ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Restoring US Leadership on Digital Policy

ASHLEY JOHNSON I JULY 2023

The United States could regain its position as a global leader on digital policy by prioritizing a pro-innovation agenda, cooperating with its allies to advance free trade and democratic values, and pushing back against harmful narratives and policies.

KEY TAKEAWAYS

- The United States emerged as a global leader in digital policy in the 1990s thanks to its pro-innovation approach, supplemented by multistakeholder and international cooperation on key issues.
- The United States lost this position of global leadership after deprioritizing digital policy, and stands to lose even more as rising antitech sentiment translates into policies that hinder innovation and economic growth.
- The global digital policy scene in recent years has been marked by European overregulation and overreach, a rise in digital protectionist policies, and threats to democracy from China and Russia.
- The United States could restore its position of global leadership on digital policy by prioritizing innovation, free trade, and democratic values and cooperating with its allies to advance those priorities.

CONTENTS

Key Takeaways 1
Introduction 3
The History of American Digital Policy Leadership 4
- Clinton Administration Actions 5
- Noteworthy Laws 5
  - Telecommunications Act of 1996 5
  - Section 230 of the Communications Decency Act 6
  - Digital Millennium Copyright Act 7
  - Internet Tax Freedom Act 8
- International Cooperation 9
- A Multistakeholder Approach 10

The New Status Quo 11
- American Leadership Failures 11
- European Overregulation and Regulatory Imperialism 12
- Rise of Digital Protectionism 16
- Democracy Under Threat 18

Restoring American Leadership 20
- Recent Efforts 20
- Recommendations 21

Endnotes 24

INTRODUCTION

Policy matters. The United States emerged as a global leader in digital policy in the 1990s by moving early on key policy issues and adopting a light-touch, pro-innovation regulatory regime. As a result, the early Internet was largely built on American values of democracy and freedom and the United States gained a new, important source of soft power. Additionally, many of the world's most successful digital firms came out of the United States—household names such as Google, Apple, Microsoft, Amazon, and Meta—to the enormous benefit of the U.S. economy and U.S. competitiveness. Seeing America's success, other countries followed its lead with similar regimes, further cementing America's leadership status.

However, since the late-2000s, the tone of digital policy has shifted. Many policymakers, activists, and pundits decided that digital technologies and companies were a problem in need of heavy-handed regulation. Today's policy discussions are marked by both opposition to the technological innovation that drives the U.S. economy and criticism of the same large tech companies that once represented U.S. success.[1] These beliefs have gained a foothold not only in American policy discussions but also around the world, influencing regulations that both stifle innovation by imposing onerous restrictions on digital companies and harm U.S. economic leadership.

In part due to this "techlash," and in part due to multiple U.S. administrations' failure to prioritize digital policy issues, the United States has lost its once-unambiguous status as the foremost leader in digital policy. Among democratic nations, the EU has become the standard setter, exporting its flawed strategy of overregulation on issues such as privacy, competition, and emerging tech. And no wonder, as the United States is mostly on the sidelines, failing to explain why its light-touch approach is the key to digital success.

Meanwhile, thanks to China's unfair trade practices and the inaction of the United States and its allies, China has gained ground as a digital leader as well.

With a rise of digital protectionism around the world threatening the free flow of data, a rise in authoritarianism threatening democracy, and the rise of China threatening U.S. competitiveness, there is no time like the present for the United States to recommit to global digital policy leadership—not by aping the anti-innovation regime of Europe, but by resurrecting and modernizing America's original digital policy framework that led to economic success and consumer benefit. To do this, presidential administrations will have to make up their mind: Do they want to import an EU-style digital regulatory approach, which will have the result of damaging U.S. digital leadership and eroding U.S. soft power, or do they want to unambiguously endorse a light-touch, pro-innovation digital agenda?

This report recommends several steps the U.S. government can take to respond to these threats and correct its recent failures:

- The White House should make U.S. global leadership on digital policy a top priority within the current administration's mission to restore America's global standing, rejecting the heavy-handed European approach to digital policy, and making it clear that the American approach of light-touch regulation and targeted pro-innovation policies wins every time.

- The administration should forcefully push back against digital narratives and policies that hurt U.S. businesses and workers, including from allies such as the EU.
- The U.S. government should establish forums for multistakeholder participation in digital policy issues.
- The U.S. government should continue to cooperate with its allies against digital authoritarianism and seek out additional opportunities to do so.
- The State Department should lead a global narrative promoting the United States' pro-innovation approach to digital policy and why that approach, as opposed to China's or the EU's, is the key to digital-economy success in other nations.
- The State Department should push back against the United Nations Commission on Trade and Development's (UNCTAD's) "digital victims" narrative and explain why digital innovation in higher-income nations is key to driving development in lower-income nations.
- The State Department should stop funding organizations that misleadingly paint U.S. digital policy and performance in a bad light.
- The International Trade Administration (ITA) should expand its Digital Attaché Program.
- The U.S. Trade Representative (USTR) should push for more countries to sign onto the Information Technology Agreement.
- USTR should collaborate with America's allies on agreements and initiatives that facilitate cross-border data flows.
- The U.S. International Trade Commission (ITC) should better analyze digital protectionism by other countries and the U.S. Department of Commerce and USTR should develop a strategy to fight it.
- The National Institute of Standards and Technology (NIST) should take on a greater global leadership role in setting international standards and best practices.
- Congress and the Department of Justice should lead on addressing concrete online harms such as revenge pornography, data breaches, cybercrime, and intellectual property (IP) theft domestically.
- Congress should maintain a pro-innovation approach to regulating digital policy issues.

THE HISTORY OF AMERICAN DIGITAL POLICY LEADERSHIP

By taking the lead on important and emerging issues, including digital policy, the federal government in the United States can more effectively promote American interests, which would increase U.S. competitiveness and ultimately strengthen the U.S. economy. Global leadership on digital policy also allows the United States to spread American values, including innovation, democracy, independence, equality, individualism, and meritocracy.[2]

The U.S. system is built on these values, which have produced world-leading digital firms and a thriving digital sector that creates jobs and wealth for millions of Americans and boosts overall U.S. competitiveness on a global scale. According to the Bureau of Economic Analysis, in 2021,

the U.S. digital economy was responsible for 10.3 percent of U.S. gross domestic product (GDP) and 8 million jobs.[3]

This success would not have been possible without the pro-innovation policies of the late 1990s that encouraged growth and investment into the then-burgeoning digital economy and formed the foundation of U.S. digital policy.

Clinton Administration Actions

The White House set the tone of U.S. digital policy in the 1990s, largely guided by President Bill Clinton's chief policy advisor, Ira Magaziner. Magaziner drafted the Clinton administration's "Framework for Global Electronic Commerce," released in July 1997, which outlined five principles for American digital policy to facilitate the growth of the digital economy:

1. The private sector should lead.
2. Governments should avoid undue restrictions on electronic commerce.
3. Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent, and simple legal environment for commerce.
4. Governments should recognize the unique qualities of the Internet.
5. Electronic commerce over the Internet should be facilitated on a global basis.[4]

Guided by these principles, it is no wonder that the early days of American digital policy were marked by light-touch regulation and a pro-innovation mindset. Congress followed the administration's lead, recognizing the benefits of this approach. The text of Section 230 of the Communications Decency Act (CDA), one of the most influential Internet laws passed during the Clinton administration years, explicitly states Congress's finding: "The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation."[5]

As indicated by the fifth principle, the United States also engaged in some multistakeholder and international cooperation on certain areas of Internet policy. The "Framework for Global Electronic Commerce" singled out nine areas where international agreement would be especially important, including taxation, electronic payments, e-commerce, IP, privacy, cybersecurity, telecommunications (telecom) infrastructure, content, and technical standards.[6]

Noteworthy Laws

During the Clinton administration, Congress passed several laws that laid the groundwork for the U.S. approach to digital policy at home and abroad. Four of these—the Telecommunications Act of 1996, Section 230 of the CDA, the Digital Millennium Copyright Act (DMCA), and the Internet Tax Freedom Act (ITFA)—remain key pillars of American digital policy and have shaped the modern Internet.

Telecommunications Act of 1996

The Telecommunications Act of 1996 amends the Communications Act of 1934, the previous regulatory framework covering telecom and broadcasting, which was passed during the "Golden Age" of radio when television was still an emerging technology.[7] During the more than 60 years between the passage of the Communications Act and the Telecommunications Act, telecom

technology changed considerably. Radio technology had improved, television had become ubiquitous, and by 1995, 18 million American homes had modem-equipped computers with access to the Internet, according to Pew Research Center.[8]

The Telecommunications Act's stated purpose was to promote competition and reduce regulation in the rapidly developing telecom industry, with the aim of increasing the quality and decreasing the cost of services American consumers had access to, as well as encouraging the development of new technologies. Notable provisions included requiring telecom carriers (not including broadband networks) to interconnect their networks, preempting state or local regulations that would serve as barriers to entry for telecom carriers to provide service, and expanding the Communications Act's principle of universal service—providing telephone service to all Americans at reasonable and affordable rates—to include broadband.[9]

Research conducted by the Brookings Institute in 2016 evaluated the success of the Telecommunications Act after 20 years, concluding that despite an increase in concentration in the telecom industry in the first 5 years following the law's passage, it had achieved its goal of driving investment in new technologies and expanding broadband access and competition.[10] Information Technology and Innovation Foundation (ITIF) research likewise reflects the great strides the United States had made toward universal service: 98 percent of Americans had access to a fixed connection at broadband speeds and 85 percent had a choice between at least two providers, with the country ranking 10th in affordability, in 2022.[11]

Section 230 of the Communications Decency Act

Also in 1996, Congress passed the CDA, which was included as Title V of the Telecommunications Act. The CDA was an attempt to regulate pornographic material on the Internet, criminalizing sending or displaying obscene or indecent content to known minors.[12] A little more than a year after the law's passage, in *Reno v. American Civil Liberties Union* (1997), the Supreme Court Case struck down the CDA's anti-obscenity and anti-indecency provisions on First Amendment grounds.[13]

Parts of the CDA remain, including Section 230, the law governing online intermediary liability—the extent to which a third party is responsible for the online speech of others—in the United States.[14] Then-representatives Chris Cox (R-CA) and Ron Wyden (D-OR) wrote Section 230 in response to recent legal precedent on online intermediary liability.

