ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

November 7, 2018
Mr. Travis Hall
Telecommunications Policy Analyst, Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

RE: Privacy Request for Comment, Docket No. 180821780-8780-01

Dear Mr. Hall,

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 approach to advancing consumer privacy while protecting prosperity and innovation.[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 U.S. Department of Commerce, through the leadership of the NTIA, is seeking to determine the best path forward for a U.S. privacy framework that both protects individual's privacy and fosters innovation.[2] Achieving this balanced level of privacy regulation is crucial because overly strict rules will not only do little to increase user trust, but will limit digital innovation, raise costs, and limit consumer choices, thereby actually reducing technology use relative to more balanced rules.[3] Given that U.S. consumers enjoy a wealth of free or low-cost Internet services because of an effective U.S. ad-market where businesses and consumers mutually

[1] "Request for Comments on Developing the Administration's Approach to Consumer Privacy," National Telecommunications and Information Administrations, September 25, 2018, accessed October 9, 2018, https://www.ntia.doc.gov/federal-register-notice/2018/request-comments-developing-administration-s-approach-consumer-privacy.
[2] Ibid.
[3] Alan McQuinn and Daniel Castro, "Why Stronger Privacy Regulations Do Not Spur Increased Internet Use" (Information Technology and Innovation Foundation, July 2018), accessed October 9, 2018, http://www2.itif.org/2018-trust-privacy.pdf.

benefit from the choice to share data, it is incumbent on the NTIA to gets its proposal right to ensure society can continue to use data for the benefit of all.[4] ITIF supports the NTIA's efforts to start a dialogue on a meaningful, innovation-friendly U.S. privacy framework and welcomes the opportunity to provide input on this important topic.

BACKGROUND

The United States does not have a single federal data privacy law for the private sector. Instead, it has multiple privacy laws and regulators. Some laws create privacy rules for a specific sector, like health care or financial services, whereas others focus on providing specific safeguards, such as protecting children's privacy.[5] Where there are no sector-specific rules, the U.S. government frequently allows industries to self-regulate privacy protections through voluntary agreements, peer pressure, and other methods to coordinate behavior without violating anti-trust rules.[6]

The Federal Trade Commission (FTC) has broad authority to take enforcement action against businesses that engage in unfair or deceptive behavior.[7] For example, when companies participate in industry codes of conduct or publish privacy policies, but do not keep their promises to protect consumer data, the FTC can pursue enforcement actions against them. In addition to having authority to investigate and combat unfair and deceptive practices, the FTC enforces multiple sector specific laws, such as the CAN-SPAM Act, the Children's Online Privacy Protection Act, the Truth in Lending Act, Gramm-Leach-Bliley Act (GLBA) of 1999, the Equal Credit Opportunity Act, and the Fair Credit Reporting Act.

With the European Union implementing the General Data Protection Regulation (GDPR)—a significant piece of data protection legislation with global implications—and California passing a new privacy law, coupled with several high-profile incidents involving companies exposing consumer data, the Trump

[4] Alan McQuinn, "No, Internet Users Are Not Paying With Their Data," *Inside Sources*, August 7, 2018, accessed October 9, 2018, https://www.insidesources.com/no-internet-users-not-paying-data/.
[5] Nick Wallace, Alan McQuinn, Stephen Ezell, and Daniel Castro, "How Canada, the EU, and the U.S. Can Work Together to Promote ICT Development and Use" (Information Technology and Innovation Foundation, June 2018), http://www2.itif.org/2018-canada-eu-us-ict-development.pdf.
[6] Daniel Castro, "Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising" (Information Technology and Innovation Foundation, December 2011), http://www.itif.org/files/2011-self-regulation-online-behavioral-advertising.pdf.
[7] Ibid.

administration is now seeking to develop an updated general framework for consumer data privacy.[8] The Department of Commerce has led these efforts through two of its agencies, the NTIA and the National Institute of Standards and Technology (NIST).[9]

NTIA's RFC is divided into two parts: "a set of user-centric privacy outcomes that underpin the protections that should be produced by any Federal actions on consumer-privacy policy" and "a set of high-level goals that describe the outlines of the ecosystem that should be created to provide those protections." The former section consists of seven user-centric outcomes that are intended to be flexible and clear, but not a legal standard. These outcomes are transparency, control, reasonable minimization, security, access and correction, risk management, and accountability.[10] Some of these outcomes are problematic, such as reasonable minimization, as they incorrectly take the position that collection of data is inherently problematic. The latter section consists of eight goals for federal action to achieve the above outcomes for users: (1) harmonize the regulatory landscape, (2) provide legal clarity while maintaining the flexibility to innovation, (3) comprehensive application to avoid a fragmented regulatory system, (4) employ a risk and outcome-based approach, (5) interoperability with other privacy frameworks, (6) provide incentives for privacy research, (7) Federal Trade Commission (FTC) enforcement, and (7) scalability.[11]

ITIF looks forward to participating in the process and submits the following responses to NTIA's questions.

