March 30, 2023

U.S. Government Public-Private Sector Call to Advance Democracy-Affirming Anti-Censorship Technologies to Combat Authoritarian Regimes

The U.S. Government has issued a call to the private sector to advance democracy through countering the misuse and abuse of technology, fighting corruption, protecting civic space, and advancing labor rights. In an effort to champion tenets of Internet freedom, this U.S. Government initiative extends the State Department's work by calling on the private sector, including key communications and technology manufacturers, to combat authoritarian use of network-level filtering technology for repressive censorship by supporting and furthering censorship-resistant technologies and technical standards.

The world continues to see authoritarian regimes abuse technology as a tool to suppress critics, journalists, human rights defenders, and societies writ large. Often, these authoritarian regimes exploit security weaknesses in common Internet technologies in their attempts to censor information and communication and curtail freedom of expression. This presents both an imperative and an opportunity to improve Internet security, resilience, and access for vulnerable users threatened by regimes that do not respect the rule of law or democratic values.

Many foundational networking technologies and protocols can be implemented in ways that provide security benefits while also building in fundamental resistance to repressive network filtering by authoritarian regimes. Additionally, existing efforts which focus on improving the privacy enhancing properties of Internet technologies can be implemented in ways that bolster censorship resistance, while also protecting against the misuse of such technologies for criminal purposes, such as terrorism, human trafficking, or child exploitation.

The U.S. Government seeks to support Internet freedom, combat repressive censorship, and bolster security. Progress has already been made on this front. Private companies and governments around the world have pushed for, or implemented, security features that not only provide additional security to everyday users, but also limit the impact of authoritarian censorship. But there is more to be done. We encourage the private sector to meaningfully engage with governments and civil society both in the promotion of an open, free, global, interoperable, reliable, and secure Internet, and in considering the safety of our citizens from harms, online and offline.

As an initial matter, we encourage the adoption or utilization of the following practices:

(1) **Deploying and fostering adoption of network censorship-resistant implementations:** Consider advancing the use of networking technologies in key ways, from providing

capacity and support to standardization efforts to ensuring implementation of these network technologies include strong network censorship-resistant properties.

(2) **Accessible Virtual Private Network (VPN) Support:** Consider efforts to lower the barrier to access for users in highly-censored environments. This could include integrating support for a wide range of VPNs, making VPN usage user-friendly with a focus on language support for areas with high amounts of government censorship and, where possible, turning VPNs on by default.

(3) **Direct Support for Anti-Censorship Technologies:** Infrastructure providers should consider lending technical and non-technical support to those who provide users in highly-censored environments free access to anti-censorship services. For example, this could include ensuring rates remain affordable to customers providing these services.

We also encourage the private sector and civil society to share updates at SummitPrivateSector@state.gov.