According to the decisions in two separate court cases, *Cubby v. CompuServe* (1991) and *Stratton Oakmont v. Prodigy* (1995), online services that exercised no control over what users posted on their platforms—including potentially unlawful or abusive content—were not liable for that content, since the service merely distributed the content.[15] However, online services that exercised good faith efforts to moderate content and remove potentially unlawful or abusive material could be liable because, according to the court, they had exercised "editorial control" over that content and were therefore viewed as publishers rather than distributors.[16]

In passing the CDA, Congress wanted to incentivize content moderation, so it included Section 230 to remove the fear of liability and encourage the development of new online services and technologies that would give users control over the information they received.[17] The law contains two main provisions to accomplish this. First, Section 230(c)(1) states that online services and their users are not liable for third-party content, with exceptions for content that violates

copyright or sex trafficking law. Second, Section 230(c)(2) states that online services are not liable for their good faith efforts to remove offensive third-party content.[18]

In addition to removing obstacles to content moderation, Section 230 also protects free speech online by curtailing "collateral censorship," a form of self-censorship that occurs "when *A* censors *B* out of fear that the government will hold *A* liable for the effects of *B*'s speech."[19] This protection is particularly important for online political discourse and marginalized communities online.

Section 230 has enabled a variety of business models that rely on user-generated content, including knowledge-sharing websites, online marketplaces, social media platforms, websites that host product and business reviews, websites with comment sections, and countless blogs and forums. By keeping frivolous lawsuits at bay, thereby keeping legal costs down, Section 230 makes it easier for these business models to operate, promoting innovation and competition in these spaces in a way that ultimately benefits consumers.[20]

Compared with the rest of the world, the United States was an early mover on codifying its approach to online intermediary liability, giving it a competitive advantage in the burgeoning digital economy and setting a global norm reflected in the similar approaches many other countries later took in their own laws.[21] The language of Section 230 is also present in two of the United States' trade agreements: the U.S.-Japan Digital Trade Agreement, signed in 2019, and the United States-Mexico-Canada Agreement, which replaced the North American Free Trade Agreement in 2020.[22]

Section 230 has enabled a variety of business models that rely on user-generated content.

Particularly in recent years, Section 230 has drawn criticism from both Republicans and Democrats as a result of the ongoing techlash and partisan disagreement on how to move forward on issues related to political speech online.[23] Regardless, the law remains one of the cornerstones of U.S. digital policy, and will likely continue to play an important role with the introduction and growth of emerging technologies such as artificial intelligence (AI) and augmented reality and virtual reality (AR/VR).[24]

Digital Millennium Copyright Act

In 1998, just two years after passing the Telecommunications Act and Section 230, Congress passed the DMCA, which implemented the World Intellectual Property Organization (WIPO) Copyright Treaty (WCT) and Performances and Phonograms Treaty (WPPT).[25] WIPO is an agency of the United Nations created to promote and protect IP. Signatories of the WCT and WPPT agreed to protect the rights of copyright holders in the digital environment, with the WCT protecting authors and the WPPT protecting performers and producers of phonograms (a legal term encompassing recordings of music, spoken words, and sounds). Both treaties were concluded in 1996 and entered into force in 2002.[26]

In order to implement these treaties and effectively protect rightsholders, the DMCA includes provisions that outlaw circumventing technological measures that control access to a copyrighted work or distributing tools that would enable circumvention. The DMCA also establishes a safe

harbor for online services against liability for copyright infringement, which is similar in principle to Section 230 but differs in its execution.

Under the DMCA, online services are not liable for third-party content that violates copyright law as long as they "expeditiously" remove or disable access to the content upon becoming aware of it. There are three conditions that trigger this removal requirement: First, an online service has "actual knowledge" of infringing content; second, an online service is aware of "facts or circumstances from which infringing activity is apparent" (commonly referred to as "red flag knowledge"); or third, an online service receives a valid notice from a copyright owner alerting the service to infringing content.[27]

The DMCA has received some criticism, including over abuses of the notice and takedown system, though there are protections in place to minimize the potential for abuse.[28] Individuals who post content an online service removes due to a takedown notice can file a counter-notice that the content is not infringing, which then obligates the online service to restore access to the content.[29]

Widespread piracy would limit the ability of content producers to create legitimate business models for selling digital content, hinder U.S. competitiveness in content industries, and hurt law-abiding consumers who must pay higher prices for content or have access limited to less or lower-quality content. The toll of piracy is already significant, representing billions of dollars in lost revenue for the creators, publishers, and distributors of movies, TV programs, music, books, and software.[30] Strong copyright protections benefit the economy by creating revenue and jobs in these and other industries.

Like Section 230, the DMCA and related IP issues will likely be even more important with the emergence of AI and the metaverse, raising new challenges for lawmakers to consider.[31]

Internet Tax Freedom Act

Also in 1998, Congress passed the ITFA, establishing a three-year moratorium on Internet-specific taxes, including on Internet access or multiple or discriminatory taxes on electronic commerce (e-commerce).[32]

A multiple tax occurs when multiple jurisdictions at the same level of government—for example, multiple states—charge tax on the same e-commerce transaction. Thus, under the ITFA, if a consumer living in one state purchases a product online from a business located in another state, only one of those states can charge tax on the purchase. Meanwhile, the ITFA's ban on discriminatory taxes forbids jurisdictions from levying additional taxes or a different tax rate for e-commerce transactions compared with similar transactions that occur in person or via other means, such as over the phone.

Without the ITFA, consumers would pay more taxes for goods and services purchased online than they would if they purchased those same goods and services in person. This would create an unnecessary barrier to e-commerce, to the detriment of consumers who benefit from the larger variety and increased convenience of shopping online. Businesses also benefit from e-commerce in many ways, from gaining access to new customers to reducing overhead costs by opening online storefronts instead of physical ones. In turn, e-commerce benefits the entire economy through increased efficiency and productivity.[33]

The ITFA was instrumental not only in the growth of e-commerce, but also in broadband adoption. Taxing Internet access would create another unnecessary barrier for consumers, but unlike multiple or discriminatory taxes, this barrier would not only affect e-commerce. Considering how the Internet has become a key enabler of commerce, education, government services, and civic participation, consumers would suffer on multiple fronts. Internet access is also a fundamental component of increasing productivity and growth in the digital economy. Under the ITFA, American tax policy reflects that Internet access is not merely a consumer good but rather also a tool used by producers to increase economic efficiency and lower the cost of production.

The ITFA's initial three-year moratorium was extended multiple times and eventually became permanent when Congress passed the Trade Facilitation and Trade Enforcement Act of 2015, signed into law by President Obama in 2016. In addition, the ITFA's grandfather clause, which allowed states that had already implemented a tax on Internet access before the law's passage to keep those taxes in place, expired in 2020, removing another barrier to broadband adoption.[34]

International Cooperation

In addition to its successful, pro-innovation approach to digital policy domestically, the United States collaborated with other nations on multiple initiatives in the 1990s and early 2000s, establishing its position as a global digital policy leader. The United States took an active role in leading negotiations of global agreements on important issues such as IP and cybercrime.

For example, the United States was one of the leading countries to push for an international approach to IP via WIPO treaties, the WCT, and WPPT. This was in part because the United States' domestic copyright proposals had met resistance in Congress and acting on an international stage produced faster results.[35]

Likewise, the United States lobbied within the World Trade Organization (WTO) for the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). The resulting TRIPS Agreement entered into force in 1995 and was the first multilateral trade agreement to address IP.[36] TRIPS requires all WTO members to protect and enforce IP rights in a way that promotes innovation and the dissemination of technology. The agreement includes specific enforcement mechanisms, remedies, and dispute resolution processes countries must use for copyright. TRIPS also includes an enforcement mechanism for holding countries accountable for violations of the agreement via the WTO's dispute settlement procedures.[37] The United States also uses its trade agreements with other nations to advance IP rights through trade.[38]

Additionally, the United States actively participates in the Council of Europe's adoption of the Budapest Convention on Cybercrime, the first international treaty that addresses cybercrime. The Budapest Convention provides a common approach for signatories to take regarding cybercrime, including copyright infringement, fraud, child sexual abuse material, hate crimes, and hacking. It also enables signatories to cooperate with one another to investigate and prosecute cybercrime. The treaty was opened for signing in 2001 and went into effect in 2004. To date, 68 countries have signed and ratified the treaty, including the United States.[39]

Leading on international digital policy efforts enables the United States to spread values of democracy and innovation beyond its borders. It also helps the country maintain its competitive edge in IT. For example, advancing global IP rights allows American companies to compete in

international markets where they might otherwise have to compete with counterfeit and pirated goods and services.

A Multistakeholder Approach

The final hallmark of America's early approach to digital policy was a multistakeholder approach that encourages cooperation and consensus-building between academic researchers, nonprofits, businesses, and government when setting standards and making policy for the Internet. The U.S. government has encouraged a multistakeholder approach, even when doing so involved giving up some of its own direct control over the Internet, to build a more inclusive and transparent governance process.

While the details of digital policy can vary from country to country, there are key issues that require standardization for the Internet to function. One of these issues is the matter of Internet Protocol (IP) addresses and domain names. An IP address is a unique string of numbers that identifies each device connected to a network, enabling devices to communicate with each other. Meanwhile, a domain name is a unique string of text that corresponds to a website. For example, itif.org is the domain name that corresponds to ITIF's website.

The Internet Assigned Numbers Authority (IANA), officially established in 1988 but informally existing since the 1970s, oversees IP address allocation and domain names, among other necessary functions. Originally this task fell to one man, "numbering czar" Jon Postel, a computer scientist and researcher at the University of Southern California. But as the Internet grew, the Department of Commerce recognized the need for a new organization.[40]

The U.S. government has encouraged a multistakeholder approach, even when doing so involved giving up some of its own direct control over the Internet, to build a more inclusive and transparent governance process.