A. The Core Privacy Outcomes for U.S. Consumers

The RFC seeks information on several questions related to the seven user-centric outcomes. In particular, the RFC asks: *(1) Are there other outcomes that should be included, or outcomes that should be expanded upon as separate items? (2) Are the descriptions clear? Beyond clarity, are there any issues raised by how any of the outcomes*

[8] David Shepardson, "Trump Administration Working on Consumer Data Privacy Policy," *Reuters*, July 27, 2018, accessed October 9, 2018, https://www.reuters.com/article/us-usa-internet-privacy/trump-administration-working-on-consumer-data-privacy-policy-idUSKBN1KH2MK.

[9] While the NTIA is engaged with the comments discussed herein, NIST is leading efforts for a privacy "framework" consisting of standardized policies that organizations can adopt to reduce the risk of data misuse—similar to when it developed a cybersecurity framework. "Department of Commerce Launches Collaborative Privacy Framework Effort," National Institute of Standards and Technology, September 4, 2018, accessed October 9 ,2018, https://www.nist.gov/news-events/news/2018/09/department-commerce-launches-collaborative-privacy-framework-effort.

[10] Request for Comments on Developing the Administration's Approach to Consumer Privacy," National Telecommunications and Information Administrations.

[11] Ibid.

are described? (3) Are there any risks that accompany the list of outcomes, or the general approach taken in the list of outcomes?

One of the defining features of the Internet is continuous innovation, so the NTIA should add "increase, and not undermine, innovation" to its list of outcomes for a federal privacy framework. It is important for NTIA to state at the outset that any privacy outcomes should not undermine innovation because many privacy laws, such as the GDPR, would do so. Indeed, creating more restrictive data privacy laws is rather straightforward, but creating such laws that have minimal disruptive effects on users or businesses is much more complex, which is why this should be an explicit outcome. Additionally, policymakers should consider ways in which a federal privacy framework could enhance innovation, such as by reducing regulatory costs or limitations associated with data-driven services, including the online advertising that funds much of the free or low-cost content and services available to Internet users.

NTIA should promote this outcome through two steps.

First, any federal privacy framework should consider the economic costs of any piece of privacy legislation or enforcement action. Overly strict data protection regulations can adversely impact innovation. There are many factors of potential privacy rules that can have these adverse effects. For one, strict data protection regulations can raise compliance costs, forcing companies to devote resources to compliance, which reduces the amount of money that can be invested in innovation. For example, a 2016 study found that GDPR requirements for public authorities and companies to process personal data could result companies needing to hire an additional 75,000 workers to comply with the law.[12] Similarly, privacy rules can increase legal risks and the threat of large fines that can leave consumers worse off. For example, a 2017 Center for Data Innovation report argues that by raising the legal risks of companies developing and using artificial intelligence (AI), the GDPR will have a negative impact on the development and use of AI in Europe.[13] Moreover, some rules can reduce the effectiveness of online adverting, thereby impacting the revenue digital companies can earn from online ads and reducing the overall growth of the digital ecosystem. For example, regulations that shift online services from an "opt-out" privacy system, in which consumers can choose to not

[12] Rita Heimes and Same Pfeifle, "Study: GDPR's Global Reach to Require at Least 75,000 DPOs Worldwide." November 9, 2016, accessed October 18, 2018. https://iapp.org/news/a/study-gdprs-globalreach-to-require-at-least-75000-dpos-worldwide/.
[13] Nick Wallace and Daniel Castro, "The Impact of the EU's New Data Protection Regulation on AI," (Center for Data Innovation, March 27, 2018), accessed October 18, 2018, http://www2.datainnovation.org/2018-impact-gdpr-ai.pdf.

