ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

July 17, 2018

Fiona Alexander
Associate Administrator
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230

RE: International Internet Policy Priorities for 2018 and Beyond

Dear Ms. Alexander,

The Information Technology & Innovation Foundation (ITIF) is pleased to submit these comments in response to the National Telecommunications and Information Administration's (NTIA) request for comment (RFC) on the administration's international Internet policy priorities for 2018 and beyond.[1] ITIF is a nonprofit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation and pro-technology public policy agenda internationally, in Washington, and in the states. Through its research, policy proposals, and commentary, ITIF is working to advance and support public policies that boost innovation, e-transformation, and productivity.

The NTIA has been central to the U.S. government's efforts for advocating on behalf of rapid technological advances and innovation since its inception in 1978. In the Internet era, the NTIA has played a pivotal role in advocating for a single, interoperable, open, and global Internet. The NTIA should continue this important mission to uphold these values, but with an overriding focus on ensuring a strong global marketplace for American digital products and services. ITIF welcomes the opportunity to provide input on the most important Internet policy issues, as well as what priorities should be the NTIA's focus.

[1] "NTIA Seeks Comment on International Internet Policy Priorities for 2018 and Beyond," National Telecommunications and Information Administrations, June 4, 2018, accessed July 11, 2018 https://s3.amazonaws.com/public-inspection.federalregister.gov/2018-12075.pdf.

THE FREE FLOW OF INFORMATION AND JURISDICTION

The RFC seeks information on several questions related to global developments that affect the free flow of information and Internet-related jurisdictional issues.

Which foreign laws and policies restrict the free flow of information online?

Data is the lifeblood of the modern global economy. The increased digitalization of organizations, driven by the rapid adoption of technologies such as cloud computing and data analytics, has increased the importance of data as an input to commerce, impacting not just information industries, but traditional industries as well.[2] The use of data analytics in virtually all industries has streamlined business practices and increased efficiency, but also made the movement of data more important. Businesses use data to create value, and many can only maximize that value when data can flow freely across borders.

Despite the significant benefits to companies, consumers, and national economies that arise from the ability of organizations to easily share data across borders, dozens of countries—across every stage of development—have erected barriers to cross-border data flows, such as data-residency requirements that confine data within a country's borders, a concept known as "data localization."[3] Data localization can be explicitly required by law or is the de facto result of a culmination of other restrictive policies that make it unfeasible to transfer data, such as requiring companies to store a copy of the data locally, requiring companies to process data locally, and mandating individual or government consent for data transfers. Countries justify these policies primarily based on three rationales: privacy, security, and enabling government access to data (this submission analyzes the privacy/cybersecurity motivations in a separate section below).[4] These barriers to data flows are a new, but rapidly growing trend. An ITIF report from May 2017 identified 34 countries that have proposed or enacted barriers to a few major categories of data: accounting, tax, and financial data (18); personal data (13); government and public data (10); data related to emerging digital services (9); telecommunications data (4); and other types (5).[5] These policies represent a new barrier to global digital trade: cutting off data flows or

---

[2] Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries," (Information Technology and Innovation Foundation, February 2015), http://www2.itif.org/2015-crossborder-data-flows.pdf.
[3] Stephen J. Ezell, Robert D. Atkinson, and Michelle A. Wein, "Localization Barriers to Trade: Threat to the Global Innovation Economy," (Information Technology and Innovation Foundation, September 2013), http://www2.itif.org/2013-localization-barriers-to-trade.pdf.
[4] Nigel Cory, "Cross-Border Data Flows: Where are the Barriers, and What Do They Cost?" (Information Technology and Innovation Foundation, May 2017), http://www2.itif.org/2017-cross-border-data-flows.pdf.
[5] Ibid.

making such flows harder or more expensive puts foreign firms at a disadvantage.[6] In essence, these tactics constitute "data protectionism" because they keep foreign competitors out of domestic markets.

