PROTECTING A FREE AND OPEN INTERNET

Written Testimony by ADRIAN SHAHBAZ
Vice President, Research and Analysis

Committee on Ways & Means
Subcommittee on Trade

Protecting American Innovation by Establishing and
Enforcing Strong Digital Trade Rules

September 20, 2024, 9:00 a.m.

Chairman Smith, Ranking Member Blumenauer, and members of the subcommittee,

It is an honor to testify before you today. I ask that my full written testimony be admitted into the record.

I am grateful to this subcommittee for elevating the human rights angle of digital trade. The protection of fundamental freedoms is necessary for upholding a rule of law system that protects innovation and enables both prosperity and security. We appreciate Congress' longstanding and bipartisan support for these issues.

I speak today on behalf of Freedom House. We are a nonprofit and nonpartisan organization founded in 1941. Our mission is to protect and expand freedom around the world. My remarks will draw on findings from Freedom House's annual Freedom on the Net report, which assesses respect for internet freedom in over 70 countries.

Internet freedom is the simple notion that the same rights held by people offline should be protected online. This includes freedom of expression, access to information, and privacy.

We also believe that an open, interoperable, and global internet contributes to the enjoyment and protection of these rights. With the right tools, a schoolteacher in Afghanistan can access the same information and platforms as a student in Washington, D.C. A free and open internet is one that

empowers individuals to learn, communicate, and form communities wherever they are in the world.

For these reasons, we expressed concerned one year ago when the United States Trade Representative dropped support for cross-border data flows at the World Trade Organization. The decision risks further fragmenting the global internet and emboldening authoritarian governments.

Two-thirds of internet users now reside in countries where political, social, or religious content is censored. More governments have criminalized nonviolent speech and put critics in jail. Increasingly, they seek to divide the global internet into patchwork of national networks that are more easily controlled.

One of the methods used to exert greater control is data localization. These are legal requirements for companies and other service providers to store data about local residents on servers based within the country. They are often passed under the premise of defending national security, growing the digital economy, or protecting users' privacy.

In our research, we have found that these laws can have negative implications for people's freedoms, because they grant a country's security agencies more power to monitor and imprisonment people who criticize the government or speak up on banned issues. This is particularly true in countries with weak respect for free expression and the rule of law.

One of the clearest examples is China, a one-party state that holds the dubious distinction as the world's worst abuser of freedom. Many US-based news outlets and social media platforms are blocked, including Facebook, WhatsApp, Instagram, YouTube, and X. Those companies that remain in business face data localization requirements and restrictions on cross-border data flows.

Certain providers are required to store personal information about clients and users on local servers, where it is subject to requests from security agencies. Those requests can put companies in a very difficult position – particularly when they are demands to censor legitimate speech, or to help the Chinese Community Party to gather data about journalists, dissidents, and members of persecuted ethnic and religious communities. According to a 2022 survey by the US-China Business Council, these restrictions "disproportionately harm the operations and competitiveness of foreign businesses in China that leverage global infrastructure".

The Russian government has long admired China's so-called Great Firewall of internet controls. Over time, authorities have passed legislation and developed technical infrastructure to build what they have called a "sovereign internet." Right now, many Russians rely on virtual private networks (VPNs) and other circumvention tools to communicate with family and friends across borders, and to access independent news sources that are based in freer countries. The sovereign internet project would allow Moscow to totally isolate the country from the rest of the internet during mass protests and other major events, cutting off Russians' ability to communicate with the outside world.

As part of this effort, the Russian government has passed a series of law that require companies to collect data on their users, store it on servers based in the country, and hand it over to security agencies like the Federal Security Service (or FSB) when they request it. Companies face demands to comply with unjust censorship and surveillance. Authorities have banned criticism, organizing, and objective reporting on the war in Ukraine. Companies that refuse to comply with the government's demands to enforce their unjust laws are eventually forced to leave the country.

The Chinese and Russian governments are working with other authoritarian leaders to reshape global cyber norms in their interests. At the United Nations and other multilateral fora, they seek to legitimize their domestic crackdowns on freedom and privilege their ability to control data.

If global norms further shift in favor of data localization and restrictions on cross-border data flows, there is a risk that companies in authoritarian countries and backsliding democracies will face increased demands to censor legitimate materials and hand over data about their users. In places where one's political opinions, religious beliefs, and gender or sexuality can be labeled as extremist, these trends may lead to increased persecution of journalists, lawyers, politicians, and ordinary people who speak out against the government.

The United States plays a critically important role in protecting the free flow of information and data across borders – a necessary condition not only for the protection of rights but for the protection of innovation, prosperity, and security. In line with the United States International Cyberspace and Digital Policy Strategy, the US should "develop shared mechanisms that will help maintain an open, interoperable, secure, and reliable internet as well as trusted cross-border data flows." To ensure the United States continues its leadership role in this space, Congress should:

1. Urge the Biden administration and the next presidential administration to ensure the USTR is firmly committed to protecting the free flow of data.
2. Work with the Executive Branch to ensure robust US participation at multilateral institutions. American absence in these spaces makes it easier for authoritarian regimes to push their models of digital authoritarianism internationally.
3. Ensure US trade policy takes a potential trading partner's record on human rights – including protection of a free and open internet – into account.
4. Continue to provide funding for the protection of a free and open internet, including support for local civil society organizations that work on these issues, as well as for popular circumvention tools that allow people in closed environments to access information.
5. Pass legislation to improve transparency across technology products and practices, including content moderation, recommendation and algorithmic systems, collection and use of data, and political and targeted advertising. Laws should also provide opportunities for vetted researchers to access platform data, in order to inform additional policy development.

It is essential for the US and likeminded allies to offer an alternative to the authoritarian model of digital governance. We should better safeguard people's rights and data while still protecting the global internet.

I will gladly answer any questions you may have. Thank you again for the opportunity to participate in today's briefing.