In 1998, the National Telecommunications and Information Administration (NTIA) issued a proposed rule on "Improvement of Technical Management of Internet Names and Addresses," informally known as the "Green Paper."[41] As a result, the Internet Corporation for Assigned Names and Numbers (ICANN) was incorporated in California as a nonprofit and took over IANA's functions, handling issues such as cybersquatting—the practice of registering domain names with the intent of profiting off someone else's trademark—and conflicts over domain names.[42]

Since 2009, the U.S. Department of Commerce no longer supervises ICANN.[43] Today, ICANN's board of directors includes members from around the world and its governmental advisory committee has representatives from 181 governments, including the United States.[44]

A similar example of the United States promoting a multistakeholder approach is the Internet Engineering Task Force (IETF). The organization, founded in 1986, makes voluntary standards for Internet users, network operators, and equipment vendors, including the technical standards for the communication protocols used in the Internet. This standards-setting process involves IETF producing requests for comments (RFCs) and turning those RFCs into standards, with participation from researchers and implementation by software developers, hardware manufacturers, and network operators.[45]

THE NEW STATUS QUO

Despite successfully establishing its digital policy leadership in the 1990s and early 2000s with pro-innovation policies, an active role in multilateral forums, and a multistakeholder approach, the United States has faltered in recent years, due in part to a lack of interest in digital policy and rising antitech sentiment. Meanwhile, other countries have stepped in to fill the void, either by spreading their own global influence on digital policy or turning inward and taking a nationalist approach. This new dynamic threatens American and democratic values and U.S. competitiveness.

American Leadership Failures

U.S. digital policy leadership has been declining over the past two decades, which have been marked by multiple failures from recent administrations and Congress. In particular, growing partisanship, antitech sentiment, and lack of interest have stalled progress on digital policy in the United States, creating a vacuum of power the EU has begun to fill with policies that fail to prioritize innovation and China has taken advantage of to increase its influence.

America's digital policy woes started at the top. After the Clinton administration's strong focus on technology, subsequent administrations largely failed to follow up. Early on in the George W. Bush administration, digital policy issues took a backseat following the events of September 11, 2001, which shifted the government's focus to the wars in Afghanistan and Iraq and the global war on terror.[46]

President Obama gained a reputation as a tech-savvy president, taking advantage of social media to expand his bully pulpit to a new medium. His administration saw some digital policy successes as the Federal Communications Commission (FCC) developed its National Broadband Plan to expand Americans' access to high-speed Internet and, later, established guidelines for 5G.[47] But the White House pressured then-FCC chairman Tom Wheeler to take a vastly over-regulatory approach to net neutrality that was not needed and only incited partisan bickering.[48]

America's digital policy woes started at the top. After the Clinton administration's strong focus on technology, subsequent administrations largely failed to follow up.

The FCC net neutrality regulations passed during the Obama administration were rightly scrapped during the Trump administration. But this regulatory back and forth created uncertainty for businesses and highlighted the need for net neutrality legislation, which still does not exist.[49] President Trump withdrew from the Trans-Pacific Partnership (TPP), a trade agreement President Obama spearheaded between 12 trans-Pacific countries that, among other benefits, would have protected global data flows by prohibiting data localization policies that confine data to within a country's borders.[50]

Finally, President Biden's digital policy has reflected the current techlash, calling on Republicans and Democrats to unite against "Big Tech" in a *Wall Street Journal* op-ed calling for federal privacy legislation, changes to Section 230, and stronger enforcement of antitrust law.[51] This size-based approach to regulation fails to recognize that harm can occur on any online service of any size. Moreover, large tech companies benefit the U.S. economy by creating exports, innovation, and high-wage jobs with good benefits.[52]

The Biden administration also launched the Declaration for the Future of the Internet, a nonbinding statement signed by 61 countries, including the United States and all EU member states. The goal of the statement is to promote universal Internet access, data privacy and security, fair economic competition, secure and interoperable digital infrastructure, freedom of expression, and sustainability.[53] However, the signatory countries are unlikely to reach an agreement on all these issues—and if they do, they may end up letting the strongest regulator (the EU) impose its regime on everyone else, which would essentially mean exporting European overregulation around the world.[54]

Outside the White House, and particularly in recent years, increased partisanship within the Federal Trade Commission (FTC) has blocked progress on digital policy and other issues.[55] Antitech sentiment has also taken hold within the agency. FTC's chair, Lina Khan—nominated by President Biden in 2021—has long expressed criticism of Big Tech companies such as Apple, Amazon, Meta, and Google.[56] Under Khan, FTC has taken a new, populist approach to antitrust, particularly targeting Big Tech companies, that fails to prioritize consumers and innovation.[57]

At the same time, when more moderate voices in the administration attempt to push back against egregious EU actions in order to protect U.S. firms and workers, they are kept on a short leash and criticized. This was the case when seven progressive members of Congress criticized Secretary of Commerce Gina Raimondo's efforts to negotiate new digital trade rules in the Indo Pacific Economic Framework that would extend nondiscrimination principles, which prohibit countries from enacting policies that purposely discriminate against a firm from another country, to digital commerce. The members argued that these nondiscrimination provisions would undermine progressive competition and antitrust goals.[58] This argument amounts to sacrificing global market share for U.S. tech firms—which improves the U.S. trade balance, spurs growth, and supports good jobs—in the name of attacking large American firms.[59] The U.S. government also failed to release an official position on the EU's AI Act, instead only circulating an "unofficial" position to European government officials pushing for changes to the proposed legislation.[60]

Congress has also dropped the ball on spectrum policy in recent years. America used to lead the world as the first to auction spectrum licenses, which drove the development of the wireless economy. However, American leadership in this area is now at risk. In 2023, Congress let the FCC's auction authority lapse and failed to create incentives to repurpose federal spectrum for more productive commercial uses. If Congress does not reinstate the FCC's auction authority, it could reduce America's access to next-generation wireless technologies and applications.[61]

European Overregulation and Regulatory Imperialism

The European approach to digital policy, though marked by some shared values with the United States and other democratic countries, differs from the U.S. approach. The U.S. approach is pro-innovation, marked by minimal regulation, which has enabled U.S. firms to emerge as leaders in the digital space and boosted U.S. economic competitiveness. On the other hand, Europe takes a precautionary approach, marked by overregulation and skepticism of new technology, which limits innovation and growth.[62] Moreover, U.S. policy is based on a tradition of free speech (while the EU restricts some forms of speech that are legal in the United States) and the EU antitrust approach is based on protecting competitors (while the U.S. approach is based on protecting consumers).

No law exemplifies the European approach to digital policy better than the EU's General Data Protection Regulation (GDPR), adopted in 2016 and implemented in 2018. The GDPR is a comprehensive data privacy law touted by the EU as "the toughest privacy and security law in the world."[63] It applies to data controllers and processors either established in the EU or that process Europeans' personal data and enshrines certain rights of users and responsibilities of data controllers and processors.

Notable rights in the GDPR include the right of users to access, port, delete, or rectify their personal data. Responsibilities of data controllers and processors include retaining data protection officers, completing impact assessments, obtaining opt-in consent from users to process their personal data, and notifying users when their data is compromised. The GDPR also mandates transparency in data collection practices, data minimization (collecting no more data than is necessary to meet specific needs), purpose specification (disclosing the purpose of data collection to users and only using data for those purposes), and privacy by design.[64]

Evidence about the effects of the GDPR following its implementation demonstrates the economic consequences of European overregulation.

Several of the GDPR's provisions impose high costs on data controllers and processors and even translate to high costs to the EU economy in the form of less productivity and innovation. For example, obtaining opt-in consent from users is significantly costlier than providing users the ability to opt-out and results in far fewer users giving their consent, which leads to less data and therefore fewer beneficial uses of data.[65] Less data also reduces the effectiveness of targeted advertising, an important source of revenue for many businesses.[66]

Additionally, data minimization and purpose specification limit beneficial uses of data. Data minimization limits organizations' ability to analyze data in the development of new products and services, and purpose specification restricts organizations from reusing collected data for new purposes or applying data analytics to collected data. Both of these provisions limit the potential for future innovation.

Evidence about the effects of the GDPR following its implementation demonstrates the economic consequences of European overregulation. A 2019 report by ITIF's Center for Data Innovation finds that, in its first year, the GDPR negatively affected the EU economy and businesses, drained company resources, hurt European tech start-ups, reduced competition in digital advertising, strained regulatory resources, negatively impacted users' online access, presented difficult or impossible implementation and compliance challenges for businesses or entire countries, and failed at its objective of increasing consumer trust.[67]

The GDPR has also inflicted major harm on businesses and consumers in non-EU countries, including the United States. Researchers from the University of Oxford found in 2022, from a sample of companies across 61 countries and 34 industries, that firms affected by GDPR experienced an 8 percent reduction of profits and 2 percent reduction of sales after enforcement of the law began. Notably, small firms—those with fewer than 500 employees—saw a greater reduction in profits and sales than did larger firms, though firms of all sizes suffered.[68] According to the National Bureau of Economic Research, the GDPR also led to a reduction of innovative apps by over one-third, while the entry of new apps fell by one-half.[69]

Additionally, the European Court of Justice decided in July 2020 in *Schrems II* that the EU-U.S. Privacy Shield—a transatlantic legal framework for data protection that made it easier for organizations to manage and transfer data in a way that complied with the GDPR—was not sufficient to protect Europeans' personal data.[70] The demise of the Privacy Shield affected more than 5,000 firms in the United States and Europe.[71]

Despite these consequences, the EU has continued its precautionary approach with more recent legislation. It adopted the Digital Services Act package, including the Digital Services Act (DSA) and Digital Markets Act (DMA), in 2022, with covered entities required to comply by 2024. The DSA replaces and updates the E-Commerce Directive (2000) governing online intermediary liability, while the DMA is meant to increase competition in digital markets and governs "gatekeepers," certain large online platforms that serve as intermediaries between users and businesses.[72]

The E-Commerce Directive protected online services from intermediary liability if they provided caching or hosting services or acted as "mere conduits" of information, meaning they did not create or modify the information or select its recipient.[73] The DSA contains similar wording but adds a number of other obligations for online services. Namely, it requires online services to take measures to counter illegal content and activity, allow users to challenge content moderation decisions, and provide transparency into algorithms used for recommendations. It also bans advertisements that target children or use certain categories of personal data to target users and creates additional obligations for large online services, including independent audits, risk management, codes of conduct, and giving researchers and authorities access to data.[74]