NTIA should consider expanding U.S. government agency efforts to identify, track, and push back on barriers to data flows. NTIA should coordinate with U.S. Trade Representatives (USTR) and other agencies in efforts to engage international organizations to identify and publish barriers to data flows and digital trade. For example, USTR already collects and publishes an extensive list of barriers to data flows and digital trade that U.S. firms have encountered overseas. As part of its annual effort to track trade barriers around the world in the National Trade Estimate, USTR has spun-off a separate report on barriers to digital trade in 2017 and 2018.[7] In it, USTR categorizes and summarizes the various digital trade barriers U.S. firms face. NTIA should work with USTR to push international organizations to also identify and track these barriers. In addition, NTIA should step up its tracking and advocacy on the rules that affect over-the-top (OTT) services, including at the International Telecommunication Union (ITU), to push back against the rising tide of countries' protectionist policies.

As an extension of this, the United States should make it a goal to push international organizations, such as the World Trade Organization and the Organization of Economic Cooperation and Development (OECD), to set up a process to monitor, catalogue, and report on policies that negatively affect digital trade and data flows and are related to localization barriers. The ideal outcome would be for barriers to data flows to become part of the WTO's Integrated Trade Intelligence Portal. The United States and others should also push international institutions, such as the United Nations Conference on Trade and Development (UNCTAD), the International Monetary Fund, and multilateral development banks (e.g., the World Bank and the InterAmerican Development Bank), to advocate for the free flow of data across borders and push back against countries that force data localization within their borders. NTIA should specifically push these international organizations to recognize that forced data localization not only hurts companies in nations that process large amounts of data, but can also be extremely detrimental to budding data-processing markets.

---

[6] There is no one definition of digital trade. The definition used is from the USITC's Digital Trade in the U.S. and Global Economies, Part 2. United States International Trade Commission (USITC), Digital Trade in the U.S. and Global Economies, Part 2 (Washington, DC: USITC, August 2014), https://www.usitc.gov/publications/332/pub4485.pdf.

[7] "Key Barriers to Digital Trade," *Office of the United States Trade Representative*, accessed July 17. 2018, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2017/march/key-barriers-digital-trade.

Policymakers should not attempt to use data localization requirements to solve cybersecurity concerns. Security breaches can happen no matter where data are stored—data centers everywhere are exposed to similar risks. Data breaches are the result of security failures, such as poor network design, weak encryption, or improper access controls.[8] The only way to prevent these types of attacks is to implement better security controls—but whether data is stored domestically has no bearing on security. A secure server in Colombia is no different from a secure server in Brazil. Data security depends on the technical, physical, and administrative controls implemented by the service provider, which can be strong or weak, regardless of where the data is stored. Moreover, policymakers can pass laws that hold companies responsible for data breaches, even if they occur abroad. Likewise, consumers and businesses can use contracts to ensure that they can hold companies accountable for data breaches that occur abroad.

Regardless, many countries have enacted rules to limit the movement of data outside their borders. While countries with explicit local data-storage requirements get the most attention, some nations have made their data protection rules so onerous—such as by requiring consent for any data transfers abroad—that companies have no choice but to store data locally. For example, South Korea's Personal Information Protection Act requires companies to obtain consent from "data subjects" (i.e., the individuals associated with particular datasets) prior to exporting that data, as well as details about who receives the data, the purpose, the period the data will be retained, and the specific personal information provided.[9] However, this main effect is a mercantilist one, requiring companies to use domestic providers for data storage and processing.

What is the impact on U.S. companies and users in general?

Barriers to data flows undermine firm competitiveness and economic productivity. Maximizing the value of data requires it to move. Innovation and economic growth are increasingly driven by how firms collect, transfer, analyze, and act on data. Absent "data protectionism," digital trade and cross-border data flows are expected to continue to grow much faster than the overall rate of global trade.