have their data used by a company, to an "opt in" privacy system, in which companies can only use data after obtaining affirmative consent from users, will significantly harm advertising-based business models.[14] Overly restrictive and badly-designed data protection laws can also result in less access to data or constrain how it can be used—both of which limits innovation. For example, the GDPR requirement of "purpose specification"—which prohibits the reuse of data for purposes not compatible for with those for which it was first collected—prevents companies from experimenting with beneficial secondary uses for existing data.[15]

Second, the federal privacy framework should incentivize continuous improvement in terms of privacy-enhancing policies and technologies. Frequently, companies iterate on their privacy policies and technologies over time to improve the overall consumer experience. This process, however, often comes with growing pains. For example, Google recently created some controversy when it rolled out a new function on its Google Maps app, called Location History, that would pause location data collection to increase user privacy.[16] However, the function's wording suggested that it would pause all data collection from the company rather than that particular app. Responding to this controversy, Google updated its policies to clarify how the function worked, improve transparency, and still enable users increased privacy through the feature. NTIA's privacy framework should encourage this iterative process because it leads to better outcomes for consumers and flexibility for businesses. Indeed, while companies experiment with many new privacy-enhancing technologies, such as Apple's work with differential privacy, these technologies will not solve every privacy problem nor will they suit every business model.[17] By promoting innovation as a privacy outcome, NTIA's privacy framework can promote a flexible model that ensures companies continue to learn and improve upon consumer privacy.

By including this addition as an outcome for any legislative or executive solution, not only will NTIA ensure it balances other privacy outcomes that if misapplied have the potential to limit the supply of innovative technologies and services and therefore harm consumers, but it will ensure that consumers can continue to

[14] Avi Goldfarb and Catherine E. Tucker, "Privacy Regulation and Online Advertising." SSRN Scholarly Paper ID 1600259, 2010, Rochester, NY, Social Science Research Network, accessed October 18, 2018, https://papers.ssrn.com/abstract=1600259.
[15] Regulation 2016/679 (General Data Protection Regulation), Article 6, (see page L 119/36-37), accessed December 19, 2017, http://ec.europa.eu/justice/dataprotection/reform/files/regulation_oj_en.pdf.
[16] Ryan Nakashima, "AP Exclusive: Google tracks your movements, like it or not," *Associated Press*, August 13, 2018, accessed October 18, 2018, https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb.
[17] "Differential Privacy," Apple, accessed October 18, 2018, https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf.

benefit from low-cost, high-quality online services, while at the same time ensuring that the United States continues to lead in the Internet economy.[18]

B. High-level Goals for an End-State for U.S. Consumer Privacy Protections

The RFC seeks information on several questions related to the eight high-level goals to achieve the ideal consumer privacy protection framework. In particular, the RFC asks: *(1) Are there other goals that should be included, or outcomes that should be expanded upon? (2) Are the descriptions clear? Beyond clarity, are there any issues raised by how the issues are described? (3) Are there any risks that accompany the list of goals, or the general approach taken by the Department?*

ITIF welcomes and supports the NTIA's high-level goals for an end-state for U.S. consumer privacy protections. However, ITIF recommends NTIA make two changes to these goals.

First, the description of the goal to "employ a risk and outcome-based approach" should specifically state that different types of data have different types of potential privacy harms associated with them, and not treat all data the same. There are four types of personally identifiable information[19]:

- **Observable information** is personal information that can be perceived first-hand by other individuals. This category includes both observable personal information created by the individual about him or herself, as well as observable personal information captured by a third party. An example of the former is personal correspondence, such as letters or emails that a person has written. Examples of the latter primarily come from recorded media, such as video surveillance (e.g., CCTV camera footage), photographs (e.g., personal photos), or audio recordings (e.g., recording of a conversation). Media captures personal data in a way that, while recorded by a third party, any individual can observe it for themselves by looking at the photo, watching the video, or listening to the recording.

[18] Alan McQuinn and Daniel Castro, "Why Strong Privacy Regulations Do Not Spur Increased Internet Use" (Information technology and Innovation Foundation, July 2018), accessed October 18, 2018, http://www2.itif.org/2018-trust-privacy.pdf.
[19] Daniel Castro and Alan McQuinn, "ITIF Comments to the FTC on Informational Injury Workshop" (Information Technology and Innovation Foundation, October 2017), accessed October 18, 2018, https://itif.org/publications/2017/10/27/itif-filing-ftc-informational-injury-workshop.

