosecuted, jailed, or fined for libel or defamation (including in cases of "libel tourism")?

4. Does the government place restrictions on anonymous communication or require user registration? (0-4 points)

- Are website owners, bloggers, or users in general required to register with the government?
- Are users able to post comments online or purchase mobile phones anonymously or does the government require that they use their real names

or register with the government?
- Are users prohibited from using encryption software to protect their communications?
- Are there laws restricting the use of encryption and other security tools, or requiring that the government be given access to encryption keys and algorithms?

5. To what extent is there state surveillance of internet and ICT activities without judicial or other independent oversight, including systematic retention of user traffic data? (0-6 points)
- Do the authorities regularly monitor websites, blogs, and chat rooms, or the content of email and mobile text messages?
- To what extent are restrictions on the privacy of digital media users transparent, proportional to the stated aims, and accompanied by an independent process for lodging complaints of violations?
- Where the judiciary is independent, are there procedures in place for judicial oversight of surveillance and to what extent are these followed?
- Where the judiciary lacks independence, is there another independent oversight body in place to guard against abusive use of surveillance technology and to what extent is it able to carry out its responsibilities free of government interference?
- Is content intercepted during internet surveillance admissible in court or has it been used to convict users in cases involving free speech?

6. To what extent are providers of access to digital technologies required to aid the government in monitoring the communications of their users? (0-6 points)

Note: Each of the following access providers are scored separately:

6a. Internet service providers (ISPs) and other backbone internet providers (0-2 points)

6b. Cybercafes and other business entities that allow public internet access (0-2 points)

6c. Mobile phone companies (0-2 points)
- Are access providers required to monitor their users and supply information about their digital activities to the government (either through technical interception or via manual monitoring, such as user registration in cybercafes)?
- Are access providers prosecuted for not doing so?
- Does the state attempt to control access providers through less formal methods, such as codes of conduct?
- Can the government obtain information about users without a legal process?

7. Are bloggers, other ICT users, websites, or their property subject to extralegal intimidation or physical violence by state authorities or any other actor? (0–5 points)
- Are individuals subject to murder, beatings, harassment, threats, travel restrictions, or torture as a result of online activities, including membership in certain online communities?
- Do armed militias, organized crime elements, insurgent groups, political or religious extremists, or other organizations regularly target online commentators?
- Have online journalists, bloggers, or others fled the country or gone into hiding to avoid such action?
- Have cybercafes or property of online commentators been targets of physical attacks or the confiscation or destruction of property as retribution for online activities or expression?

8. Are websites, governmental and private entities, ICT users, or service providers subject to widespread "technical violence," including cyberattacks, hacking, and other malicious threats? (0-3 points)
- Are financial, commercial, and governmental entities subject to significant and targeted cyberattacks (e.g. cyberespionage, data gathering, DDoS attacks), including those originating from outside of the country?
- Have websites belonging to opposition or civil society groups within the country's boundaries been temporarily or permanently disabled due to cyberattacks, particularly at politically sensitive times?
- Are websites or blogs subject to targeted technical attacks as retribution for posting certain content (e.g. on political and social topics)?
- Are laws and policies in place to prevent and protect against cyberattacks (including the launching of systematic attacks by nonstate actors from within the country's borders) and are they enforced?

Contributors

Freedom House Research Team

- Sanja Kelly, Director, *Freedom on the Net*
- Mai Truong, Program Manager (Africa)
- Adrian Shahbaz, Research Manager (MENA)
- Madeline Earp, Senior Research Analyst (Asia)
- Jessica White, Research Analyst (Latin America & EU)
- Rose Dlougatch, Senior Research Associate (Eurasia)

Report Authors and Advisors

- **Argentina:** Eduardo Ferreyra, Valeria Milanes, Jeannette Torrez, Leandro Ucciferri, Free Expression & Privacy team, Association for Civil Rights (ADC)
- **Armenia:** Artur Papyan, Internet Journalist at RFE/RL and media development consultant
- **Australia:** Dr. Alana Maurushat, Senior Lecturer, Faculty of Law, and Co-Director, Cyberspace Law and Policy Community, The University of New South Wales
- **Azerbaijan:** Arzu Geybulla, Azerbaijani journalist
- **Brazil:** Fabrício Bertini Pasquot Polido, Professor, Law School of the Federal University of Minas Gerais, and Head of the Center for International Studies on Internet, Innovation, and Intellectual Property (GNET); Carolina Rossini, Vice President of International Policy, Public Knowledge, and Board Member, Open Knowledge Foundation, InternetLab, and CodingRights
- **Cambodia:** Sopheap Chak, Executive Director, Cambodian Center for Human Rights, and human rights blogger
- **Canada:** Allen Mendehlson, Canadian lawyer specializing in internet and technology law
- **Colombia:** Law, Internet, and Society Group, Fundación Karisma
- **Cuba:** Ernesto Hernández Busto, Cuban journalist and writer
- **Estonia:** Linnar Viik, Lecturer, Board Member, Estonian IT College
- **France:** Jean-Loup Richet, Researcher, University of Nantes
- **Georgia:** Teona Turashvili, E-Governance Direction Lead, Institute for Development of Freedom of Information (IDFI)
- **Germany:** Philipp Otto, Founder and Head, iRights. Lab think tank and iRights.Media publishing house, Editor in Chief, iRights.info, political strategist, advisor to the German government and companies; Henning Lahmann, Policy Analyst, iRights.Lab
- **Hungary:** Dalma Dojcsák and Máté Szabó, Hungarian Civil Liberties Union
- **Iceland:** Caroline Nellemann, independent consultant, specialist in digital media and civic engagement
- **India:** Sarvjeet Singh, Programme Manager, Centre for Communication Governance at National Law University, Delhi; Parul Sharma, Analyst, Center for Communication Governance; assistance from Nishtha Sinha and Vaibhav Dutt, Students, B.A., LL.B. (Hons.), National Law University
- **Indonesia:** Indriaswati Dyah Saptaningrum, Senior Researcher, ELSAM (The Institute for Policy Research and Advocacy)
- **Iran:** Kyle Bowen and Mahmood Enayat, Small Media
- **Italy:** Giampiero Giacomello, Associate Professor of International Relations, University of Bologna
- **Japan:** Dr. Leslie M. Tkach-Kawasaki, Associate Professor, University of Tsukuba

