American Edge Project:

How American Values Can Keep The Global Internet Free, Open And Accessible

/edge

AMERICAN EDGE PROJECT

/edge
AMERICAN EDGE PROJECT

How American Values Can Keep The Global Internet Free, Open And Accessible
May 2023

Introduction: A Free And Open Internet Is A Critical Tool In The Competition Between Techno-Democracies And Techno-Autocracies

Since the early days of the internet, the United States has led the world in advocating to keep it free and open. America has championed the values of free expression and open trade, of participatory governance, and of technological advancement that promotes freedom, opportunity, and equality.

Internet freedom has not been a Democratic or Republican principle: it has been an American idea rooted in American values. And it has not been simply an aspiration: it has been a sustained bipartisan effort for more than three decades by past presidents and Congresses who have worked to establish a regulatory framework that embraces and advances these values and expands that framework widely across the globe. A free and open internet echoes the ideals of egalitarianism and equality that have been embedded in the fabric of American life, from the Declaration of Independence to Lincoln's Emancipation Proclamation to Martin Luther King's "I Have a Dream" speech. Internet freedom is deeply entwined with American values, building off centuries of First Amendment jurisprudence.

Today, however, a free and open internet is under threat. Digital authoritarianism is on the rise, and digital autocracies, namely China[1] and Russia, are advancing a vision for an internet that looks decidedly un-American. America's internet is rooted in expression and freedom, while China's is rooted in censorship and surveillance. America's internet is open, inclusive, and distributed; China's is closed, controlling and paternalistic.

According to Freedom House's annual Freedom on the Net report, internet freedom has declined globally for 12 consecutive years. Some troubling trends endure: China, with one-fifth of the world's population, has ranked last in the world for internet freedom for eight straight years. In statements, the director of the Federal Bureau of Investigation (FBI) asserted: "We…see a coordinated effort across the Chinese government to lie, cheat

[1] *Our critique of China in this paper is directed solely at the leadership of the Chinese Communist Party (CCP) and not the Chinese people, for whom we have a deep respect and admiration and whose voices are rarely reflected in CCP policy and actions.*

and steal their way into unfairly dominating entire technology sectors, putting competing U.S. companies out of business." Some new threats are emerging as well. According to Freedom House, in 2022, a record number of national governments blocked websites with nonviolent political, social, or religious content, undermining the rights to free expression and access to information. Russia has used the internet as a battlefront in its unjust and unprovoked war against Ukraine.

With internet freedom spiraling downward year after year, now, more than ever, we need a policy agenda that will reverse this decline. America's version of the internet – not China's – is best suited to advance liberty, promote economic growth, protect our security, and check digital authoritarianism. Our approach here is not motivated by protectionism: we do not seek to use technology or policy as a means of protecting domestic companies from fair foreign competition. Instead, the focus should be on protecting America's security, preserving freedom of expression, and advancing innovation. This new agenda should advance American interests while also expanding the rights and improving the livelihoods of internet users throughout the world.

This policy brief outlines three pillars for a free and open internet that should occur concurrently.

- First, America should slow the spread of foreign digital authoritarianism.
- Second, we should promote free speech within and across borders.
- Third, we should build a stronger internet to connect people to each other and to their governments.

This agenda will slow the spread of digital authoritarianism and usher in an era of greater economic opportunity, increased political accountability, and expanded human rights. Equally important, this agenda will ensure the United States maintains its global edge in technological innovation.

Pillar #1: Slow The Spread Of Digital Authoritarianism

The greatest threat to a free and open internet is digital authoritarianism. This threat, defined as the use of information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations, is on the rise. To check its spread, we must protect American democracy from foreign influence operations, implement security protocols to protect global information flows, check China's global technology ambitions, including the deployment of technologies affiliated with the Chinese Community Party (CCP), and avoid data localization. America's private sector companies also need to be empowered to serve as ambassadors of U.S. values.