- **Observed information** is information collected about an individual based on a third party's observation or provided by the individual, but does not allow someone else to replicate the observation. This data can encompass a wide variety of information that describes an individual, such as their basic information (e.g., place of birth, date of birth, etc.), physical traits (e.g., weight, eye color, etc.), personal preferences (e.g., likes and dislikes, political views, search history, reading habits, media consumption, etc.), social traits (e.g., degrees, religious affiliations, nationality, criminal history, etc.), family information (e.g., marital status, child information, etc.), employment information (e.g. job history, salary, etc.), biological conditions (e.g., sexual orientation, medical conditions, medical lab results, disability information, etc.), and geolocation information.

- **Computed information** is information inferred or derived from observable or observed information.[20] Computed information is produced when observable or observed information is manipulated through computation to produce new information that describes an individual in some way. For example, companies construct online advertising profiles for consumers based on many different sources of observed information, such as direct-mail responses, search history, and demographic information. Or some companies use algorithms to analyze video feeds to count how many people walk past a certain location. Similarly, biometrics are derived through a computational process from scans of unique physical characteristics on a person's body. For example, the Transportation Security Agency (TSA) uses backscatter x-ray machines to scan individuals' bodies during security screenings at airports to generate a generic outline of a human body with areas containing potential contraband highlighted in the image.[21] Information in this category is primarily used to create value for the organizations that computed the information, and often has fewer privacy implications for individuals. However, computed information may be generated from multiple sets of data and combined to give a "mosaic" picture of an individual's life.[22]

---

[20] The definitions we use in this report for "observed information" and "computed information" are similar to the ones the Article 29 Working Group has used for "observed data" and "inferred data." See Article 29 Data Protection Working Party, "Guidelines on the right to data portability," December 13, 2016, revised April 5 2017, 10, https://iapp.org/media/pdf/resource_center/WP29-2017-04-data-portability-guidance.pdf,.

[21] Transportation Security Administration, "TSA completes installation of state-of-the-art checkpoint screening equipment at six Minnesota airports," *news release,* June 8, 2017, accessed October 24, 2017, https://www.tsa.gov/news/releases/2017/06/08/tsa-completes-installation-state-art-checkpoint-screening-equipment-six.

[22] Benjamin Wittes, "Database: Digital Privacy and the Mosaic," *Brookings Institution*, April 1, 2011, accessed October 26, 2017, https://www.brookings.edu/research/databuse-digital-privacy-and-the-mosaic/.

- **Associated information** is information that a third party associates with an individual. Associated information, by itself and unlike the other three categories, does not provide any descriptive information about an individual (i.e. it does not describe qualities about an individual). For example, a library card number alone does not provide any information about its owner. (Someone may be able to infer information about an individual based on the fact that he or she has a library card, but the numbers in the library card itself generally convey no meaning about the individual.) There are many different types of associated information, such as government identification information (e.g., Social Security numbers, driver's license numbers, security clearances, etc.), contact information (e.g., name, home addresses, phone numbers, email addresses, etc.), device identifiers (e.g., IP addresses, MAC address, browser cookies, etc.), property information (e.g., land titles, vehicle registration numbers, etc.), online authentication information (e.g., screen names, passwords, security tokens, etc.), and financial information (e.g., bank account numbers, credit card numbers, insurance details, etc.). Information in this category, since it does not describe an individual, has no inherent privacy implications itself. However, this information can be used to perpetrate actions that have privacy implications. For example, the PIN number of a bank card has no inherent privacy implications, but a third party might use a stolen PIN number to check someone's balance at a bank, an action which clearly has privacy implications.

Each of these types of information come with their own set of risks of harms, and a federal privacy framework should reflect these different risks. For example, where the primary concern is autonomy violations, such as with observable information, laws should prohibit collecting this information, such as laws restricting government surveillance. Where the primary concern is discrimination, such as with observed information, laws should prohibit the discriminatory conduct.[23]

NTIA's privacy framework should distinguish between these different types of information rather than treating all information the same.

