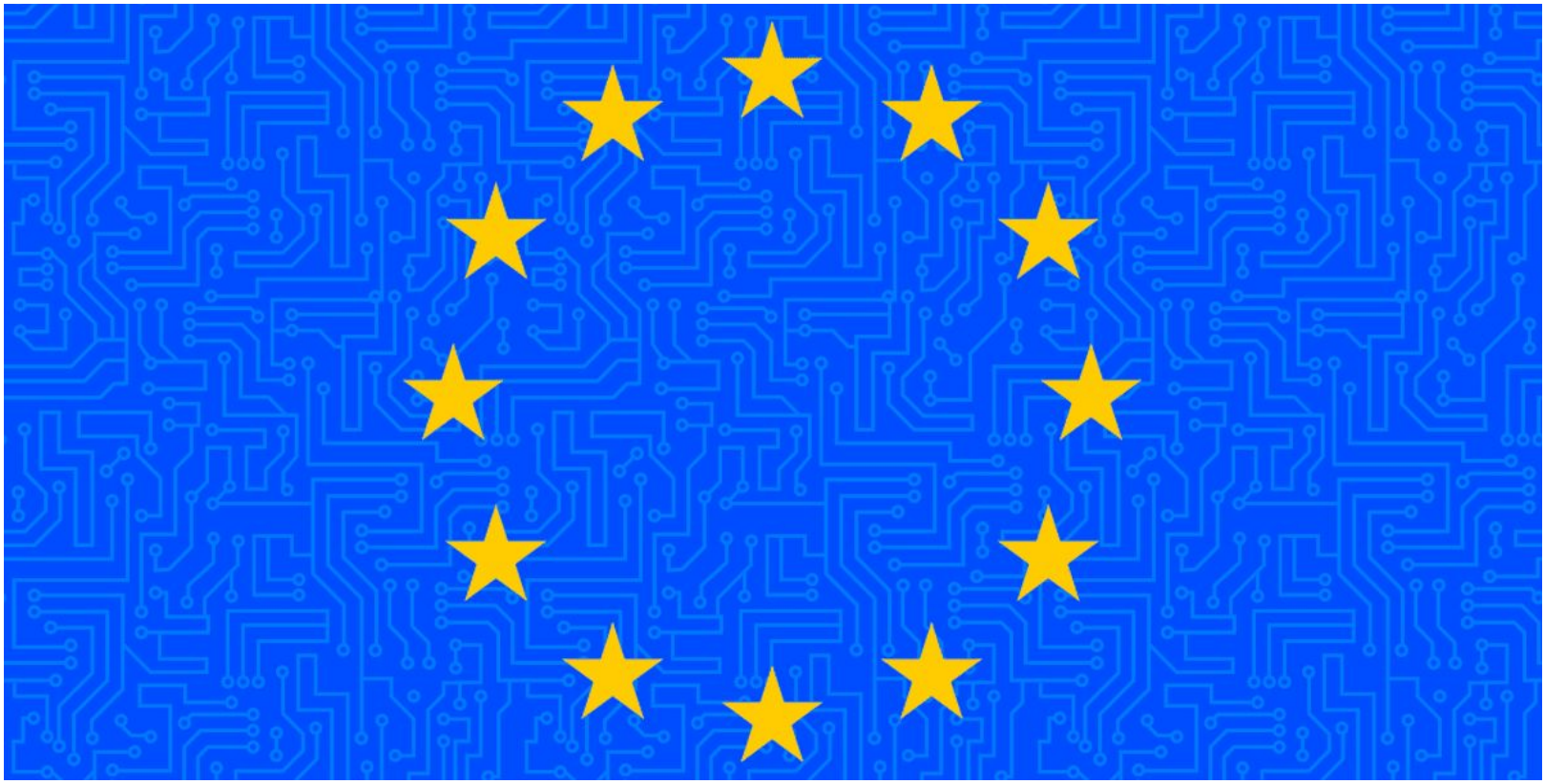

Preserve What Works, Fix What is Broken:

EFF's Policy Principles for the Digital Services Act

ELECTRONIC FRONTIER FOUNDATION

Published 2020

Contents

Preserve What Works, Fix What is Broken..... 4

Rules on Liability and Monitoring: Preserve What Works..... 5

Introducing Interoperability Obligations: Empowering Users and Innovators..... 8

Fair and Just Notice and Action Procedures: Fix What is Broken..... 11

Put Users First: Implement Strong User Controls..... 14

Preserve What Works, Fix What is Broken

The Internet has seen better times. Meant to liberate users, being online has become synonymous with being locked into a few powerful platforms, being tracked across the web without options to dissent and being left at the mercy of algorithmic decision systems that curate our online lives. Fundamental principles like transparency, openness, and informational self-determination that used to be central to the early days of the Internet seem to have been undermined significantly in the past decades.