(i) Protect American democracy from foreign influence. The totality of American information systems – military, commercial, research, industrial, governmental, electoral, and others – are repeatedly under threat from foreign actors, including hackers from China and Russia. China steals more than $500 billion in U.S. intellectual property each year. FBI Director Christopher Wray recently said that the agency currently has more than 2,000 cyberattacks from China under investigation. In May 2022, security researchers revealed that hackers linked to the Chinese government attempted to steal sensitive data from more than 36 companies. According to Director Wray, "there is just no country that presents a broader threat to our ideas, our innovation, and our economic security than China."

Additionally, the U.S.-China Economic and Security Review Commission's 2022 Annual Report to Congress found that Beijing's increasing reliance on hostile cyber operations "pose[s] a serious threat to U.S. government, business and critical infrastructure networks in the new and highly competitive cyber domain."

Foreign influence operations include:

- Using false personas and fabricated stories on social media platforms to discredit U.S. individuals and institutions.
- Targeting U.S. officials and other U.S. persons through traditional intelligence tradecraft.

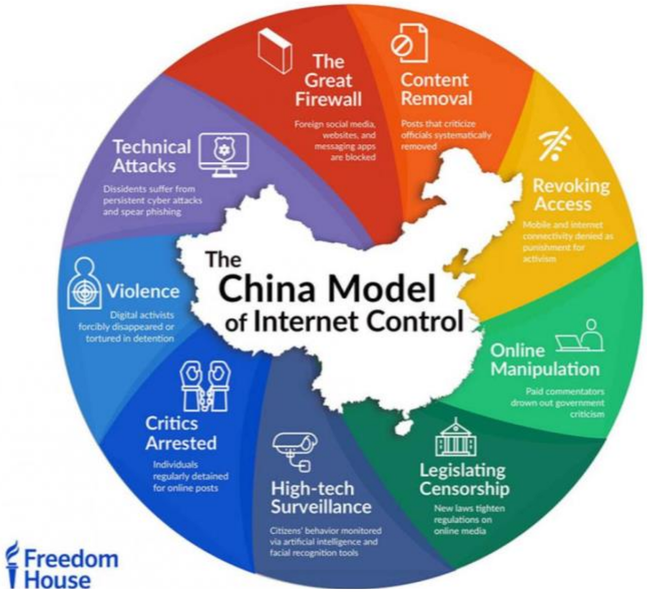
- Undermining the electoral process, including suppressing voting, providing illegal campaign financing, and conducting cyberattacks against candidates and the voting infrastructure.

To combat this cyber warfare, policymakers should increase funding for government agencies combating foreign influence operations, including expanding staffing and creating offices dedicated exclusively to foreign cybersecurity investigations, prosecutions, and risk mitigation of foreign influence operations.

Governments should devote resources to cybersecurity operations that will assist in deterring foreign election interference. Platforms should establish dedicated, scalable election security teams to identify foreign election interference, and where they identify a violation of law, they should report it to law enforcement authorities.

Key Elements of China’s Digital Authoritarianism

Freedom House assesses internet freedom levels in 70 countries around the world through its Freedom on the Net report. For eight consecutive years, China has ranked as "the world’s worst abuser of internet freedom." The graphic below shows the depth and breadth of China’s “digital authoritarianism.” Worse, China’s government is now exporting its version of internet control to other countries.


The China Model of Internet Control
The Great Firewall
Foreign social media, websites, and messaging apps are blocked
Content Removal
Posts that criticize officials systematically removed
Revoking Access
Mobile and internet connectivity denied as punishment for activism
Online Manipulation
Paid commentators drown out government criticism
Legislating Censorship
New laws tighten regulations on online media
High-tech Surveillance
Citizens' behavior monitored via artificial intelligence and facial recognition tools
Critics Arrested
Individuals regularly detained for online posts
Violence
Digital activists forcibly disappeared or tortured in detention
Technical Attacks
Dissidents suffer from persistent cyber attacks and spear phishing
Freedom House

Additionally, governments should also develop strategies for ensuring the responsible development and for accelerating the deployment of artificial intelligence (AI). Powerful AI has the potential to arm our adversaries and strengthen their ability to disrupt our democracy. China has invested heavily in AI, and it has deployed its AI technologies in products it sells throughout the world. In fact, a recent Harvard report said that China could beat the U.S. in AI, as well as 5G and quantum computing. To combat this threat, like-minded governments and companies should work together – like the recently announced partnership between the U.S. and India on AI – to develop an alternate vision for AI that is grounded in American conceptions of openness, liberty, and equality.