At the firm level, barriers to data flows make firms less competitive, as a company will by definition be forced to spend more than necessary on IT services. Companies will likely have to pay more for data-storage services, especially those in smaller countries (which will not naturally be home to a data center). Such barriers also

[8] Daniel Castro and Alan McQuinn, "Unlocking Encryption: Information Security and the Rule of Law," (Information Technology and Innovation Foundation, March 2016), http://www2.itif.org/2016-unlocking-encryption.pdf.
[9] Anupam Chandler and Uyen P. Le, "Data Nationalism," *Emory Law Journal 64*, No.3, March 2015, accessed July 17, 2018, http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf.

prevent companies from transferring data that is needed for day-to-day activities, such as for human resources, which means companies may have to pay for duplicative services. Likewise, companies may be compelled to spend more on compliance activities, such as hiring a data-protection officer, or putting in place software and systems to get individuals' or the government's approval to transfer data. These additional costs are either borne by the customer or the firm, which undermines the firm's competitiveness (especially for foreign firms who are at some disadvantage vis-a-vis domestic firms) by cutting into profit margins. This economic impact ripples throughout an economy as barriers to data flows affect data processing and Internet services—or any service that depends on the use of data for delivery, which in today's economy is most businesses.

In terms of sector-level impacts, ITIF submissions to the U.S. International Trade Commission have analyzed the impact on U.S. cloud service firms and Internet-based services.[10] For example, for cloud services, while quantifying the specific cost of restrictions on U.S. cloud computing providers in foreign markets is complex, at a conceptual level, there are some clearly identifiable impacts:

- There is direct impact from excluding U.S. cloud computing providers from accessing and servicing a market due to data localization. This also applies to countries which have highly restrictive market-access conditions for cloud services or use security reviews and other registration and licensing requirements for ICT infrastructure and services as tools to discriminate against foreign cloud computing providers and essentially exclude them from their markets. This practice inevitably affects U.S. firms' competitiveness due to the loss of benefits that would otherwise come from economies of scale.
- Some restrictions make cross-border data flows prohibitively difficult and costly or outright illegal, thus forcing firms to setup their own ICT infrastructure or use contracted providers. This type of localization barrier discriminates against foreign firms as it forces foreign enterprises to produce/provide locally what the enterprise would otherwise produce outside the nation's borders and export to another economy. This practice makes U.S. cloud computing providers less competitive due to forgone benefits in economies of scale and the increased costs that come from the duplication of facilities and the additional costs involved in regulatory compliance activities.
- Data centers are a service, but just as important, act as a critical digital platform for other services. A U.S. firm, using a U.S. cloud service, would find it easier to extend its use of these services to a new

[10] Nigel Cory, "Testimony Before the United States International Trade Commission on Global Digital Trade," (The Information Technology and Innovation Foundation, 2018), https://itif.org/publications/2018/03/29/testimony-united-states-international-trade-commission-global-digital-trade.

foreign market if a related cloud-based provider was already operating in that market. However, where restrictions preclude this, it reduces U.S. cloud service revenues.

- Countries can make market or contract access (especially for public procurement) contingent on the use of local technology infrastructure, which again, discriminates against U.S. cloud computing providers which may otherwise be able to provide the service remotely.

Several studies have documented the broad negative impact of data localization laws.

- A 2014 ECIPE study estimated the economic costs related to proposed or enacted data localization requirements and related data-privacy and security laws in Brazil, China, the European Union, India, Indonesia, South Korea, and Vietnam.[11] It found that policies that increase data-processing costs negatively impact economic growth through higher prices on data services.
- A 2014 International Trade Commission (ITC) study showed that barriers to digital trade and data flows impose costs on U.S. firms and the U.S. economy. The ITC study analyzed the impact of barriers to digital trade and data flows on three levels of the U.S. economy: the firm level, through 10 case studies of U.S. companies involved in digital trade; the industry level, through a survey of U.S. businesses in seven digitally intensive industries; and at the economy level, through a computable general equilibrium and econometric model.[12] The study estimated that removing foreign digital trade barriers would increase U.S. GDP by $16.7 to $41.4 billion (0.1 to 0.3 percent) and wages by 0.7 to 1.4 percent in the seven sectors.[13] Moreover, the study included a survey that asked whether

[11] The study uses a computable general equilibrium model (CGE) called GTAP8. The effect on productivity is created using a so-called augmented product market-regulatory index for all regulatory barriers on data, including data localization, to calculate domestic price increases or total factor productivity losses. Matthias Bauer, Hosuk Lee-Makiyama, Erik can der Marel, Bert Verschelde, "The Costs of Data Localisation: Friendly Fire on Economic Recovery," (European Centre for International Political Economy, March 2014), http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.