Meanwhile, the DMA creates obligations for "gatekeepers" related to their treatment of businesses that use the gatekeeper platform to connect with users and consumers who use the gatekeeper platform to connect with businesses. These obligations arbitrarily apply to certain companies and give an unfair advantage to those companies' competitors—and are therefore likely to deter innovation. Additionally, by providing EU member states with enforcement powers, the DMA also increases regulatory fragmentation in Europe, which makes it difficult for companies to scale across multiple countries.[75]

Moreover, the DSA and DMA disproportionately target American firms, despite being European laws. European regulators singled out 19 platforms as large online services subject to additional obligations in the DSA. Of these 19 platforms, 15 are American, 2 are Chinese, and only 2 are European.[76] American companies are also likely to dominate the ranks of gatekeeper platforms subject to the DMA: platforms with EU turnover of over €7.5 billion in the last three fiscal years or fair market value of at least €75 billion in the last fiscal year, more than 45 million monthly active users in the EU, and more than 10,000 yearly active business users in the EU, along with a few other qualifiers.[77] This is part of a larger trend of Europe unfairly attacking U.S. tech firms while still expecting to retain access to and continue to benefit from the services these firms offer.[78]

As a final example of European overregulation, the AI Act is a proposed regulation that would serve as the EU's legal framework for AI. It categorizes AI applications into three categories based on risk: those that create an unacceptable risk and are banned, those that are high-risk and are regulated, and those that are low-risk and are unregulated. Applications create an unacceptable risk if they violate fundamental rights or EU values, with specific examples

including AI-based social scoring by public authorities and real-time remote biometric identification systems for law enforcement. Applications create a high risk if they would risk the health and safety or fundamental rights of individuals, with specific examples including biometric identification and categorization, management and operation of critical infrastructure, education and vocational training, employment, access to essential services, law enforcement, migration and border control, and administration of justice and democratic processes.[79]

Driven by fears—both founded and unfounded—of AI's potential impact on society, the AI Act risks deterring research and investment in AI due to the high compliance costs associated with high-risk applications, including conformity assessments, transparency requirements, and post-market monitoring obligations. The AI Act also fails to achieve the EU's goal of technology-neutral regulation in that it regulates certain AI applications more strictly than other technologies that could create similar risks. A truly technology-neutral approach would focus on the novel risks posed by AI.[80]

Proponents of the European approach to digital policy call it "values based," and compare it favorably to the U.S. approach, which they see as driven by corporate interests and greed.[81] But the U.S. approach is equally based on values, though not necessarily the same ones. The United States more highly values innovation, progress, and growth, and this is reflected in its approach to digital policy.

If the European approach were as effective as proponents claim, the EU would not need to unfairly target U.S. tech firms with its laws, in effect punishing the United States for the success of its pro-innovation approach. By comparison, Europe has failed to produce world-leading digital firms and has lost market share, especially to China.[82] Clearly the United States is more effective at producing innovative, globally competitive firms, and the EU would do better to emulate the U.S. approach rather than double down on overregulation, which will only continue to undermine European competitiveness.

Unfortunately, despite its flaws, the European approach has had an outsize influence on other countries, a phenomenon known as the "Brussels effect." This is in part due to a lack of American action and leadership on digital policy in recent years, but also due to the EU's extraterritorial regulation, exemplified by the GDPR, DSA, and DMA.[83]

The GDPR is a prime example of this process. Not only does the GDPR apply to many non-EU data controllers and processors—effectively giving the EU the power to regulate non-EU companies—but since its adoption, it has also influenced many non-EU jurisdictions' privacy laws. Notably, the California Consumer Privacy Act (CCPA), the first state-level comprehensive data privacy law passed in the United States, drew inspiration from the GDPR. In turn, since its passage in 2018, the CCPA has inspired other state-level privacy laws in the United States.

Via the Brussels effect, the EU has taken a global lead on certain digital policy issues, exporting its precautionary approach outside its borders, including to the United States. If America does not step back up to its role as a digital policy leader to advance a pro-innovation agenda, it will continue to lose its competitive edge, which is crucial not only for U.S. economic growth but also for balancing against the growing Chinese influence. Stepping up does not mean mimicking European-style regulations, but rather promoting and defending the type of light-touch digital regulations that have led to many of America's economic successes in the digital economy.

Rise of Digital Protectionism

In the Internet's early days, its more idealistic proponents believed that the Internet would break down national barriers by facilitating worldwide communication and the spread of information. The Internet has certainly revolutionized society in many positive ways, but national barriers remain as relevant as ever, and countries have asserted those barriers in the digital space as much as they do in the physical realm, including by establishing and enforcing policies that restrict digital free trade and cross-border data flows.

Many of these policies fall under the category of data localization. Data localization policies include restricting the transfer of certain types of data outside a country's borders, restricting the transfer of broad categories of data deemed "sensitive," and de facto localization policies that make data transfers so cumbersome that firms have no real option but to store data locally. These policies are increasingly popular. According to ITIF research, 62 countries had implemented data localization policies in 2021, compared with 35 in 2017.[84]

This recent trend toward economic nationalism threatens innovation and economic growth worldwide. The digital economy depends on the free flow of data, and given the increasing importance of the digital economy to countries' overall economic well-being, it is no surprise that restricting data flows has an overall negative impact on a country's economy, including by reducing the volume of trade, lowering productivity, and increasing prices for industries that rely on data.[85]

Despite the costs, countries have multiple justifications for their digital protectionism. Some cite data privacy and security concerns and the need for law enforcement and regulatory oversight of data.[86] Others are more open about their protectionism, albeit using different terms. For example, European officials call for "digital sovereignty," or "taking back control" from foreign (usually U.S.-based) firms and trading partners, similar to the EU's justification for its regulations, such as the DSA and DMA, that disproportionately target American firms.[87] Developing countries frame the issue in a similar way, portraying data localization policies as fighting against "digital colonialism" by the United States.[88]

Unsurprisingly, authoritarian countries are frequently among the top offenders when it comes to data localization, as requiring foreign firms to store data locally allows for greater censorship and surveillance. China and Russia both have numerous local data storage requirements.[89] Unfortunately, these and other authoritarian countries are far from the only offenders. Multiple democratic nations have their own data localization laws dating back at least a decade. Australia prohibited the overseas storage of electronic health records in 2013, Germany included local data storage requirements in a 2016 telecommunications law, and India's central bank enacted data localization requirements for payment data in 2018, to name a few.[90]

Other forms of digital protectionism and "innovation mercantilism"—the strategy of using protectionist policies to expand domestic production and exports of high-tech goods and services—take the form of local content requirements or mandates that a certain percentage of goods and services sold in a country be produced with local content. Such requirements exist in Russia (for pharmaceutical production), Uruguay (for wind farms), and Nigeria (for information, communications, and technology products), to name a few.[91]

Local content requirements may boost affected domestic industries in the short term, but they come with multiple long-term detrimental effects. Most obviously, they ensure that consumers predominately have access to lower-quality goods and services. If an industry produced high-quality goods and services, it would not require protectionist intervention. Local content requirements instead give an unfair advantage to domestic industries that would otherwise fail to compete with higher-quality foreign goods and services.

Beyond the immediate effect on consumers, local content requirements create and exacerbate inefficiencies in the affected industries because domestic firms have little incentive to innovate in order to outperform their foreign competitors. Local content requirements are also detrimental to unaffected sectors of the economy. Research from the Organization for Economic Co-operation and Development (OECD) finds that countries with local content requirements experience a decrease in exports from nonaffected sectors as the country's economic activity becomes increasingly concentrated on the affected industries.[92]

The digital economy depends on the free flow of data, and given the increasing importance of the digital economy to countries' overall economic well-being, it is no surprise that restricting data flows has an overall negative impact on a country's economy.

Some countries, including the United States, have enacted government procurement policies that favor goods and services produced domestically. Proponents of this "Buy American"—or "Buy European," or whatever the case may be—approach often cite national security concerns, boosting competitiveness of a domestic industry, job creation, or a combination of the three as their justification. But in some cases, these policies are based on flawed analysis and would not produce their desired results. For example, the Build America Buy America Act, part of the 2021 Infrastructure Investment and Jobs Act, may require the federal government to maximize its use of domestically produced information technology (IT) in infrastructure projects. This is likely to raise costs and reduce infrastructure build, which would run contrary to the law's purpose.[93]

Finally, some countries enact digital protectionist policies under the guise of trying to revive struggling industries. These frequently take the form of "tech pays" proposals, which require major tech companies—once again, disproportionately U.S.-based firms—to pay for news content, entertainment media, or broadband.

Proposals to make news aggregators pay publishers for content typically target Google News and Facebook. Such proposals, which have cropped up in Belgium, Germany, Spain, France, Australia, and Canada with mixed results, stem from concerns over the decline of local journalism and failure of some publishers to adapt to changes in how news is delivered and consumed in the Internet age. However, the truth is news aggregators drive traffic to publishers in ways that were previously impossible. This leads to more clicks on news stories and more advertising and subscription revenue for publishers. On the flip side, many attempts to force news aggregators to pay for content has resulted in aggregators limiting or removing news content in those countries, less traffic and revenue to publishers, and decreased access to news for residents of those countries.[94]

Similarly, Canada passed a law in 2023, the Online Streaming Act, that will require streaming services such as Netflix, Disney+, and Spotify to pay for and promote Canadian content. The law

is designed to bolster Canada's creative industries—and once again, American companies must foot the bill.[95] Australia also has announced plans to impose local content quotas on international streaming services starting in 2024 as part of the government's five-year "Revive" National Cultural Policy.[96]

Finally, telecom companies in multiple jurisdictions, including the EU and South Korea, have pushed for tech pays proposals for broadband. Such a framework would force large digital firms such as Google, Netflix, Meta, Apple, Amazon, and Microsoft—all American companies—to pay fees toward telecom infrastructure in order to fund 5G and fiber networks. The justification behind these proposed fees is that these companies generate a large amount of Internet traffic.[97] But ultimately these fees are likely to be passed onto consumers. Otherwise, if companies foot the bills, the quality of their services is likely to decline.