But like any technology, the Internet, and the services built upon it, are ours to shape. The past years have shown that existing laws are barely capable of reigning in Big Tech's unfettered powers. What is needed is an update to key laws in order to adapt them to the changed platform economy of the 21st century -- while protecting the elements of the current legal order that work.

In the European Union, there is an opportunity to do exactly that: adopt future-proof regulation that preserves the provisions that have inspired innovation and protected fundamental rights, while empowering users and innovators. In 2020, the European Commission announced an ambitious strategy to promote a distinctly European vision on how to regulate big tech. As part of that strategy, the Commission will publish its proposal for the Digital Services Act package in the upcoming months. The Digital Services Act (DSA) is the most significant reform of Europe's central platform legislation, the e-Commerce Directive, the EU has undertaken in twenty years. It is an unparalleled opportunity to formulate a bold, evidence based vision to address some of today's most pressing challenges.

We support the Commission's commitment to build a better and alternative future for the Internet, and welcome its ambition to find creative solutions to complex issues like lacking transparency, privatized content moderation or gatekeeper-dominated markets. We have already contributed to the Commission's consultation on the DSA and will continue to work closely with the EU institutions to share our experiences of fighting for digital rights through impact litigation, grassroots activism, and technology development.

But we are also wary of the recent slew of laws like the Copyright Directive and regulatory initiatives in Germany, France, and Austria that try to address similar issues but have endangered the freedom of expression online by giving private platforms even greater responsibilities to police user content. The DSA is an important opportunity to clarify the EU's commitment to fundamental rights online, and to secure basic rights that will be built upon in the years to come.

In our policy advocacy surrounding the DSA, we will focus on four key areas: platform liability, interoperability mandates, procedural justice and user control. As we have been introducing the principles that will guide our policy work, our message to the EU has been clear: Preserve what works. Fix what is broken. And put users back in control.

Rules on Liability and Monitoring: Preserve What Works

Principle 1: Online intermediaries Should Not be Held Liable for User Content

Intermediaries have a pivotal role to play in ensuring the availability of content and the development of the Internet. They are a driver of free speech, as they enable people to share content with audiences at an unprecedented scale. One of the reasons for the success of online intermediaries is the immunity they enjoy for third-party content. This is one of the fundamental principles that we believe must continue to underpin Internet regulation: Platforms should not be held responsible for the ideas, images, videos, or speech that users post or share online. If such a principle were not in place, platforms would be pushed to affirmatively monitor how users behave; would filter and check users' content; and would block and remove everything that is controversial, objectionable, or potentially illegal to avoid legal responsibility. By the same token, users would likely not feel inclined to speak freely in the first place; they would avoid sharing their artistic expression or publishing a critical essay about political developments. Worse yet, without legal protection, service providers could easily become targets for corporations, governments, or bad actors who want to target and silence users.

The EU should therefore make sure that online intermediaries continue to benefit from comprehensive liability exemptions and not be held liable for content provided by users. The current nebulous distinction between passive and active host providers for exemptions to apply should be given up: Intermediaries should not be held liable for user content as long as they are not involved in co-creating or modifying that content in a way that substantially contributes to illegality, and provided that they do not have

actual knowledge about its illegal or infringing character. Any additional obligations must be proportionate and not curtail the free expression of users and innovation.

Principle 2: Only Court Orders Should Trigger Liability

Intermediaries should not be held liable for choosing not to remove content simply because they received a private notification by a user. In order to protect freedom of speech, the EU should adopt the principle that actual knowledge of illegality is only obtained by intermediaries if they are presented with a court order. It should be up to independent judicial entities, not platforms or disgruntled users, to decide the legality of any other user's content. Any exceptions to this principle should be limited to content that is manifestly unlawful; that is, content that is obviously illegal irrespective of the context. Notices about such content should be sufficiently precise and substantiated.