[12] The seven sectors are content, digital communications, finance and insurance, manufacturing, retail trade, selected other services, and wholesale trade. USITC, Digital Trade in the U.S. and Global Economies, Part 2.

[13] The GTAP model translates the sector-specific employment effects from the survey into changes in real GDP, real wages, aggregate employment, and sector-level production in the United States. The simulations take the sector-specific effects on U.S. employment as given and estimate the magnitude of foreign barriers that they imply. The simulations also estimate how workers move from other sectors in the economy. The CGE model analysis is based on the standard GTAP model, with one extension. The size of the labor force (and therefore the quantity of labor supplied) in each region is treated as an endogenous variable, and there is a constant elasticity labor supply curve for each region. The 57 sectors in

companies in these sectors faced localization and data-privacy and protection requirements, also asking them to rank these along a scale of one (not an obstacle) to five (a very substantial obstacle). Eighty-two percent of large firms and 52 percent of small- and medium-sized enterprises (SMEs) in the digital-communications sector reported facing localization barriers to digital trade.[14] The severity of these barriers varied: 34 percent of large firms in digital communications faced localization requirements; 27 percent of content firms considered localization barriers as "substantial or very substantial"; and 20 percent of large retail firms and 19 percent of large financial firms considered them "substantial or very substantial."[15]

- A 2015 Leviathan (an information security company) study shows that local companies could have to pay significantly more for cloud services in Brazil and Europe if data localization policies had cut them off from the most cost-competitive global cloud computing providers.[16] The report estimates that such restrictions would force local companies to pay 30 to 60 percent more for their computing needs than if they could go outside the country's borders.[17] For example, the study estimates that if Brazil were to enact data localization as part of its "Internet Bill of Rights," local companies would have to pay an average of 54 percent more than the lowest worldwide price to use cloud services.[18]
- A 2016 ECIPE study shows that data localization diminishes productivity and that this impact far outweighs whatever marginal gains the domestic ICT sector might gain from such digital protectionism.[19]

---

the GTAP database are aggregated into 14 sectors, 5 of which correspond to the digitally intensive sectors described in chapters 3 and 4 of this report—communications (content and digital communications); finance (finance and insurance); trade (retail and wholesale trade, manufacturing); and services (other services). The study uses GTAP simulations to estimate this impact. U.S. employment in the digitally intensive sectors is an exogenous variable of the model, while the trade costs on these sectors' imports into certain countries are endogenous variables in the model. With this closure, the model calibrates tariff-equivalent magnitudes of the import barriers in the digitally intensive sectors. This closure ensures that the CGE model matches the survey estimated sector-level employment effects through a reduction in the barriers to imports in the relevant sectors and countries.

[14] Ibid.

[15] Ibid.

[16] "Qualifying the Cost of Forced Localization," (Leviathan Security Group, June 2015), accessed July 11, 2018, https://www.leviathansecurity.com/blog/quantifying-the-cost-of-forced-localization

[17] Ibid.

[18] Ibid.

[19] Matthias Bauer, Martina Ferracane, Hosuk Lee-Makiyama, Erik van der Marel, "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States," (European Centre for

- A 2016 Center for International Governance Innovation (CIGI) and Chatham House study shows that restrictive data regulations, including forced data localization, increase prices and decrease productivity across 10 downstream sectors (i.e., the users of data or data-related services).[20] The study also analyzes the impact of these measures on the broader economy in Brazil, China, the European Union, India, Indonesia, Russia, South Korea, and Vietnam.

Furthermore, barriers to cross-border data flows undermine innovation and access to innovative services. Countries that enact barriers to data flows make it harder and more expensive for their companies to gain exposure and to benefit from the ideas, research, technologies, and best practices that accompany data flows and the innovative new goods and services that rely on data. Countries that artificially prop up domestic businesses with such digital-protectionist policies—which disadvantage foreign firms—set them up to fail because they will always be less competitive and innovative than those companies in global markets that operate without similar protection. Barriers to data flows also mean delays and higher costs in the development of new and innovative goods, as companies may be unable to use their preferred research partners and are forced to use second choice partners (if they do so at all). Data-localization policies undermine the ability of companies, such as Procter & Gamble (P&G), that use new and innovative global "open-innovation" platforms to facilitate collaboration among firms, universities, and other research organizations to drive their own innovation.[21]

Have courts in other countries issued Internet-related judgments that apply national laws to the global Internet? What have been the practical effects on U.S. companies of such judgements?