Second, NTIA should add one top-level goal to the list: to improve U.S. competitiveness. Competitiveness is the ability of a nation's traded sectors to effectively compete in global markets in the absence of subsidies and

[23] Ibid.

government protections, while receiving a strong price premium that enables strong terms of trade.[24] Many countries have started using data protection legislation to disadvantage U.S. firms, from the EU's GDPR to data localization requirements many nations have imposed. Indeed, the United States' lead on innovation is no longer as secure as it once was, and any regulatory approach to privacy that does not consider issues of U.S. competitiveness will certainly further disadvantage U.S. firms and workers.[25] The NTIA's privacy framework should consider how U.S. businesses are positioned vis-à-vis their foreign competitors with regard to the restrictions placed on them for use and collection of data, and ensure U.S. businesses continue to have access to data necessary to be competitive. In addition, the U.S. should insist that commitments to the free flow of data go hand-in-hand with any concessions it makes to other countries' privacy rules.

C. The Next Steps to Achieve these Goals

The RFC seeks information on several questions related to the next steps and measures that the administration can take to effectuate the high-end goals and user-centric outcomes. In particular, the RFC asks: *Should the Department convene people and organizations to further explore additional commercial data privacy-related issues? If so, what is the recommended focus and desired outcomes?*

Evidenced-based policymaking is an important tool to ensure that laws and regulations are effective. Before the administration pursues a new consumer privacy framework, it should identify in advance what metrics it will use to measure the effectiveness of any changes to U.S. privacy law. For example, metrics such as the number and size of data breaches, the amount of financial fraud from identity theft, the number of identity theft complaints, greater cross-border data flows, consumer privacy concerns in federal surveys, and many others, could all give a clearer picture of the impact of any changes in law. Without a clear, predetermined understanding of what a "winning" privacy framework would look like, a new set of data privacy rules might simply create higher costs and more market uncertainty that reduce innovation and competitiveness, as past efforts, such as the Gramm-Leach-Bliley Act (GLBA) did for privacy in financial services.[26] For example, the

[24] Robert D. Atkinson, "The Competitiveness Edge: A Policymakers' Guide to Developing a National Strategy" (Information Technology and Innovation Foundation, December 2017), accessed October 18, 2018, http://www2.itif.org/2017-competitive-edge.pdf.

[25] Robert D. Atkinson, "If We Had a National Competitiveness Policy Based on Innovation, How Would We Know It Was Working?" *Information Technology and Innovation Foundation*, June 5, 2018, accessed October 18, 2018, https://itif.org/publications/2018/06/05/if-we-had-national-competitiveness-policy-based-innovation-how-would-we-know.

[26] Daniel Castro and Alan McQuinn, "Comments to the Consumer Financial Protection Bureau on Bank Privacy Notices," (Information Technology and Innovation Foundation, August 10, 2016), http://www2.itif.org/2016-cfpb-comments.pdf.

mandatory privacy notices required by GLBA cost financial institutions approximately $700 million annually, with little value for consumers.[27]

E. FTC Enforcement

The RFC seeks information on the FTC's role as the prominent U.S. enforcement agency related to data protection issues. In particular, the RFC asks: *In order to achieve the goals laid out in this RFC, would changes need to be made with regard to the FTC's resources, processes, and/or statutory authority?*

As the primary regulator for consumer privacy, the FTC provides an important function in protecting consumers and ensuring competition in many areas of the U.S. economy. No matter what path the administration takes to update the U.S. consumer privacy framework, the FTC should continue to be the primary U.S. privacy enforcement agency. However, to accomplish this mission, the FTC will need more resources and expanded authority.[28]

Regarding resources, the FTC has been woefully under-equipped for some time. Since 2010, the Commission's funding has fallen 5 percent when adjusted for inflation.[29] In addition, in 2015, the FTC had only 57 full-time staff working on data protection issues.[30] And several former FTC alumni have lamented that the commission has trouble hiring the requisite technical expertise due to insufficient resources.[31] The FTC needs additional funding to pursue privacy and security cases and hire more staff with this expertise.

---

[27] Daniel Castro, "Bank Privacy Notices Cost Consumers Over $700M Annually," (Information Technology and Innovation Foundation, June 22, 2012), https://www.innovationfiles.org/bank-privacy-notices-costs-consumers-over-700m-annually/.

[28] Maureen K. Ohlhausen, "Putting the FTC Cop Back on the Beat" (Federal Trade Commission, November 18, 2017), accessed October 18, 2018, https://www.ftc.gov/system/files/documents/public_statements/1280393/putting_the_ftc_cop_back_on_the_beat_mko.pdf.

[29] David McCabe, "Mergers are spiking, but antitrust cop funding isn't," *Axios*, May 7, 2018, accessed October 19, 2018, https://www.axios.com/antitrust-doj-ftc-funding-2f69ed8c-b486-4a08-ab57-d3535ae43b52.html.