Principle 3: No Mandatory Monitoring or Filtering

The ban on general monitoring under the current e-Commerce Directive has the purpose of protecting users, by guaranteeing their freedom of expression and their rights to personal data as memorialized in the Fundamental Rights Charter. Should this important principle be abandoned, it would not only have disastrous consequences for the freedom of users, but would also inevitably lead to shadow regulation; that is, privatized enforcement by platforms without transparency, accountability, or other safeguards.

The Member States of the European Union should thus not be permitted to impose obligations on digital service providers to affirmatively monitor their platforms or networks for illegal content that users post, transmit, or store. Nor should there be a general obligation for platforms to actively monitor facts or circumstances indicating illegal activity by users. The ban on general monitoring obligations should include a ban on mandated automated filter systems that evaluate the legality of third-party content or which prevent the (re)upload of illegal content. Additionally, no liability should be based on an intermediary's failure to detect illegal content. Related privacy rights, such as the right not to be subjected to automated individual decision-making, must also be protected in this context.

Principle 4: Limit the Scope of Takedown Orders

Recent cases have demonstrated the perils of worldwide content takedown orders. In Glawischnig-Piesczek, the Court of Justice of the EU held that a court of a Member State can order platforms not only to take down defamatory content globally, but also to take down identical or "equivalent" material. This was a terrible outcome as the content in question may be deemed illegal in one State, but is clearly lawful in many other States. Also, by referring to "automated technologies" to detect similar language, the court opened the gates of monitoring by filters, which are notoriously inaccurate and prone to overblocking legitimate material.

The reform of EU Internet legislation is an opportunity to acknowledge that the Internet is global and takedown orders of global reach are immensely unjust and impair users'

freedom. New rules should make sure that court orders—and particularly injunctions—should not be used to superimpose the laws of one country on every other state in the world. Takedown orders should be limited to the content in question and based on the principles of necessity and proportionality in terms of its geographical scope. Otherwise, it is possible that we will see one country's government dictating what residents of other countries can say, see, or share online. This would lead to a "race to the bottom" toward creating an ever more restrictive global Internet.

Introducing Interoperability Obligations: Empowering Users and Innovators

Principle 1: General Interoperability Obligations

EFF's vision is a legal regime that fosters innovation and puts users back in control of their data, privacy, and online experiences. We believe that interoperability has a major role to play to make this vision of a Public Interest Internet come to life, which is why we propose interoperability obligations for platforms with significant market power. What we mean by that is simple: platforms that control significant shares of a market, and act as gatekeepers to that market, must offer possibilities for competing, not-incumbent platforms to interoperate with their key features.

While Europeans already have a right to data portability under the GDPR, this right comes with limits. It is not encompassing (users cannot port all personal data), it is conditional (only possible where "technically feasible"), and it is not clear where users should port their data to. Interoperability is the missing piece to breathe life into the right to portability. Interoperability through technical interfaces would enable users to communicate with friends across platform boundaries, or to be able to follow their favorite content across different platforms without having to create several accounts. Users would no longer be forced to stay on a platform that disregards their privacy, covertly collects their data, or jeopardizes their security, for fear of losing their social network. Instead, users would have the chance to make real and informed choices.

Principle 2: Delegability

But it doesn't end here. Interoperability should also happen at the level of user interfaces, and should allow for as much flexibility and diversity as users want. Therefore, platforms with significant market power should also make it possible for competing third parties to act on users' behalf. If users want to, they should be able to delegate elements of their online experience to different competent actors. For example, if you don't like Facebook content moderation practices, you should be able to delegate that task to another organization, like a non-profit specializing in community based content moderation.

Principle 3: Limit Commercial Use of Data

To avoid the exploitation of interoperability, any data made available through interoperability should not be available for general commercial use. Most major platforms are built on business models that rely on the (often coveted) collection and sale of users' data, thereby monetizing users' attention and exploiting their personal data. Therefore, any data made available for the purpose of interoperability should only be used for maintaining interoperability, safeguarding users' privacy, or ensuring data security. By prohibiting the commercial use of data used for implementing or maintaining interoperability, we also want to positively incentivize competitors with innovative, responsible, and privacy-protective business models.

Principle 4: Privacy

It is crucial to empower users to take control of how, when, why, and with whom their data is being shared. This means that key principles underpinning the GDPR and other applicable legislation—such as data minimization, privacy by design, and privacy by default—must be respected. This should also include easy-to-use interfaces through which users can give their explicit consent regarding any use of their data (as well as revoke that consent at any time).