(ii) Implement security protocols to protect global information flows. Information cannot flow freely across borders if transactions with foreign entities pose significant national security threats to American citizens. Businesses headquartered in countries that are adversaries to America – or owned by parent companies located in those countries – may present national security risks.

Policymakers must take these risks seriously and protect against them. These protections are critical to safeguarding American user data, protecting American strategic interests, and enabling innovative foreign products and services to be offered in the United States. Without adequate safeguards in place around data and content, policymakers should ban such foreign products and services. Such necessary safeguards include divestiture of algorithmic control from companies affiliated with foreign entities, similar to the ways in which the Federal Communication Commission (FCC) precludes foreign entities from controlling broadcast.

The United States government is considering a range of policy tools that will enable it to identify businesses and transactions that pose a national security threat. The Information and Communications Technology and Services supply chain rule is one example. The rule establishes a process for the government to investigate transactions to ensure that they do not pose national security risks. Another tool is the review process run by the Committee on Foreign Investment in the United States (CFIUS), which evaluates foreign investments to determine whether they present a problematic security risk. When they do, CFIUS has broad authority to remedy the risk, including by requiring divestment of an acquisition. In 2019, CFIUS determined that a Chinese conglomerate should be compelled to sell dating app Grindr because of concerns about the national security implications. In addition, the Merger Filing Fee Modernization Act of 2022 requires merger parties to disclose information about subsidies received from "foreign entities of concern," including entities controlled by China and Russia.

Policymakers should continue to develop and utilize the tools they currently have available for these reviews while also exploring additional tools that might help them reduce the national security threats that stem from foreign products.

(iii) Check China's global technology ambitions, including disrupting the deployment of Chinese technologies to our allies. China poses a threat to America's leadership in innovation. It aspires to lead the world in innovation and is making vast investments in securing this leadership position. China has been particularly focused on investing in the technologies of the future — like artificial intelligence, quantum computing, and virtual reality — while American investment has been slow and plodding in comparison. As the Information Technology & Innovation Foundation (ITIF) stated in a recent report, "[t]he superiority of the U.S. military rests largely on its technological superiority," so overdependence on Chinese technology will pose a threat to U.S. national security. The study also notes that China now leads America in total gross innovation and will surpass our population-adjusted innovation by 2035. To protect our national security and ensure the continued prominence of American values in global innovation, Congress and the Biden Administration should take steps to disrupt the deployment of Chinese technologies to our allies and reduce the world's dependency on technology made in China.

The recently passed CHIPS and Science Act is a start. It will help to support manufacturing in the chips market and has already had an effect in creating jobs in communities that need them. But American investment in technology should go beyond a small number of chip manufacturers and should support new tools such as artificial intelligence, autonomous vehicles, and virtual reality. Investment should not be limited to grant programs and tax incentives for companies, but should also extend to worker training and funding for academic research. When sanctions and export controls are necessary, they should be imposed clearly and narrowly so that American companies can easily understand their compliance obligations while continuing to offer their services without being forced to cede market share to foreign competitors.

As the Lexington Institute has argued, American technology companies are important to protecting American security and ensuring that the United States, not China, leads the world in innovation. Governments at all levels should be focused on accelerating private sector innovation, like with the CHIPS Act, and strengthening our supply lines, especially of strategically important technologies.

(iv) Oppose data localization efforts and protect security of data. Companies should store data in a location that will enable them to deliver the best possible and most secure service to users. In some cases, it may mean storing data as close as possible to a user. In other cases — particularly where companies have global storage models — it may mean storing data farther from a user. In either case, companies should be able to make determinations about data location based on performance and security, not politics.

China has imposed data localization mandates that make it more difficult for companies to operate there, and that may expose users to increased censorship and surveillance. The Chinese model threatens basic human rights while also making it more difficult for companies to innovate and serve users across the world.

Governments should disavow China's approach. Governments should not impose data localization mandates that use data storage as a way to conduct surveillance or to establish local jurisdiction for a foreign company. Instead, companies should be able to decide where to store data without government interference.