These examples prove that few, if any, countries are innocent of digital protectionism and innovation mercantilism. However, China is by far the most flagrant and frequent offender. As of 2021, China had the most regulations on data—including data localization and de facto localization policies—of any country in the world, according to ITIF research. In fact, with 29 regulations, China had more than twice as many regulations as India, in second place with 12.[98] China also imposes local content requirements on government procurement, in violation of the WTO's Agreement on Government Procurement (GPA), although China is not a party to, and therefore not currently bound by, the GPA.[99]

Innovation mercantilism is a hallmark of Chinese digital policy. The Chinese government limits foreign firms' access to the Chinese market and thus their global market share. Meanwhile, Chinese firms benefit from tax incentives, subsidies, low-cost financing, forced technology transfers, and IP theft. This dynamic impacts not only countries with otherwise successful firms that compete with Chinese firms but also the global economy as less innovative Chinese firms unfairly outcompete more innovative foreign firms, leading to less global innovation.[100]

The global trend of digital protectionism, and particularly China's innovation mercantilism, represents a growing threat to innovation, free trade, and U.S. competitiveness. This trend is likely to continue without a strong response from the United States and its allies, including a commitment to digital free trade and pressure for China to abide by the global, rules-based trading system.

Democracy Under Threat

Just as the United States has been able to leverage its digital policy leadership to spread American and democratic values, authoritarian countries have turned to digital policy as a means of achieving their ends. As many democratic nations have turned away from global cooperation and toward digital protectionism in their digital policy, China and Russia have exerted more control over their respective spheres of influence. Meanwhile, the United States and its allies have neglected to properly respond to this growing threat.

The Western democratic approach to digital policy prioritizes free speech, personal privacy, and individual freedom online. But China and Russia have taken the opposite approach: digital authoritarianism, which is marked by censorship, surveillance, and state control.

Western media often exaggerates the sophistication and extent of China's surveillance. Much of this misinformation centers around an alleged social credit system in China that gathers data about citizens' behavior from mass surveillance, collects and ranks that information using AI algorithms, and assigns each citizen a social score that determines their place in society, with rewards for high scores and punishments for low scores. However, the reality of social credit in China is that the system is far more disorganized, less widespread, and lower tech than its portrayal in Western media.[101]

The myth of China's social credit system obscures the reality of surveillance in the country. Much of this surveillance takes place in the Chinese province of Xinjiang, where the government holds up to 1 million of the ethnic Uyghur people in "political reeducation" camps. Human Rights Watch reverse-engineered an app the police and other officials in Xinjiang use to collect residents' personal information, report on "suspicious" activities, and investigate people flagged as "problematic," with examples of activities deemed suspicious including use of virtual private networks (VPNs) or encrypted online services, engaging in Islamic religious activities, and any activity that deviates from an individual's normal behavior. The Chinese government justifies this surveillance as a means to combat extremism and terrorism.[102]

The Western democratic approach to digital policy prioritizes free speech, personal privacy, and individual freedom online. But China and Russia have taken the opposite approach.

The Chinese government also heavily censors the Internet within its borders, blocking access to many websites, including Facebook, Twitter, and Instagram.[103] In the first quarter of 2023, the Cyberspace Administration of China, the country's Internet regulator, shut down 4,200 websites, removed 55 apps from app stores, and ordered the administrators of 2,200 websites to rectify their content for offenses such as providing unauthorized news content and failing to stop the spread of "harmful content." The government also deletes individual accounts that spread misinformation or politically liberal ideology, and has blocked many VPNs that would allow Chinese residents to access banned content. Collectively, these government actions make up the country's "Great Firewall," which sections off the Chinese Internet from the global Internet.[104]

Russia engages in similar censorship with an Internet blacklist created in 2012 that allows Roskomnadzor, the country's media regulator, to block any website for any reason, without oversight. The list includes independent news sites and websites run by political opposition leaders. Meanwhile, Russian antiterrorist law requires IT companies to retain copies of all user communications for six months and communications metadata for three years, and companies must turn this data over to the authorities upon request. Like China, Russia also restricts residents' access to VPNs.[105]

Both China and Russia prop up domestic tech companies that are willing to accede to government surveillance and censorship, replacing the foreign online services that are popular in other countries. Russia refers to this strategy as establishing a "sovereign Russian Internet."[106] The Chinese and Russian approach present attractive models for other authoritarian regimes, which could lead to a global rise in digital authoritarianism, especially without a strong, unified response from the United States and its allies.

RESTORING AMERICAN LEADERSHIP

In the face of European overregulation, rising digital protectionism, and digital threats to democracy, it is more important than ever for the United States to step back up as a global digital policy leader. From a leadership position, the United States can promote a pro-innovation, pro-democracy, and pro-free trade agenda. A few of the United States' more recent efforts demonstrate that America is still capable of stepping up if it makes global digital policy leadership a top government priority and engages with its allies.

Recent Efforts

The 21st century has not been solely marked by American digital policy leadership failures. A few key policies from the past two decades demonstrate that the United States is still capable of acting as a global leader on digital policy if it maintains a pro-innovation approach and commitment to international and multistakeholder cooperation.

One area where the United States has led is on 5G development and deployment. Toward the end of the Obama administration in 2016, the FCC adopted guidelines for the development of 5G, the fifth generation of wireless cellular technology and the successor to 4G. These guidelines opened up spectrum for 5G networks, making the United States the first country to do so.[107] Under Chairman Ajit Pai, who served from 2017 to 2021, the FCC pursued a strategy of allocating additional spectrum for 5G, updating infrastructure policy, and modernizing regulations to encourage investment in 5G, called the 5G FAST Plan.[108]

The FCC established its 5G Fund for Rural America in 2020, making $9 billion available to make 5G wireless service available in rural areas.[109] Additionally, Congress passed and the FCC implemented the Secure and Trusted Communications Network Act of 2019, which aims to ensure supply chain integrity by establishing a $1.9 billion reimbursement program tor telecom carriers with 10 million or fewer subscribers to "rip and replace" equipment from suppliers that pose "unacceptable risk" to U.S. national security, including Chinese companies Huawei and ZTE.[110]

A second recent digital policy success came out of Congress in 2022: the CHIPS and Science Act. In an effort to strengthen American manufacturing, create jobs, bolster supply chains, and compete with China, the Act provides $76 billion in funding for U.S. semiconductor research and development, manufacturing, and investment. It also provides $81 billion for the National Science Foundation (NSF) over five years for scientific research and STEM (science, technology, engineering, and mathematics) education, nearly $10 billion for NIST for manufacturing, an increase in funding for the Department of Energy, and $10 billion over five years for 20 geographically distributed regional technology and innovation hubs. Additionally, the Act created 25 percent investment tax credits for manufacturing semiconductors and related equipment.[111]

The CHIPS and Science Act spurred an immediate increase in investment in the semiconductor industry. By December 2022, just months after the Act was signed into law, companies had announced more than 50 new semiconductor ecosystem projects in the United States, over $210 billion in private investments in 20 states, and 44,000 new jobs.[112]

Finally, a major forthcoming success for American digital policy leadership will be the Global Cross-Border Privacy Rules (CBPR). The Global CBPR borrows from Asia-Pacific Economic Cooperation's (APEC's) CBPR system, a government-backed privacy certification developed by

APEC's 21 member countries. The system enables the free flow of data between participating countries—currently Australia, Canada, Japan, South Korea, Mexico, the Philippines, Singapore, Taiwan, and the United States—as those governments have a guarantee that data from CBPR-certified companies complies with international data privacy standards.[113] Though China endorsed the system in 2011, it has never joined.[114]

Canada, Japan, South Korea, the Philippines, Singapore, Taiwan, and the United States came together in 2022 to establish the Global CBPR Forum, which will develop a certification system similar to APEC's CBPR, periodically review members' privacy standards, and foster cross-border data flows and interoperability.[115] The Global CBPR regime represents a more realistic data transfer mechanism for countries from around the world to sign up to, as opposed to the EU's top-down drive for harmonization with the GDPR.

The federal government needs to build on these modest successes and turbocharge its pro-innovation digital policy engagement.

Recommendations

Restoring U.S. global leadership on digital policy requires leveraging America's strengths, strengthening America's alliances, and maintaining America's pro-innovation approach. There are a number of actions the federal government can take to correct past leadership failures and respond to the threats of overregulation, digital protectionism, and the authoritarian influence of China and Russia.

- The White House should make U.S. global leadership on digital policy a top priority, expanding on the Biden administration's stated mission to restore America's global standing and setting the tone for the rest of the federal government.[116] In doing so, the White House should reject the heavy-handed European approach to digital policy and make it clear that the American approach of light-touch regulation and targeted pro-innovation policies is more beneficial for consumers, businesses, and the economy.
- The administration should push back against digital narratives and policies that hurt U.S. businesses and workers, including from allies such as the EU. For example, the administration should add European "digital sovereignty" via data localization and the DSA's and the DMA's disproportionate targeting of U.S. firms to its current and future trade discussions with the EU and its member states. Ultimately, if the EU persists in restricting U.S. firms from processing data about Europeans, the U.S. government should respond in kind by creating a reciprocal policy regarding Americans' data held by EU companies. The administration should commit to taking public positions on influential foreign legislative proposals that would hurt U.S. companies and consumers, including the EU AI Act, Canada's Online News Act, and the United Kingdom's Online Safety Bill.
- The U.S. government should establish forums for multistakeholder participation on digital policy issues, particularly among democratic nations that share many of the same values. For example, one such forum should develop a set of voluntary, consensus-based guidelines for social media companies to follow when moderating online political speech.[117]
- The U.S. government should continue to cooperate with its allies against digital authoritarianism and should seek out additional opportunities to do so. Specifically, the

United States and its allies should work together to combat China's and Russia's efforts to expand their influence in the digital sphere and exert more control over other countries' digital policy decisions in ways that run counter to U.S. and democratic values.