[30] Nuala O'Connor, "Statement of Nuala O'Connor before the U.S. Senate Committee on Commerce, Science, and Transportation - Consumer Data Privacy: Examining Lessons From the European Union's General Data Protection Regulation and the California Consumer Privacy Act," (Center for Democracy and Technology, October 10, 2018, accessed October 19, 2018, https://cdt.org/files/2018/10/2018-10-09-FINAL-Nuala-OConnor-Written-Testimony-Senate-Commerce.pdf.

[31] For example, see the comments of Jessica Rich, former director of the FTC's Bureau of Consumer Protection. Tony Romm, "The Agency in Charge of Policing Facebook and Google is 103 Years Old. Can it Modernize?" *Washington*

Moreover, the FTC needs expanded authority to extract meaningful fines from companies that intentionally mislead consumers or violate their privacy. For one, because the Commission's existing enforcement falls under Section 5 of the FTC Act, it does not possess original fining authority. Before a company can be fined by the FTC for misbehavior, it must agree to be placed under a consent decree, and then subsequently violate that agreement. (Certainly, a consent decree is no small punishment. It can confine a company to stagnant business practices, deter them from taking risks, and create greater barriers to new firms by subjecting them to costly, cumbersome, and complex de facto regulations under threat of potential lawsuits.[32])

Furthermore, the amount of the fine that the FTC has the authority to levy is often a de minimis amount of an infringing company's profits. For example, when Google violated its consent decree in 2012, it was only fined $22.5 million for the infraction—a fee that is fractional compared to the company's annual revenue.[33] While fees need to be proportional to the actual harm caused to consumers, rather than to trivial violations of privacy policies, if fees are too small they are unlikely to deter data misuse from other actors in the future. Importantly, while Congress should give the FTC the authority to pursue larger fines against infringing companies, the FTC should take a deliberative harms-based approach, as overly aggressive fines can have a deteriorative effect on innovation.[34] For example, GDPR's fines can be up to 4 percent of global turnover for a company or EUR 20 million, whichever is greater.[35] The mere threat of these absurdly steep fines has already caused some businesses to shut down their services in Europe.[36] The U.S. government should not repeat the European Union's mistakes.

Post, May 4, 2018, accessed October 19, 2018, https://www.washingtonpost.com/news/the-switch/wp/2018/05/04/can-facebook-and-googles-new-federal-watchdogs-regulate-tech/.

[32] Daniel Castro and Alan McQuinn, "How and When Regulators Should Intervene" (Information Technology and Innovation Foundation, February 2016), http://www2.itif.org/2015-how-when-regulators-intervene.pdf.

[33] J. Thomas Rosch, "Dissenting Statement of Commissioner J. Thomas Rosch, In the Matter of Google Inc., FTC Docket No. C-4336" (Federal Trade Commission, August 9, 2012), accessed October 19, 2018, https://www.ftc.gov/sites/default/files/documents/public_statements/dissenting-statement-commissioner-j.thomas-rosch-google-inc./safari/120809googleincstatement.pdf.

[34] McQuinn and Castro, "Why Strong Privacy Regulations Do Not Spur Increased Internet Use."

[35] Regulation 2016/679 (General Data Protection Regulation).

[36] Daniel Castro and Alan McQuinn, "GDPR Freeloaders: Why Other Countries Should Fight Back," *Information Technology and Innovation Foundation*, August 16, 2018, accessed October 19, 2018, https://itif.org/publications/2018/08/16/gdpr-freeloaders-why-other-countries-should-fight-back.

Because the FTC is prohibited from using traditional rulemaking processes, it has created de facto law around privacy and security through its enforcement actions and consent decrees.[37] This process circumvents the democratic process and decreases transparency in rulemakings.[38] The administration should support Congress in expanding the FTC's authority by enabling it to conduct rulemakings around privacy. This approach will enable the FTC to establish clear rules through its public processes and act against companies that knowingly violate them. However, such rulemakings should maintain the FTC's remit to address substantial consumer harms. In these rulemakings, the administration should ensure that the FTC pays attention to harm and intent when using its enforcement authority against companies to avoid creating perverse incentives.[39] These criteria will enable the regulator to decide on the appropriate response, where unintentional and harmless actions elicit the smallest penalty and intentional and harmful actions elicit the largest. Penalties should be designed to encourage companies to make sure they do not willfully commit infractions or impose real harm on users.