Pillar #2: Promote Free Speech Within And Across Borders

A cornerstone of a free and open internet is the free flow of information across borders. The internet is not open if governments control what people say online, limiting their ability to discuss politically sensitive topics. It is not open if internet access is routinely cut off in an effort to stymie debate and sharing. And it is not open if small businesses cannot use the internet to sell goods across borders because regulations impose high costs and burdensome obligations.

To promote the free flow of information, U.S. policymakers should encourage industry standards and best practices to protect freedom of expression online, implement intermediary liability laws that protect free speech and safety, and stop the spread of internet shutdowns.

(i) Encourage industry standards that protect freedom of expression online. Free speech is a core American value. People should be permitted to express themselves freely online unless their speech is illegal or causes real-world harm.

Policymakers should work with companies to develop industry standards and best practices that allow maximum expression online, grounded in existing First Amendment jurisprudence. In addition, governments should be prohibited from imposing content restrictions outside the country’s borders since the context in which speech occurs can dictate its impact, and what might be harmful in one country might not be in another. Similarly, when a country requests that platforms remove content that is unlawful, platforms should use IP-blocking technology to restrict access to the content only in the country where it is illegal while leaving it available elsewhere. This would help expand speech, debate, and transparency.

(ii) Implement intermediary liability laws that protect free speech. Intermediary liability laws are a critical component of online expression and have helped the internet evolve into what it is today. Platforms would face vast legal risk if they could be dragged into court anytime a user posts something that might be illegal. A sharp increase in legal liability would mean that platforms would either close off user-generated content entirely or significantly limit it. That might mean that you couldn't post something on Instagram without moderators vetting it in advance, or you might not be able to post anything on Twitter unless you've been pre-vetted. The effect would likely be to reduce online expression. For smaller companies with fewer resources to devote to content moderation, it might mean that they would significantly reduce the amount of user-generated content they allow, meaning that people might not be able to comment on posts, share videos, or leave reviews for local businesses.

Intermediary liability protections have made it possible for both large and small platforms to host content posted by users and to reduce barriers to information access and sharing. Many countries have laws that limit platform liability for content posted by their users. One of the most well-known is Section 230 of the Telecommunications Act of 1996, which shields websites from liability for content posted by users. The law's shield does not extend to federal criminal law, intellectual property, or sex trafficking law, among other things. Other governments should similarly protect internet platforms from liability for merely hosting content.

(iii) Stop the spread of internet shutdowns. If people are unable to get online, they can't express themselves or connect with friends and family. Without access to the internet, businesses face challenges in reaching existing customers and growing their business to new markets. Yet despite the impact on people and businesses when internet access is disrupted, there were 187 internet shutdowns in 35 countries in 2022. The Indian government was responsible for 84 shutdowns, and nearly all the shutdowns occurred in Asia, the Middle East, and Africa. In 2021, one shutdown lasted more than 2,000 days, and three shutdowns lasted more than 500 days. Despite encouraging evidence that there was a reduction in shutdowns in 2022, governments continue to use this tactic as a means of suppressing dissent and reducing transparency.

These shutdowns have economic costs, undermine human rights, and are inconsistent with core American values. Governments should refrain from shutting down internet access and denying people the ability to access information and to connect with friends and family.

Pillar #3: Build A Stronger Internet To Connect People To Each Other And To Their Governments

The path to a more open and accessible internet must include the use of technology to advance democracy. The U.S. government can use technology to make it easier for people to exercise their democratic rights, to facilitate government transparency, and to connect people to critical public resources such as healthcare and education. Participatory governance – a government "by the people" – is at the heart of American history and its founding constitutional principles.

To realize this vision, policymakers at all levels should develop plans to leverage technology to better connect citizens to their governments and increase civic engagement, ensure universal internet access, develop digital literacy programs, pass federal privacy legislation, and invest in America's tech talent.

(i) Use technology to connect citizens to their governments and increase civic engagement. The U.S. government should build online tools that make it easy for citizens to track legislation that has been introduced as it moves through the process, to track regulatory rules and public comments on them, and to follow judicial proceedings by reading legal briefs and opinions. State and local governments should also publish voter education information online so that potential voters can easily obtain authoritative information about the voting process, including how to register. Companies should work with governments to support these initiatives, such as by building products that provide accurate information about voting.