Principle 5: Security

But users' data and communications should not only be kept private, but also safe. Interoperability measures should always center on users' security and should never be construed as a reason that prevents platforms from taking efforts to keep users safe. However, if intermediaries do have to suspend interoperability to fix security issues, they should not exploit such situations to break interoperability but rather communicate transparently, resolve the problem, and reinstate interoperability interfaces within a reasonable and clearly defined timeframe.

Principle 6: Documentation and Non-Discrimination

Finally, it is crucial to make sure that interoperability does not become a tool for powerful incumbents to act as gatekeepers and to further enshrine their dominant

position. Our goal of user empowerment is served best when diversity and plurality are strongest, so interoperability should benefit as many competitors as possible, rather than just a few favored parties. To offer users more choice, access to interoperability interfaces should not discriminate between different competitors and should not come with strenuous obligations or content restrictions. Interoperability interfaces, such as APIs, must also be easy to find, well-documented, and transparent.

Fair and Just Notice and Action Procedures: Fix What is Broken

Principle 1: Reporting Mechanisms

Intermediaries should not be held liable for choosing not to remove content simply because they received a private notification by a user. Save for exceptions, the EU should adopt the principle that actual knowledge of illegality is only obtained by intermediaries if they are presented with a court order.

However, the EU should adopt harmonized rules on reporting mechanisms that help users to notify platforms about potentially illegal content and behaviour. Reporting potentially illegal content online sounds simple, but can be daunting in practice. Different platforms use different systems to report content or activities, and the categories used to differentiate between different types of content can differ widely - but can also be confusing and hard to grasp. Some platforms don't provide meaningful notification options at all. Reporting potentially illegal content should be easy, and any follow-up actions by the platform transparent for its users.

Principle 2: A Standard for Transparency and Justice in Notice and Action

Content moderation is often opaque - companies generally do not give users enough information about what speech is permissible, or why certain pieces of content has been taken down. To make content moderation more transparent, platforms should provide users with a notice when content has been removed (or their account has been suspended). Such a notice should identify the content removed, the specific rule that it

was found to violate, and how the content was detected. It should also offer an easily accessible explanation of the process through which the user can appeal the decision. Platforms should provide a user-friendly, visible, and swift appeals process to allow for the meaningful resolution of content moderation disputes. Appeals mechanisms must also be accessible, easy to use and follow a clearly communicated timeline. They should allow users to present additional information, and must include human review. At the end of the appeals process, users should be notified, and should be provided with a statement explaining the reasoning behind the decision taken in a language the user can understand. It is also crucial that users are informed that even if they choose to partake in a dispute resolution process, they don't forfeit their rights to seek justice before independent judicial authorities, like a court in their home jurisdiction.

Principle 3: Open the Blackbox that is Automated Decision Making

Most major platforms use algorithms to automate part of their content moderation practices. Content moderation is a precarious and risky job, and many hope that automated content moderation tools could be the silver bullet that will solve content moderation's many problems. Unfortunately, content moderation is messy, highly context-dependent and incredibly hard to do right, and automated moderation tools make many, many mistakes. These challenges have become especially apparent during the COVID-19 pandemic, as many platforms replaced human moderators with automated content moderation tools.

In the light of automated content moderation's fundamental flaws, platforms should provide as much transparency as possible about how they use algorithmic tools. If platforms use automated decision making to restrict content, they should flag at which step of the process algorithmic tools were used, explain the logic behind the automated decisions taken, and also explain how users can contest the decision.

Principle 4: Reinstatement of Wrongfully Removed Content

Content moderation systems make mistakes all the time - regardless of whether they are human or automated--that can cause real harm. Efforts to moderate content deemed offensive or illegal consistently have disproportionate impacts on already marginalized groups. Content moderation often interferes with counterspeech, attempts to reclaim specific terms, or calling out racism by sharing the racist statements made.

Because erroneous content moderation decisions are so common and have such negative effects, it is crucial that platforms reinstate users' content when the removal decision cannot be justified by a sensible interpretation of the platforms' rules or the removal was simply in error. The Digital Services Act should promote quick and easy reinstatement of wrongfully removed content or wrongly disabled accounts.

Principle 5: Coordinated and Effective Regulatory Oversight

Good laws are crucial, but their enforcement is just as important. The European legislators should therefore make sure that independent authorities can hold platforms accountable. Coordination between independent national authorities should be

strengthened to enable EU-wide enforcement, and platforms should be incentivized to follow their due diligence duties through, for example, meaningful sanctions harmonized across the European Union.