In recent years, foreign courts have passed Internet-related judgements that apply national laws to the global Internet, impeding on the sovereignty of other nations and individuals around the world. A prime example of this is the EU's right to be forgotten, which has become enshrined in the recently-enacted General Data

International Political Economy, March 2016), http://ecipe.org//app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf.

[20] As part of the proxy variable for data regulations, the study uses part of the OECD's Product Market Regulation in services to create a proxy that comes close to matching the types of regulations that are used regarding data. The real policy regulations for the select countries are then added to this index to estimate the real costs. Matthias Bauer, Martina F. Ferracane, and Erik van der Marel, "Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization," (Centre for International Governance Innovation and Chatham House, May 2016), https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf.

[21] USITC, *Digital Trade in the U.S. and Global Economies, Part 2*.

Protection Regulation (GDPR).[22] In 2014, the EU's highest court ruled that Europeans have "the right to be forgotten,"—the ability to request that search engines remove links from queries associated with their names if those results are irrelevant, incorrect, or outdated.[23] As a result of this ruling, Google agreed to delist search results from all Google domains based on geo-location signals, keeping the ruling targeted to the area it was created in: Europe.[24] However, the French data protection authority, the Commission Nationale de l'informatique et des Libertés (CNIL), wanted to expand the reach of this law to the global Internet, fining Google €100,000 ($112,000) for failing to remove links associated with French right to be forgotten requests from its global search index.[25]

The problem with making domestic laws the de facto laws for the global Internet is that all countries do not share the same values and laws. For example, there is no global consensus on the right to be forgotten. In fact, critics around the world have derided this policy because of its negative impact on free speech and how the people who most stand to benefit from this type of policy are convicted sex offenders, board-sanctioned doctors, and disgraced politicians who want their past indiscretions removed from the public record.[26]

These actions stand in contrast to U.S. rights on freedom of expression. In such cases, the U.S. government—through agencies such as the NTIA—should push back on foreign government's infringements on its jurisdiction. To accomplish this, NTIA should argue that countries should balance their own national sovereignty with respect for the global nature of the Internet. ITIF developed a framework for Internet

[22] "Commission Publishes Guidance on Upcoming New Data Protection Rules," European Commission, January 24, 2018, accessed July 12, 2018, http://europa.eu/rapid/press-release_IP-18-386_en.htm.
[23] Alan Travis and Charles Arthur, "EU Court Backs 'Right to be Forgotten': Google Must Amend Results on Request," *the Guardian*, May 13, 2014, accessed July 11, 2018, https://www.theguardian.com/technology/2014/may/13/right-to-be-forgotten-eu-court-google-search-results.
[24] Peter Fleischer, "Adapting Our Approach to the European Right to be Forgotten," *Google*, March 4, 2016, accessed July 11, 2018, https://blog.google/around-the-globe/google-europe/adapting-our-approach-to-european-rig/.
[25] Mark Scott, "Google Fined by French Privacy Regulator," *New York Times*, March 24, 2016, accessed July 11, 2018, https://www.nytimes.com/2016/03/25/technology/google-fined-by-french-privacy-regulator.html.
[26] Daniel Castro, "Time to Forget the 'Right to be Forgotten'," *the Hill*, May 30, 2014, accessed July 11, 2018, http://thehill.com/blogs/pundits-blog/technology/207762-time-to-forget-the-right-to-be-forgotten. Charles Arthur, "Google Faces Deluge of Requests to Wipe Details From Search Index," *The Guardian*, May 15, 2014, accessed July 11, 2018, https://www.theguardian.com/technology/2014/may/15/hundreds-google-wipe-details-search-index-right-forgotten.