- The State Department should lead on a global narrative arguing why the United States' pro-innovation approach to digital policy is best for countries hoping to thrive in the digital economy and compete with China. This narrative should include debunking the "harm gap" between EU and U.S. approaches—the argument that the EU's "values based" approach is significantly more effective than the U.S. approach at protecting consumers from online harm. There is indeed a "third way" between Chinese digital authoritarianism and European statist regulation and the U.S. government needs to actively educate other nations on this reality.
- The State Department should push back against the UNCTAD narrative that developing countries are victims of foreign firms, and therefore they are justified to enact protectionist measures, including data localization, to protect their interests in the digital economy.[118] This should include much more engagement by the U.S. government and other groups such as think tanks in UN-related forums to counter this anti-American narrative and explain why digital innovation in higher-income nations is key to driving development in lower-income nations.
- The State Department should stop funding organizations that misleadingly paint U.S. digital policy and performance in a bad light, including the advocacy group Freedom House's annual *Freedom on the Net* report, which takes a highly subjective, ideological approach to analyzing Internet freedom.[119]
- The State Department should identify and work with a group of small to mid-sized countries that want to increase their competitiveness in the global digital economy and become digital leaders, such as Estonia, Slovenia, and the Kyrgyz Republic. These and other countries are desperate for guidance and support on how to drive digital innovation in their nations. The United States should fill that role. The goal of cooperation should be to advance a pro-innovation, pro-democracy approach to digital policy and champion it on a global stage.
- ITA should expand its Digital Attaché Program, a network of digital trade officers in U.S. embassies currently in 16 markets who help U.S. firms increase their global online market access and navigate regulatory and digital policy challenges.[120] It should also expand the program into new markets in order to continue promoting U.S. firms' global competitiveness.
- USTR should push for more countries to sign onto the ITA, a WTO agreement with 82 signatory countries that have agreed to fully eliminate tariffs on hundreds of IT products. Joining the ITA generates positive economic growth in developing countries and signals to the global community that these countries are open for trade and investment.[121]
- USTR should collaborate with America's allies on agreements and initiatives that facilitate cross-border data flows, such as the renegotiated EU-U.S. Data Privacy Framework that replaced Privacy Shield.[122] These types of frameworks make it easier for organizations to manage and transfer data across borders and thus benefit the digital economy.

- ITC should develop a strategy to define digital protectionist actions by foreign countries, investigate these actions, and take action against offenders when appropriate. The Department of Commerce and USTR should simultaneously enact policies that advance digital free trade.
- NIST should take on a greater global leadership role when it comes to setting voluntary standards and best practices for businesses. It should begin by leveraging its Cybersecurity Framework and AI Risk Management Framework as examples of robust technical standards companies from all countries benefit from following.[123]
- Congress and the Department of Justice should lead on addressing concrete online harms domestically to protect businesses and consumers and set an international example. Congress should outlaw nonconsensual or revenge pornography and establish both a uniform federal standard for data breach notification and a clear regulator for cryptocurrencies and nonfungible tokens (NFTs).[124] Meanwhile, the Department of Justice should continue to pursue perpetrators of cyber and intellectual property crime.
- Congress should maintain the pro-innovation approach to regulating digital policy issues that paved the way for American global leadership in the 1990s. This should include preserving the strong online intermediary protections in Section 230, passing comprehensive data privacy legislation that preempts state laws while promoting digital innovation, and keeping consumer welfare at the heart of antitrust jurisprudence.

About the Author

Ashley Johnson (@ashleyjnsn) is a senior policy analyst at ITIF. She researches and writes about Internet policy issues such as privacy, security, and platform regulation. She was previously at Software.org: the BSA Foundation and holds a master's degree in security policy from The George Washington University and a bachelor's degree in sociology from Brigham Young University.

About ITIF

The Information Technology and Innovation Foundation (ITIF) is an independent 501(c)(3) nonprofit, nonpartisan research and educational institute that has been recognized repeatedly as the world's leading think tank for science and technology policy. Its mission is to formulate, evaluate, and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. For more information, visit itif.org/about.

ENDNOTES

1. Robert D. Atkinson et al., "A Policymaker's Guide to the 'Techlash'—What It Is and Why It's a Threat to Growth and Progress" (ITIF, October 2019), https://itif.org/publications/2019/10/28/policymakers-guide-techlash/.
2. "American Values," U.S. Department of State, accessed May 10, 2022, https://www.state.gov/courses/answeringdifficultquestions/assets/m/resources/DifficultQuestions-AmericanValues.pdf.
3. Tina Highfill and Christopher Surfield, "New and Revised Statistics of the U.S. Digital Economy, 2005-2021" (BEA, November 2022), https://www.bea.gov/system/files/2022-11/new-and-revised-statistics-of-the-us-digital-economy-2005-2021.pdf.
4. "Read the Framework," Clinton White House Archives, accessed July 17, 2023, https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html.
5. 47 U.S.C. § 230 (1996).
6. "Read the Framework."
7. Pub. L. No. 104-104, 110 Stat. 56 (1996); The Editors of Encyclopedia Britannica, "Golden Age of American radio," Encyclopedia Britannica, June 6, 2017, https://www.britannica.com/topic/Golden-Age-of-American-radio.
8. "Americans Going Online… Explosive Growth, Uncertain Destinations" (Pew Research Center, October 1995), https://www.pewresearch.org/politics/1995/10/16/americans-going-online-explosive-growth-uncertain-destinations/.
9. Pub. L. No. 104-104, 110 Stat. 56 (1996).
10. Stuart N. Brotman, "Was the 1996 Telecommunications Act successful in promoting competition?" Brookings Institute, February 8, 2016, https://www.brookings.edu/blog/techtank/2016/02/08/was-the-1996-telecommunications-act-successful-in-promoting-competition/.
11. Jessica Dine and Joe Kane, "The State of US Broadband in 2022: Reassessing the Whole Picture" (ITIF, December 2022), https://itif.org/publications/2022/12/05/state-of-us-broadband-in-2022-reassessing-the-whole-picture/.
12. Pub. L. No. 104-104, 110 Stat. 56 Title V (1996).
13. *Reno v. American Civil Liberties Union, 521 US 844* (1997).
14. 47 U.S.C. § 230 (1996).
15. *Cubby, Inc v. CompuServe, Inc., 776 F. Supp. 135* (S.D.N.Y. 1991).
16. *Stratton Oakmont, Inc v. Prodigy Servs. Co., No. 31063/94, 1995 N.Y. Misc. LEXIS 229* (N.Y. Sup. Ct. May 24, 1995).
17. 47 U.S.C. § 230 (1996).
18. Ibid.
19. Jack MBalkin, "Free Speech and Hostile Environments," *Yale Law School Faculty Scholarship Series* 253 (1999), https://jackbalkin.yale.edu/free-speech-and-hostile-environments.
20. Ashley Johnson and Daniel Castro, "Overview of Section 230: What It Is, Why It Was Created, and What It Has Achieved" (ITIF, February 2021), https://itif.org/publications/2021/02/22/overview-section-230-what-it-why-it-was-created-and-what-it-has-achieved/.
21. Ashley Johnson and Daniel Castro, "How Other Countries Have Dealt With Intermediary Liability" (ITIF, February 2021), https://itif.org/publications/2021/02/22/how-other-countries-have-dealt-intermediary-liability/; Anupam Chander, "Section 230 and the International Law of Facebook," *Yale*

Journal of Law and Technology 24 (2022), https://law.yale.edu/sites/default/files/area/center/isp/documents/chander.pdf.

22. Johnson and Castro, "How Other Countries."
23. Ashley Johnson and Daniel Castro, "Fact-Checking the Critiques of Section 230: What Are the Real Problems?" (ITIF, February 2021), https://itif.org/publications/2021/02/22/fact-checking-critiques-section-230-what-are-real-problems/; Atkinson et al., "A Policymaker's Guide"; "How to Address Political Speech on Social Media in the United States" (ITIF, October 2022), https://itif.org/publications/2022/10/11/how-to-address-political-speech-on-social-media-in-the-united-states/.
24. Ashley Johnson, "Generative AI Is the Next Challenge for Section 230" (ITIF, April 12, 2023), https://itif.org/publications/2023/04/12/generative-ai-is-the-next-challenge-for-section-230/; Daniel Castro, "Content Moderation in Multi-User Immersive Experiences: AR/VR and the Future of Online Speech" (ITIF, February 2022), https://itif.org/publications/2022/02/28/content-moderation-multi-user-immersive-experiences-arvr-and-future-online/.
25. Pub. L. No. 105-304 112 Stat. 2860 (1998).
26. "Summary of the WIPO Copyright Treaty (WCT) (1996)," WIPO, accessed April 28, 2023, https://www.wipo.int/treaties/en/ip/wct/summary_wct.html; "Summary of the WIPO Performances and Phonograms Treaty (WPPT) (1996)," WIPO, accessed April 28, 2023, https://www.wipo.int/treaties/en/ip/wppt/summary_wppt.html.
27. Pub. L. No. 105-304 112 Stat. 2860 (1998).
28. Robert D. Atkinson, Daniel Castro, and Alan McQuinn, "Comments to U.S. Copyright Office on Notice-and-Takedown Process" (ITIF, March 21, 2016), http://www2.itif.org/2016-section-512-comments.pdf.
29. Pub. L. No. 105-304 112 Stat. 2860 (1998).
30. Ashley Johnson, "22 Years After the DMCA, Online Piracy Is Still a Widespread Problem" (ITIF, February 7, 2020), https://itif.org/publications/2020/02/07/22-years-after-dmca-online-piracy-still-widespread-problem/.
31. Daniel Castro, "Critics of Generative AI Are Worrying About the Wrong IP Issues" (Center for Data Innovation, March 2023), https://www2.datainnovation.org/2023-ai-art-ip.pdf; Juan Londoño, Jaci McDole, and Daniel Castro, "IP and the Metaverse: The Digital Millennium Copyright Act Will Face Serious Challenges in the Metaverse" (ITIF, September 19, 2022), https://www2.datainnovation.org/2023-ai-art-ip.pdf.
32. Pub. L. No. 105-277 112 Stat. 2681 Title XI (1998).
33. Aurelien Portuese and Trelysa Long, "The Process of Creative Destruction, Illustrated: The US Retail Industry" (ITIF, October 2022), https://itif.org/publications/2022/10/03/the-process-of-creative-destruction-illustrated-the-us-retail-industry/.
34. Jeffrey M. Stupak, "The Internet Tax Freedom Act: In Brief" (Congressional Research Service, April 2016), https://sgp.fas.org/crs/misc/R43772.pdf.
35. Graeme Dinwoodie, "The WIPO Copyright Treaty: A Transition to the Future of International Copyright Lawmaking," *Case Western Reserve Law Review* 57, no. 4 (2007), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1601235.
36. Peter K. Yu, "The Objectives and Principles of the TRIPS Agreement," *Houston Law Review* 46, no. 4 (December 2009), https://scholarship.law.tamu.edu/cgi/viewcontent.cgi?article=1456&context=facscholar.
37. "Overview: the TRIPS Agreement," WTO, accessed June 30, 2023, https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm.