Put Users First: Implement Strong User Controls

Principle 1: Give Users Control Over Content

Many services like Facebook and Twitter originally presented a strictly chronological list of posts from users' friends. Over time, most large platforms have traded that chronological presentation for more complex (and opaque) algorithms that order, curate and distribute content, including advertising, and other promoted content. These algorithms, determined by the platform, are not necessarily centered on satisfying users' needs, but usually pursue the sole goal of maximizing the time and attention people spend on a given website. Posts with more "engagement" are prioritised, even if that engagement is driven by strong emotions like anger or despair provoked by the post. While users sometimes can return to the chronological stream, the design of platforms' interfaces often nudges them to switch back. Interfaces that are misleading or manipulating users, including "dark patterns", often contravene core principles of European data protection laws and should be addressed in the Digital Services Act where appropriate.

Platforms' algorithmic tools leverage their intimate knowledge of their users, assembled from thousands of seemingly unrelated data points. Many of the inferences drawn from that data feel unexpected to users: platforms have access to data that reaches further back than most users realize, and are able to draw conclusions from both individual and collective behavior. Assumptions about users' preferences are thus often made by making inferences from seemingly unrelated data points. This may shape (and often limit) the ways in which users can interact with content online and can also amplify misinformation and polarization in ways that can undermine the transparent, deliberative exchange of information on which democratic societies are built.

Users do not have to accept this. There are many third-party plugins that re-frame social platforms' appearance and content according to peoples' needs and preferences. But right now, most of these plugins require technical expertise to discover and install, and platforms have a strong incentive to hide and prevent user adoption of such independent tools. The DSA is Europe's golden opportunity to create a friendlier legal environment to encourage and support this user-oriented market. The regulation should support interoperability and permit competitive compatibility, and should establish explicit, enforceable rules against over-aggressive terms of service that seek to forbid all reverse-engineering and interconnection. Beyond the Digital Services Act, the EU must actively support open source and commercial projects in Europe that offer localised or user-empowering front-ends to platforms, and help foster a vibrant and viable market for these tools.

Giving people—as opposed to platforms—more control over content is a crucial step to addressing some of the most pervasive problems online that are currently poorly managed through content moderation practices. User controls should not require a heightened threshold of technological literacy needed to traverse the web safely. Instead, users of social media platforms with significant market power should be empowered to choose content they want to interact with—and filter out content they do not want to see—in a simple and user-friendly manner. Users should also have the option to decide against algorithmically-curated recommendations altogether, or to choose other heuristics to order content.

Principle 2: Algorithmic Transparency

Besides being given more control over the content with which they interact, users also deserve more transparency from companies to understand why content or search results are shown to them—or hidden from them. Online platforms should provide meaningful information about the algorithmic tools they use in content moderation (i.e., content recommendation systems, tools for flagging content) and content curation (for example in ranking or downranking content). Platforms should also offer easily accessible explanations that allow users to understand when, for which tasks, and to which extent algorithmic tools are used. To alleviate the burden on individual users to make sense of how algorithms are used, platforms with significant market power should allow independent researchers and relevant regulators to audit their algorithmic tools to make sure they are used as intended.

Principle 3: Accountable Governance

Online platforms govern their users through their terms of service, community guidelines, or standards. These documents often entail the fundamental rules that determine what users are afforded to do on a platform, and what behavior is constrained. Platforms regularly update those documents, often in minor but sometimes in major ways—and usually without consulting or notifying their users of the changes. Users of such platforms must be notified whenever the rules that govern them change, must be asked for their consent and should be informed of the consequences of their choice. They should also be provided with a meaningful explanation of any substantial changes in a language they understand. Additionally, platforms should present their

terms of service in machine-readable format and make all previous versions of their terms of service easily accessible to the public.

Principle 4: Right to Anonymity Online

There are countless reasons why individuals may not want to share their identity publicly online. While anonymity used to be common on the Internet, it has become increasingly more difficult to remain anonymous online. In their hopes to tackle hate speech or "fake news", policymakers in the EU and beyond have been proposing duties for platforms to enforce the use of legal names.

For many people, however—including members of the LGBTQ+ community, sex workers, and victims of domestic abuse—such rules could have devastating effects and lead to harassment or other forms of attribution. We believe that as a general principle, Member States should respect the will of individuals not to disclose their identities online. The Digital Services Act should affirm users' informational self-determination also in this regard and introduce the European right to anonymity online. Deviating terms of service should be subject to fairness control.