policymaking that can guide this effort.[27] First, if the issue involved the Internet's technical architecture, then a country should rely on and work within a global, multi-stakeholder entity, such as the Internet Corporation for Assigned Names and Numbers (ICANN), to decide core Internet functions. Second, if an issue directly affects individuals or companies outside its borders, then countries should look to formal international agreements on the subject. If there is a conflict, then the policy should not be pursued. In many cases there will be conflicts. For example, many nations do not agree on fundamental principles related to free speech. While nations with stricter norms regarding free speech (e.g., banning pornography) should not attempt to impose their values on other nations through rules that affect the Internet, likewise the United States should not attempt to impose its values on other nations.

If the policy does not conflict with international agreements, then the final question is whether an informal consensus exists among countries that a certain policy goal is desirable. If this consensus exists, countries can pursue that policy, cautiously ensuring that they minimize its impact on individuals outside their borders. These countries can then work to build a formal international consensus on the policy. If there is no consensus, countries should work to build that consensus or find a policy alternative that does not affect people outside their jurisdiction.

The framework proposed here is conceptually simple. Many of the conflicts between nations in Internet policy come about because of different goals or values. For example, some countries may come to the conclusion that access to information trumps privacy, while others prefer the reverse. Attempting to impose domestic values on the world, as arguably the European Union is doing with the GDPR by forcing other nations to adhere to its data protection standards, is not appropriate. Yet even though all nations may not agree on the same goals or values, that does not mean they cannot work together to build a global Internet system that works well. Collaboration is necessary to address many challenges on the Internet, from setting technical standards to preventing digital crime, and cooperation and coordination is required for countries to share in the benefits of the global network economy. By evangelizing a common framework for analyzing cross-border Internet policy issues and understanding which issues should be contested and which should not, NTIA can help foreign policymakers avoid unnecessary conflicts and better identify the validity of criticism of different Internet policy proposals. In fact, of all the steps NTIA can take to ensure a stronger global Internet, perhaps the most important is to work to establish such a nuanced and balanced framework as the global norm.

---

[27] Daniel Castro and Robert Atkinson, "Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy," (the Information Technology and Innovation Foundation, September 2014, accessed July 11, 2018, http://www2.itif.org/2014-crossborder-internet-policy.pdf.

PRIVACY AND SECURITY

Many countries have created strict data privacy regulations that impose significant compliance costs on businesses and reduce their revenues by limiting targeted advertising.[28] Higher costs and lower revenues reduces the investments companies can make to maintain and improve their online services. As a result, companies can raise costs for consumers, such as by switching from providing free services to charging for them. With this in mind, ITIF submits the following responses to NTIA's question about how to promote smart and non-discriminatory privacy rules in the United States and abroad.

Which international venues are the most appropriate to address questions of digital privacy? What privacy issues should NTIA prioritize in those international venues?

The U.S. model of regulating consumer privacy—using a combination of light-touch regulation for most industries and additional sector-specific regulation for particularly sensitive information, such as health, financial, and education data—has contributed to the flourishing digital economy. Yet this model of balanced and mostly innovation-friendly regulation is under attack. On the international front, the European Union is pressuring the United States (and other countries) to adopt similar rules or risk its businesses losing access to the EU market. And domestically, California has passed a new data privacy law that could subvert the typical exchange of access to free online services in exchange for targeted online advertising. The federal government, and the NTIA in particular, should resist these efforts on both fronts.

First, the European Union's GDPR went into effect on May 25, 2018. This law adversely impacts U.S. businesses trying to offer online services to European customers by raising compliance costs, threatening companies with substantial penalties for mistakes, reducing the viability of free business models, and reducing access to data. One of the biggest problems with the GDPR is that it requires companies to obtain affirmative consent from users before using their data, thereby adversely affecting business, especially those with advertising-based business models. Perhaps the definitive study on the effects of these types of rules is from academics Ari Goldfarb and Catherine Tucker, who in 2010 found that the European Union's ePrivacy Directive limited how advertisers could collect and use information about consumers for targeted advertising, which negatively impacted the efficacy of online advertising.[29] The authors found that after the affirmative