38. Shayerah Ilias Akhtar, Ian F. Fergusson, Liana Wong, "Intellectual Property Rights and International Trade" (Congressional Research Service, May 2020), https://crsreports.congress.gov/product/pdf/RL/RL34292.
39. "The Budapest Convention (ETS No. 185) and its Protocols," Council of Europe, accessed June 30, 2023, https://www.coe.int/en/web/cybercrime/the-budapest-convention.
40. Joel Snyder, Konstantinos Komaitis, and Andrei Robachevsky, "The History of IANA: An Extended Timeline with Citations and Commentary," Internet Society, May 9, 2016, https://www.internetsociety.org/ianatimeline/.
41. "Improvement of Technical Management of Internet Names and Addresses; Proposed Rule," 63 Fed. Reg. 8825-8833 (February 20, 1998), https://ntia.gov/federal-register-notice/improvement-technical-management-internet-names-and-addresses-proposed-rule.
42. Snyder, Komaitis, and Robachevsky, "The History of IANA."
43. Ibid.
44. "Board of Directors," ICANN, accessed June 5, 2023, https://www.icann.org/en/board/directors; "ICANN Governmental Advisory Committee (GAC)," ICANN, accessed June 5, 2023, https://gac.icann.org/.
45. "Introduction to the IETF," IETF, accessed June 28, 2023, https://www.ietf.org/about/introduction/.
46. Declan McCullagh, "Bush leaves behind a mixed technology legacy," *CNET*, January 19, 2009, https://www.cnet.com/tech/tech-industry/bush-leaves-behind-a-mixed-technology-legacy/.
47. Terrence O'Brien, "Obama's legacy: The most tech-savvy president," *Engadget*, January 21, 2017, https://www.engadget.com/2017-01-21-obamas-legacy-the-most-tech-savvy-president.html.
48. Ezra Mechaber, "President Obama Urges FCC to Implement Stronger Net Neutrality Rules," Obama White House Archives, November 10, 2014, https://obamawhitehouse.archives.gov/blog/2014/11/10/president-obama-urges-fcc-implement-stronger-net-neutrality-rules.
49. Robert D. Atkinson, "Net Neutrality Still Needs a Legislative Fix," *RealClearPolicy*, December 15, 2017, https://www.realclearpolicy.com/articles/2017/12/15/net_neutrality_still_needs_a_legislative_fix.html.
50. Nigel Cory, "How Critics of the 'TPP' Trans-Pacific Partnership Muddle Facts, Fictions and Fears," *Entrepreneur*, October 7, 2016, https://www.entrepreneur.com/science-technology/how-critics-of-the-tpp-trans-pacific-partnership-muddle/283427.
51. Joe Biden, "Republicans and Democrats, Unite Against Big Tech Abuses," *Wall Street Journal*, January 11, 2023, https://www.wsj.com/articles/unite-against-big-tech-abuses-social-media-privacy-competition-antitrust-children-algorithm-11673439411.
52. Robert D. Atkinson, "Be Grateful for 'Big Tech,'" *RealClearPolicy*, June 6, 2018, https://www.realclearpolicy.com/articles/2018/06/06/be_grateful_for_big_tech_110659.html.
53. "A Declaration for the Future of the Internet," White House, published April 28, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf.
54. Ashley Johnson and Robert D. Atkinson, "The Declaration for the Future of the Internet Is an Invitation for the EU to Dictate Global Policy" (ITIF, April 28, 2022), https://itif.org/publications/2022/04/28/declaration-future-internet-invitation-eu-dictate-global-policy/.
55. Leah Nylen, "FTC Faces New Partisan, Legal Headwinds in Writing Privacy Rules," *Bloomberg*, August 11, 2022, https://www.bloomberg.com/news/articles/2022-08-11/ftc-faces-new-partisan-legal-headwinds-in-writing-privacy-rules#xj4y7vzkg; Christine Wilson, "Why I'm Resigning as an FTC

Commissioner," *Wall Street Journal*, February 14, 2023, https://www.wsj.com/articles/why-im-resigning-from-the-ftc-commissioner-ftc-lina-khan-regulation-rule-violation-antitrust-339f115d.

56. Tom Maxwell, "Biden names anti-tech critic as head of the FTC," *Input*, June 16, 2021, https://www.inverse.com/input/tech/biden-names-lina-khan-ftc-chairwoman.
57. Dara Kerr, "Lina Khan is taking swings at Big Tech as FTC chair, and changing how it does business," NPR, March 9, 2023, https://www.npr.org/2023/03/07/1161312602/lina-khan-ftc-tech; Nicole Goodkind, "Lina Khan is the face of the populist antitrust moment. But how much power does the FTC chair wield?" *Fortune* June 30, 2021, https://fortune.com/2021/06/30/ftc-chair-lina-khan-populist-antitrust-movement-what-can-she-do-federal-trade-commission/.
58. Elizabeth Warren et al., "Letter to USTR, Commerce," Congress of the United States, April 21, 2023, https://www.warren.senate.gov/imo/media/doc/2023.04.21%20Letter%20to%20USTR,%20Commerce%20re.%20digital%20trade%20and%20competition.pdf.
59. Nigel Cory and Robert D. Atkinson, "The Administration Should Disregard Progressives' Unfair Attacks on Its Digital Trade Agenda" (ITIF, May 25, 2023), https://itif.org/publications/2023/05/25/the-administration-should-disregard-progressives-unfair-attacks-on-its-digital-trade-agenda/.
60. Luca Bertuzzi, "The US unofficial position on upcoming EU Artificial Intelligence rules," *Euractiv*, October 24, 2022, https://www.euractiv.com/section/digital/news/the-us-unofficial-position-on-upcoming-eu-artificial-intelligence-rules/.
61. Gopal Ratnam, "FCC spectrum auction authority lapses amid questions on military need," *Roll Call*, March 10, 2023, https://rollcall.com/2023/03/10/fcc-spectrum-auction-authority-lapses-amid-questions-on-military-need/.
62. Robert D. Atkinson, "Advancing U.S. Goals in the U.S.-EU Trade and Technology Council" (ITIF, September 2021), https://itif.org/publications/2021/09/13/advancing-us-goals-us-eu-trade-and-technology-council/.
63. Ben Wolford, "What is GDPR, the EU's new data protection law?" GDPR.EU, accessed May 11, 2023, https://gdpr.eu/what-is-gdpr/?cn-reloaded=1.
64. Regulation (EU) 2016/679.
65. Alan McQuinn, "The Economics of 'Opt-Out' Versus 'Opt-In' Privacy Rules" (ITIF, October 6, 2017), https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules/.
66. Ashley Johnson, "Comments to the NTIA Regarding Privacy, Equity, and Civil Rights" (ITIF, March 6, 2023), https://itif.org/publications/2023/03/06/comments-to-the-ntia-regarding-privacy-equity-and-civil-rights/.
67. Eline Chivot and Daniel Castro, "What the Evidence Shows About the Impact of the GDPR After One Year" (Center for Data Innovation, June 2019), http://www2.datainnovation.org/2019-gdpr-one-year.pdf.
68. Chinchih Chen, Carl Benedikt Frey, and Giorgio Presidente, "Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally," *The Oxford Martin Working Paper Series on Technological and Economic Change*, No. 2022-1 (January 2022), https://www.oxfordmartin.ox.ac.uk/downloads/Privacy-Regulation-and-Firm-Performance-Giorgio-WP-Upload-2022-1.pdf.
69. Rebecca Janssen et al., "GDPR and the Lost Generation of Innovative Apps" (National Bureau of Economic Research, May 2022), https://www.nber.org/system/files/working_papers/w30028/w30028.pdf.
70. Joshua P. Meltzer, "The Court of Justice of the European Union in Schrems II: The impact of GDPR on data flows and national security," Brookings Institution, August 5, 2020,

https://www.brookings.edu/articles/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/.

71. Nigel Cory, Daniel Castro, and Ellysse Dick, "'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation" (ITIF, December 2020), https://itif.org/publications/2020/12/03/schrems-ii-what-invalidating-eu-us-privacy-shield-means-transatlantic/.
72. Regulation (EU) 2022/2065; Regulation (EU) 2022/1925.
73. Directive 2000/31/EC.
74. Regulation (EU) 2022/2065.
75. Aurelien Porteuse, "The Digital Markets Act: A Triumph of Regulation Over Innovation" (ITIF, August 2022), https://itif.org/events/2022/09/22/digital-markets-act-a-triumph-of-regulation-over-innovation/.
76. Natasha Lomas, "Europe names 19 platforms that must report algorithmic risks under DSA," *TechCrunch*, April 25, 2023, https://techcrunch.com/2023/04/25/europe-names-19-platforms-that-must-report-algorithmic-risks-under-dsa/.
77. Regulation (EU) 2022/1925.
78. Nigel Cory and Robert D. Atkinson, "Fair's Fair: Biden Should Use the IRA's Tax Credits to End Europe's Targeting of U.S. Tech" (ITIF, March 3, 2023), https://itif.org/publications/2023/03/03/fairs-fair-biden-should-use-the-iras-tax-credits-to-end-europes-targeting-of-us-tech/.
79. Regulation COM/2021/206 final.
80. Patrick Grady, "The AI Act Should Be Technology-Neutral" (Center for Data Innovation, February 2023), https://www2.datainnovation.org/2023-ai-act-technology-neutral.pdf.
81. Marietje Schaake, "How democracies can claim back power in the digital world," *MIT Technology Review*, September 29, 2020, https://www.technologyreview.com/2020/09/29/1009088/democracies-power-digital-social-media-governance-tech-companies-opinion/.
82. Alicia Garcia-Herrero and David Martinez Turegano, "Europe is losing competitiveness in global value chains while China surges," *Bruegel,* November 27, 2020, https://www.bruegel.org/2020/11/europe-is-losing-competitiveness-in-global-value-chains-while-china-surges/.
83. Anu Bradford, "The Brussels Effect," *Northwestern University Law Review* 107, no. 1 (2012), https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1081&context=nulr&httpsredir=1&referer=.
84. Nigel Cory and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them" (ITIF, July 2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/.
85. Ibid.
86. Ibid.
87. Nigel Cory and Robert D. Atkinson, "Hope for the Best, But Prepare for the Worst at the US-EU Trade and Technology Council" (ITIF, December 2, 2022), https://itif.org/publications/2022/12/02/hope-for-the-best-but-prepare-for-the-worst-at-the-us-eu-trade-and-technology-council/.
88. Jacqueline Hicks, "'Digital colonialism': Why countries like India want to take control of data from Big Tech," *The Print*, September 29, 2019, https://theprint.in/tech/digital-colonialism-why-countries-like-india-want-to-take-control-of-data-from-big-tech/298217/.