- **Kazakhstan:** Adilzhan Nurmakov, Senior Lecturer, KIMEP University
- **Kenya:** Grace Githaiga, Associate, Kenya ICT Action Network (KICTANet)
- **Kyrgyzstan:** Artem Goryainov, IT Programs Director, Public Foundation CIIP
- **Lebanon:** Firas Talhouk, Program Manager, Public Policy Lab at the Issam Fares Institute for Public Policy and International Affairs, American University of Beirut
- **Libya:** Fadil Aliriza, journalist, researcher, political analyst, and Tunisia Project Manager, Carnegie Endowment for International Peace
- **Malawi:** Gregory Gondwe, Bureau Chief, Times Media Group, Malawi
- **Malaysia:** K Kabilan, Managing Editor, BeritaDaily.com, and online media consultant
- **Mexico:** Jorge Luis Sierra, Knight International Journalism Fellow, International Center for Journalists, and award-winning Mexican journalist
- **Morocco:** Bouziane Zaid, Associate Professor of Media and Communication, Al Akhawayn University in Ifrane
- **Myanmar:** Min Zin, Executive Director, Institute for Strategy and Policy: Myanmar
- **Nigeria:** 'Gbenga Sesan, Executive Director, Paradigm Initiative Nigeria
- **Pakistan:** Nighat Dad, Executive Director, Digital Rights Foundation, Pakistan; Adnan Ahmad Chaudhri, Associate Researcher, Digital Rights Foundation
- **Singapore:** Cherian George, Associate Professor, School of Communication, Hong Kong Baptist University
- **South Africa:** Zororo Mavindidze, Senior Researcher, Freedom of Expression Institute
- **South Korea:** Dr. Yenn Lee, Doctoral Training Advisor, SOAS, University of London (School of Oriental and African Studies)
- **Sri Lanka:** N. V. Nugawela, consultant and researcher
- **Sudan:** Azaz Elshami, independent researcher and development consultant
- **Syria:** Dlshad Othman, information security expert
- **Uganda:** Lillian Nalwoga, Policy Officer, CIPESA, and President, Internet Society Uganda Chapter
- **Ukraine:** Tetyana Lokot, Ukrainian media researcher, Lecturer in Journalism, Dublin City University
- **United Kingdom:** Aaron Ceross, Researcher in Cyber Security, University of Oxford
- **United States:** Laura Reed, independent researcher
- **Uzbekistan:** Dr. Zhanna Hördegen, Research Associate, University Research Priority Program (URPP) Asia and Europe, University of Zurich, and independent consultant
- **Venezuela:** Raisa Urribarri, Director, Communications Lab for Teaching, Research and Community Extension (LIESR), University of Los Andes
- **Zambia:** Brenda Bukowa, Lecturer and Researcher, Department of Mass Communication, University of Zambia

The analysts for the reports on Angola, Bahrain, Bangladesh, Belarus, China, Ecuador, Egypt, Ethiopia, The Gambia, Jordan, Russia, Rwanda, Philippines, Saudi Arabia, Thailand, Tunisia, Turkey, United Arab Emirates, Vietnam and Zimbabwe are independent internet researchers who have asked to remain anonymous.

“The internet is an indispensable tool for promoting social justice and political liberty, used by citizens worldwide to fight for their rights, demand accountability, and amplify marginalized voices.”

Freedom House

Freedom House is a nonprofit, nonpartisan organization that supports democratic change, monitors freedom, and advocates for democracy and human rights.

1850 M Street NW, 11th Floor
Washington, DC 20036

120 Wall Street, 26th Floor
New York, NY 10005

www.freedomhouse.org
facebook.com/FreedomHouseDC
@FreedomHouseDC

202.296.5101 | info@freedomhouse.org