[28] Alan McQuinn and Daniel Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use," (the Information Technology and Innovation Foundation, July 2018), http://www2.itif.org/2018-trust-privacy.pdf.
[29] Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising." SSRN Scholarly Paper ID 1600259, 2010, Rochester, NY, Social Science Research Network, accessed June 12, 2018, https://papers.ssrn.com/abstract=1600259.

consent policy went into effect, the result was an average reduction in the effectiveness of the online ads by approximately 65 percent. This reduction occurred because websites had insufficient information about their users to make the ads relevant. Thus, click-through rates fell, reducing the amount advertisers would be willing to pay. The authors noted that if advertisers decreased their spending on online advertising based on this reduction in effectiveness, "revenue for online display advertising could fall by more than half from $8 billion to $2.8 billion."[30] Opt-in requirements raise the cost of getting permission to use data, ultimately hurting U.S. consumers by increasing costs and depriving them of innovative services. The NTIA should vocally oppose these types of unnecessarily strict data protection regulations in all relevant international forums it participates in, arguing that they are anti-innovation and do little to help consumer privacy compared to the more balanced U.S. approach.

Second, California lawmakers recently passed the California Privacy Act of 2018, which allows users to access how businesses collect data and opt-out of that information collection.[31] Unfortunately, the bill also limits companies from penalizing consumers who opt out of sharing their personal data. This undercuts access to free content and services—if there is no cost to consumers who choose not to share their data, then they will have little incentive to do so. As a result, California created a classic free-rider problem that undermines ad-supported business models. Other states may attempt to replicate this law, expanding this free-rider problem while also potentially creating a patchwork of conflicting state laws that make compliance more difficult and more expensive. Others might open the door toward many lawsuits against companies for minor transgressions. For example, the California ballot initiative on privacy (which was withdrawn after the passage of the California Privacy Act) would have created a private right of action for companies who mishandle data. And Illinois passed a biometrics law that has exposed many companies to expensive class-action lawsuits, even when there is no tangible consumer harm. The NTIA, along with others at the Department of Commerce, should work with Congress to craft federal legislation that preempts burdensome state data protection laws and regulations, guarantees consumers opt-out notice and choice, and allows Internet companies to structure their business models as they choose.

[30] Ibid.
[31] California Consumer Privacy Act of 2018, Cal. Civ. Code §1798.198(a), (2018).

EMERGING TECHNOLOGIES AND TRENDS

New technologies often generate concerns, especially if the public does not commonly use them or understand them.[32] These concerns can manifest in ill-considered policy solutions that harm innovation. NTIA should push back when foreign governments create rules that try to solve problems that have yet to be realized. ITIF submits the following responses to NTIA's questions for promoting innovation and investment for emerging technologies.

What are the current best practices for promoting innovation and investment for emerging technologies? Are these best practices universal, or are they dependent upon a country's level of economic development? How should NTIA promote these best practices?

While there are no hard and fast rules for promoting innovation and investment in emerging technologies, there are several policy principles that the NTIA can look to and advocate for in pursuit of this goal.

First, nations should embrace the innovation principle; engage in light-touch regulation for innovative technologies and business models until broader regulatory concerns appear. Unfortunately, many nations fall trap to precautionary rules for emerging technologies, which focus on pre-emptively guarding against hypothetical risks a technology might pose, long before these risks are known. Focusing solely on the potential threats of a technology, these nations pass preemptive regulations that they believe will increase consumer trust and therefore increase adoption of that technology. The reality is that overly strict regulations often impose costs, limit innovation, and do not increase trust beyond a baseline level of protections.[33] Policymakers should not succumb to these forces if they expect to enable society to take full advantage of the emerging technologies. In particular, policymakers should be extremely cautious about regulating on the basis of purely speculative fears or concerns that might not even come to pass, especially when doing so might curtail substantial economic and social benefits of the technology.[34] Instead, nations should consider the impact of policy decisions on innovation. One way to accomplish this is to address problems with new technologies as they arise with regulations that target specific, demonstrated harms. Similarly, nations should

---

[32] Adam Thierer, "Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle," *Mercatus Center*, January 25, 2013, http://mercatus.org/publication/technopanics-threat-inflation-and-danger-information-technology-precautionary-principle.