89. Michelle Wein, "The Worst Innovation Mercantilist Policies of 2014" (ITIF, December 2014), https://itif.org/publications/2014/12/08/worst-innovation-mercantilist-policies-2014/; Nigel Cory, "The Worst Innovation Mercantilist Policies of 2015" (ITIF, January 2016), https://itif.org/publications/2016/01/11/worst-innovation-mercantilist-policies-2015/; Nigel Cory, "The Worst Innovation Mercantilist Policies of 2016" (ITIF, January 2017), https://itif.org/publications/2017/01/09/worst-innovation-mercantilist-policies-2016/; Nigel Cory, "The Ten Worst Digital Protectionism and Innovation Mercantilist Policies of 2018" (ITIF, January 2019), https://itif.org/publications/2019/01/28/ten-worst-digital-protectionism-and-innovation-mercantilist-policies-2018/.
90. Michelle Wein and Stephen Ezell, "The 10 Worst Innovation Mercantilist Policies of 2013" (ITIF, January 2014), https://itif.org/publications/2014/01/06/10-worst-innovation-mercantilist-policies-2013/; Cory, "The Worst Innovation Mercantilist Policies of 2016"; Cory, "The Ten Worst."
91. Wein and Ezell, "The 10 Worst"; Cory, "The Worst Innovation Mercantilist Policies of 2015."
92. Susan Stone, James Messent, and Dorothee Flaig, "Emerging Policy Issues: Localisation Barriers to Trade," *OECD Trade Policy Papers*, No. 180 (2015), https://www.oecd-ilibrary.org/docserver/5js1m6v5qd5j-en.pdf?expires=1686254658&id=id&accname=guest&checksum=0DA21A5D319CB7A4F4E191F2214999F2.
93. Robert D. Atkinson, "How Applying 'Buy America' Provisions to IT Undermines Infrastructure Goals" (ITIF, May 2022), https://itif.org/publications/2022/05/09/how-applying-buy-america-provisions-it-undermines-infrastructure-goals/.
94. Ashley Johnson, "Nasty Side Effects if Australia Forces News Aggregators to Pay for Content" (ITIF, August 10, 2020), https://itif.org/publications/2020/08/10/nasty-side-effects-if-australia-forces-news-aggregators-pay-content/; Ashley Johnson, "Canada's Attempt to Make News Aggregators Pay for Content Could Lead to Lower-Quality News" (ITIF, October 19, 2022), https://itif.org/publications/2022/10/19/canadas-attempt-to-make-news-aggregators-pay-for-content-could-lead-to-lower-quality-news/; Daniel Castro, "Congress Should Not Break Big Tech to Fix Local News" (ITIF, February 11, 2022), https://itif.org/publications/2022/02/11/congress-should-not-break-big-tech-fix-local-news/.
95. Jesse Whittock, "Streaming Bill Regulating Netflix, Amazon And Co In Canada Becomes Law," *Deadline*, April 28, 2023, https://deadline.com/2023/04/netflix-amazon-canada-c-11-streaming-bill-now-law-regulation-1235340580/.
96. Jesse Whittock, "Australia To Set Local Content Quotas On International Streamers," *Deadline*, January 30, 2023, https://deadline.com/2023/01/australia-streamning-content-quotas-netflix-disney-plus-prime-video-1235244019/.
97. Ryan Browne and Arjun Kharpal, "Without us 'there is no Google': EU telcos ramp up pressure on Big Tech to pay for the internet," *CNBC*, March 10, 2023, https://www.cnbc.com/2023/03/10/no-networks-no-google-telcos-urge-eu-to-charge-big-tech-for-internet.html.
98. "A Global View of Barriers to Cross-Border Data Flows" (ITIF, published July 19, 2021), https://itif.org/publications/2021/07/19/global-view-barriers-cross-border-data-flows/.
99. "Why China's public procurement is an EU issue" (European Parliament, December 2016), https://www.europarl.europa.eu/RegData/etudes/ATAG/2016/593571/EPRS_ATA(2016)593571_EN.pdf; "Agreement on Government Procurement: Parties and observers," World Trade Organization, accessed June 9, 2023, https://www.wto.org/english/tratop_e/gproc_e/memobs_e.htm.
100. Robert D. Atkinson, "China's 'Innovation Mercantilism' Reduces the Rate of Global Innovation," in *Chinese State Capitalism: Diagnosis and Prognosis*, edited by Scott Kennedy and Jude Blanchette (Washington, D.C.: Center for Strategic and International Studies, 2021), 43–48, https://www2.itif.org/2021-chinese-state-capitalism.pdf.

101. Vincent Brussee, "China's social credit score – untangling myth from reality," Mercator Institute for China Studies, February 11, 2022, https://merics.org/en/comment/chinas-social-credit-score-untangling-myth-reality.

102. Human Rights Watch, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App* (Human Rights Watch, May 2019), https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass.

103. Beina Xu and Eleanor Albert, "Media Censorship in China" (Council on Foreign Relations, February 2017), https://www.cfr.org/backgrounder/media-censorship-china.

104. William Zheng, "In just 3 months, China's internet censor has closed over 4,000 websites and removed 55 apps," *South China Morning Post*, May 2, 2023, https://www.scmp.com/news/china/politics/article/3219119/just-3-months-chinas-internet-censor-has-closed-over-4000-websites-and-removed-55-apps; Elizabeth C. Economy, "The great firewall of China: Xi Jinping's internet shutdown," *The Guardian*, June 29, 2018, https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown.

105. Emily Tavenner, "Russian Cyber Sovereignty: Global Implications of an Authoritarian RuNet," American University, February 1, 2022, https://www.american.edu/sis/centers/security-technology/russian-cyber-sovereignty.cfm.

106. Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models" (Brookings, August 2019), https://www.brookings.edu/research/exporting-digital-authoritarianism/.

107. Billy Steele, "FCC adopts new rules for the foundation of 5G networks," *Engadget*, July 14, 2016, https://www.engadget.com/2016-07-14-fcc-adopts-5g-rules.html.

108. "The FCC's 5G FAST Plan," FCC, published September 28, 2018, https://docs.fcc.gov/public/attachments/DOC-354326A1.pdf.

109. "5G Fund," FCC, updated November 24, 2020, https://www.fcc.gov/5g-fund.

110. "Secure and Trusted Communications Networks Reimbursement Program," FCC, accessed June 14, 2023, https://www.fcc.gov/supplychain/reimbursement; "H.R.4998 - Secure and Trusted Communications Networks Act of 2019," Congress.gov, accessed June 14, 2023, https://www.congress.gov/bill/116th-congress/house-bill/4998.

111. "H.R.4346 - Chips and Science Act," Congress.gov, accessed June 14, 2023, https://www.congress.gov/bill/117th-congress/house-bill/4346/text.

112. Robert Casanova, "The CHIPS Act Has Already Sparked $200 Billion in Private Investments for U.S. Semiconductor Production," Semiconductor Industry Association, December 14, 2022, https://www.semiconductors.org/the-chips-act-has-already-sparked-200-billion-in-private-investments-for-u-s-semiconductor-production/.

113. "What is the Cross-Border Privacy Rules System," APEC, updated June 2023, https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system.

114. Andrei Gribakov, "Cross-Border Privacy Rules in Asia: An Overview," *Lawfare*, January 3, 2019, https://www.lawfareblog.com/cross-border-privacy-rules-asia-overview.

115. "Global Cross-Broder Privacy Rules Declaration," U.S. Department of Commerce, published April 21, 2022, https://www.commerce.gov/global-cross-border-privacy-rules-declaration.

116. "The Biden-Harris Administration Immediate Priorities," White House, accessed June 6, 2023, https://www.whitehouse.gov/priorities/.

117. Ashley Johnson and Daniel Castro, "How to Address Political Speech on Social Media in the United States" (ITIF, October 2022), https://itif.org/publications/2022/10/11/how-to-address-political-speech-on-social-media-in-the-united-states/.
118. Robert D. Atkinson, "A U.S. Grand Strategy for the Global Digital Economy" (ITIF, January 2021), https://itif.org/publications/2021/01/19/us-grand-strategy-global-digital-economy/.
119. Robert D. Atkinson and Michael McLaughlin, "Freedom Is Not Free License: Freedom House's Flawed Measurement of 'Internet Freedom'" (ITIF, June 2020), https://itif.org/publications/2020/06/08/freedom-not-free-license-freedom-houses-flawed-measurement-internet/.
120. "Digital Attaché Program," International Trade Administration, accessed June 6, 2023, https://www.trade.gov/digital-attache-program-0.
121. Stephen Ezell and John Wu, "How Joining the Information Technology Agreement Spurs Growth in Developing Nations" (ITIF, May 2017), https://itif.org/publications/2017/05/22/how-joining-information-technology-agreement-spurs-growth-developing-nations/.
122. "Questions & Answers: EU-US Data Privacy Framework," European Commission, published July 10, 2023, https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752.
123. NIST, "Framework for Improving Critical Infrastructure Cybersecurity" (Washington, D.C.: U.S. Department of Commerce, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf; NIST, "Artificial Intelligence Risk Management Framework" (Washington, D.C.: U.S. Department of Commerce, 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.
124. Daniel Castro, "NFTs: US Policies and Priorities in 2023" (ITIF, April 2023), https://itif.org/publications/2023/04/24/nfts-us-policies-and-priorities-in-2023/.