Finally, it will be important for the FTC to use expanded resources in a strategic way to go after actors causing the most harm in the digital space, not simply going after high-profile privacy cases where consumers suffered little or no actual harm. These include identity theft, spam, malware, deceptive digital advertising and service provision, and Internet piracy. These, more than privacy violations, cause the most actual consumer harm today.

G. Other Goals

Finally, the RFC seeks information on other ways to achieve U.S. leadership in privacy protections. The RFC asks: *Are there other ways to achieve U.S. leadership that are not included in this RFC, or any outcomes or high-level goals in this document that would be detrimental to achieving the goal of achieving U.S. leadership?*

The United States has traditionally had a balanced, sectoral approach to data privacy, which has enabled it to be the world leader in innovative digital services. Of the 15 largest digital firms in the world, all are either

[37] Daniel Solove and Woody Hartzog, "The FTC and the New Common Law of Privacy" 114 Columbia L. Rev. 583, (2014), accessed October 19, 2018, https://cyberlaw.stanford.edu/files/publication/files/SSRN-id2312913.pdf.
[38] Daniel Castro and Alan McQuinn, "How and When Regulators Should Intervene" (Information Technology and Innovation Foundation, February 2016), http://www2.itif.org/2015-how-when-regulators-intervene.pdf.
[39] Castro and McQuinn, "How and When Regulators Should Intervene."

American or Chinese.[40] Of the top 200, only 8 are European.[41] There is a reason for that, and one is the United States has a more light-touch approach to digital regulation, including regarding privacy. And yet, the United States has largely failed to advocate for the effectiveness of its regulatory approach to data privacy. In contrast, the European Union has actively sought to expand its regulatory model, particularly the GDPR, to other countries though both advocacy and enforcement of the rules themselves, advocating a false narrative that many have bought into that the GDPR is pro-innovation. This strategy has been successful. For example, in 2017, Colombia issued rules copying GDPR's approach to international data flows by preventing businesses from transferring personal data outside the country without the permission of users, unless the other country is found to provide an "adequate level" of protection.[42]

Not only should the administration use every available forum to push back on these negative policy approaches that damage the digital economy, but it should vocally and forcefully be advocating for the U.S. approach to data privacy abroad. The U.S. government can do this through bilateral agreements, such as those established in the Clarifying Overseas Use of Data (CLOUD) Act, through trade agreements, and in international multistakeholder forums.[43] It can do this by more actively participating in and supporting the participation of U.S. organizations in international forums. It can expand the State Department's digital attaché program and ensure that more State Department foreign service officers understand the different international approaches to data privacy and the advantages of the U.S. approach. Importantly, the U.S. government should do this no matter how the NTIA process ends or what final federal framework the Trump administration decides for U.S. data privacy.

CONCLUSION

Data is essential to a functioning global digital economy. The administration should ensure that its path forward for a U.S. privacy framework not only balances consumer protections with support for data-driven innovation but also actively advocates for that position to other nations. In establishing this path forward, the administration should consider levels of risk inherent to specific types of data and their uses, how it will

---

[40] "Europe's History Explains Why it Will Never Produce a Google," *The Economist*, October 13, 2018, accessed October 19, 2018, https://www.economist.com/europe/2018/10/13/europes-history-explains-why-it-will-never-produce-a-google.

[41] Ibid.

[42] "Adicionar un Capítulo Terecero al Tíitulo V de la Circular Única," Industria y Comercio Superintendencia, August 10, 2017, accessed October 18, 2018, http://www.sic.gov.co/sites/default/files/normatividad/082017/Circular_Externa_005_de_2017.pdf.

[43] Nigel Cory and Alan McQuinn, "Will the US capitalize on its opportunity to stop data localization?" *The Hill*, September 9, 2018, accessed October 19, 2018, https://thehill.com/opinion/cybersecurity/405422-will-the-us-capitalize-on-its-opportunity-to-stop-data-localization.

measure success, and U.S. competitiveness. Finally, the administration should respect and improve upon the role that the FTC has traditionally held as the predominant U.S. privacy regulator.

Sincerely,

Daniel Castro
Vice President, Information Technology and Innovation Foundation

Alan McQuinn
Senior Policy Analyst, Information Technology and Innovation Foundation