[33] Alan McQuinn and Daniel Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use."

[34] Daniel Castro and Alan McQuinn, "The Privacy Panic Cycle: A Guide to Public Fears About New Technologies," (the Information Technology and Innovation Foundation, September 2015), http://www2.itif.org/2015-privacy-panic.pdf.

create laws and regulations that allow businesses and governments to build products and services efficiently by minimizing the regulatory cost of data collection.[35]

Second, nations should use regulatory enforcement to incentivize companies to protect consumers. Regulatory oversight keeps companies in check, promotes fair competition, and upholds consumer protections. To maximize its effectiveness and minimize any negative effects, any enforcement action should create a system of incentives that promotes desirable behavior and discourages undesirable behavior in a marketplace, doing so in a way that limits compliance costs. However, regulators can also go too far and regulate against companies acting in good faith to bring an innovation to market. This approach would limit businesses using emerging technologies, because if innovators fear they will be punished for every mistake, they will be much less assertive in trying to develop the next application and will spend more time and effort on compliance, rather than innovation.

Instead, national regulators should evaluate enforcement actions based on two dimensions: whether the company acted intentionally or negligently and whether a company's action resulted in real consumer harm.[36] Regulators would then use a sliding scale to determine penalties, where unintentional, harmless actions receive no penalty and intentional, harmful actions receive large penalties. As they evaluate enforcement actions, regulators should treat negligence as intentional. This strategy will not punish companies for innovating and will send clear signals to companies about what behavior is off-limits to better protect consumers.

Third, nations should adopt technology-neutral rules that neither favor nor disadvantage any particular technology to create a level playing field for innovation. While regulators should take into account differing technologies, they should treat similar products and services with similar rules. Clearly, all businesses are not the same. Where there are differences in technologies, policymakers should establish rules that recognize the risks distinct to (or irrelevant to) particular applications.

Finally, nations should support standards development and data interoperability for emerging technologies. National governments should engage with the industry for private-sector led standards development and best practices around emerging technology issues, and seek opportunities to participate and promote international

[35] Daniel Castro and Josh New, "10 Policy Principles for Unlocking the Internet of Things," (Center for Data Innovation, December 2014), http://www2.datainnovation.org/2014-iot-policy-principles.pdf.
[36] Daniel Castro and Alan McQuinn, "How and When Regulators Should Intervene," (Information Technology and Innovation Foundation, February 2015), http://www2.itif.org/2015-how-whenregulators-intervene.pdf.

collaboration on consensus-based standards adoption. Moreover, nations should also promote data interoperability—the ability of different IT systems to communicate, exchange data, and cooperatively use that data—especially among new technologies. Though the private sector should lead efforts for standards development and data interoperability, national governments can bring together disparate market players across different industries, standards bodies, and encourage and promote interoperability across different types of data.

NTIA, and the federal government broadly, can play a much more proactive role in helping to articulate these principles, not only in various international forums, but in working closely with developing nations around the world to help them understand the merits of this innovation framework and implement it institutionally. Currently U.S. efforts in this space are woefully inadequate, allowing other nations and regions, especially Europe and China, win the battle for hearts and minds.

ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

CONCLUSIONS

The NTIA should ensure that U.S. international policy reflects the growing importance of emerging technology, data flows, and digital economic activity. The United States and other like-minded countries that value free trade and the free flow of data can only counter this digital protectionism by setting new, high-standard rules that protect data flows and other crucial facilitators of digital trade and data flows.

As part of this, the NTIA should drive a more-informed debate about data-related policies to dispel the misguided (but persistent) connection some policymakers have made in linking local data storage and privacy, cybersecurity, and economic development. Moreover, NTIA should adopt the innovation-friendly principles for digital privacy and emerging technologies proposed in these comments and advocate for their adoption by other nations through international forums.

Sincerely,

Daniel Castro
Vice President, Information Technology and Innovation Foundation

Nigel Cory
Associate Director, Trade Policy, Information Technology and Innovation Foundation

Alan McQuinn
Senior Policy Analyst, Information Technology and Innovation Foundation