Technology can be a powerful tool for service delivery, but only when government regulations don't stand in the way. During the pandemic, the U.S. Department of Health and Human Services (HHS) created an exception to federal health privacy regulations so that people could communicate with a doctor through widely used consumer products like Zoom, FaceTime and WhatsApp. Yet, in many cases, regulatory relief was granted only on an emergency basis. When this emergency designation is eventually lifted, these regulatory barriers will return, and people will find it more difficult to access basic services online or on their mobile phones.

Where these regulations are outdated and do not provide privacy and security benefits that outweigh their costs, governments could consider implementing more permanent reforms. For example, doctors and their patients should be able to choose from a wide range of communication tools since allowing people to use the tools they can access and use easily will likely expand the number of people who are able to benefit from valuable medical care.

(ii) Ensure universal internet access. In an increasingly digital world, internet access is paramount. As more and more people learn online, online access becomes increasingly critical for education. As more and more people get health information and services online, online access becomes increasingly critical for health. And as more and more people get information about voting and their governments online, online access becomes increasingly critical for democracy. The more our world becomes digital, the more important it is to ensure that everyone can get online.

Families and communities cannot reap the benefits of the internet if they are unable to access it; as such, closing the digital divide should be a core component of a policy agenda focused on building a more open and accessible internet. The federal government and states may need to design different solutions to bring rural and urban communities online, focusing on deploying internet infrastructure in rural communities and increasing affordability and demand in urban areas.

Policymakers should also prioritize digital equity and inclusion, such as by ensuring that data they collect on broadband access tracks disproportionate gaps for people of color. If a person is a minority or lives in an underserved community, they should have the same opportunity to access the benefits of technology as anyone else.

(iii) Develop digital literacy programs to foster healthy digital citizens. Schools should develop digital literacy programs to encourage healthy digital lifestyles, reduce the spread of disinformation, and promote digital inclusion and digital citizenship. Being a good digital citizen is not always intuitive, and just like other school programs that help to prepare students for the world outside of school, a digital citizenship curriculum can play an important role in improving people's experiences online.

Schools should offer programs on online bullying, how to evaluate information you encounter online, and privacy best practices. School districts and state governments should work with education, privacy, and safety nonprofit organizations to develop these curricula. Companies should help to fund these programs. Platforms should also offer training on the education, privacy, and safety features they offer to their users to help users better use their services. They should provide training on publicly available websites but should also dedicate time to more in-depth education with nonprofit organizations, who can, in turn, integrate these learnings into the curricula they develop.

(iv) Pass federal privacy legislation. Without a federal standard, privacy rights will likely be set by states or by foreign governments. For some people, the absence of clear federal standards will mean that they have no explicit, statutorily defined, modernized privacy rights at all.

States have responded to the absence of a federal standard by creating their own privacy rules. California, Utah, and Virginia are among the states that have recently passed a privacy law. While these laws offer some privacy protection to state residents, they create a patchwork of regulations that make it difficult for platforms — and smaller platforms in particular — to optimize their products for their users. Users who travel from state to state may be confused on what privacy rights apply when they cross state lines. As more and more states pass privacy laws, it is likely that some of these laws will conflict, meaning that a platform might be compelled to take action in one state that would violate laws in another state.

The founders of our country anticipated the problems of these state-by-state patchworks, and for that reason, they empowered Congress to pass laws governing interstate commerce. Federal privacy law is the best mechanism to protect against this fragmentation while also establishing core privacy rights for every citizen and maintaining America’s leadership role in advancing and protecting civil liberties.

Conclusion

With global internet freedom declining and increasingly under threat, techno-autocracies seem to be prevailing over techno-democracies. If countries like China and Russia continue their rise to global prominence in innovation, the internet of the future will look very different from what it does today. To shift course and to ensure that America continues to lead the world in innovation, we need to craft a policy agenda rooted in three pillars: combatting digital authoritarianism, promoting free speech within and across borders, and building a stronger internet to connect people to each other and to their governments. If we advance these three pillars, we will advance and protect American values, protect America’s national security, and foster future economic prosperity.

###