ACLP
ADVANCED COMMUNICATIONS LAW & POLICY INSTITUTE
at New York Law School

NEW YORK LAW SCHOOL

November 9, 2018

The Honorable David J. Redl
Assistant Secretary for Communications & Information
National Telecommunications & Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, D.C. 20230

Re: Docket No. 180821780-8780-01 – Developing the Administration's Approach to Consumer Privacy

Dear Assistant Secretary Redl,

The Advanced Communications Law & Policy Institute (ACLP) at New York Law School respectfully submits the following comments in the above-referenced docket.

Overview

THE ADVANCED COMMUNICATIONS LAW & POLICY INSTITUTE AT NEW YORK LAW SCHOOL
185 West Broadway, E-1016 ▪ New York, NY 10013
T 212-431-2100 ▪ **E** ACLP@nyls.edu

* * * * * *

1. INTRODUCTION & EXECUTIVE SUMMARY

NTIA is to be commended for spearheading an inquiry to identify the ideal parameters of federal action impacting consumer data privacy. As the principal advisor to the President on telecommunications and information policy matters, NTIA has a critical role to play in building momentum toward the development and implementation of a comprehensive national privacy framework. For too long, policymakers have paid meager lip-service to the framework for addressing, and merits of, key data privacy issues – creating a legal and regulatory vacuum that individual states and foreign nations have begun to fill on a patchwork basis. The result is a chaotic privacy "regime" that does little to provide consumers and innovators with the certainty and predictability that is essential to continued economic, technological, and social progress.

1.1 *Why Federal Action is Needed*

Continued failure by federal policymakers to address privacy issues in a comprehensive manner will negatively impact consumers and innovation in several ways.

First, the absence of strong, consistent, and predictable privacy protections could result in less robust broadband adoption. There is a well-documented relationship between privacy concerns and consumers' use of technology, including broadband.[1] According to recent

[1] *See, e.g., Barriers to Broadband Adoption: A Report to the FCC,* ACLP at New York Law School (Oct. 2009), http://www.nyls.edu/advanced-communications-law-and-policy-institute/wp-content/uploads/sites/169/2013/08/ACLP-Report-to-the-FCC-Barriers-to-BB-Adoption.pdf; *Connecting*

survey data collected by NTIA, "[n]early three-quarters of Internet-using households had significant concerns about online privacy and security risks in 2017," with one-third noting that "these worries caused them to hold back from some online activities."[2] More recent survey data collected by Harris found that 78% of respondents reported that a company's ability to maintain the privacy of their data "extremely important" to them, but only 20% completely trust the organizations with which they interact online.[3]

Some have attempted to use this seemingly contradictory dynamic – *i.e.,* significant consumer mistrust of online organizations coupled with continued high levels of use of digital services – to argue that comprehensive privacy action is unnecessary because consumers really don't care how their data is collected and used.[4] This canard is often deployed by those seeking to slow momentum toward formal privacy regulation and protect the business models of dominant tech firms. In reality, consumers feel they have little choice but to use major tech platforms to search for information, connect with friends, or purchase goods.[5] Moreover, in the aftermath of major data breaches and privacy violations, consumers tend to pull back on their use of certain services, demonstrating that consumer behavior does change when more information about data collection practices is made public.[6] This suggests that consumer empowerment via clear privacy protections and more transparency by data collectors could position users as stronger regulators of the marketplace.[7]

America: The National Broadband Plan, at p. 53, FCC (March 2010), https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf; *Broadband Adoption Toolkit,* at p. 4, NTIA (May 2013), https://www2.ntia.doc.gov/files/NTIA_2013_BroadbandUSA_Adoption_Toolkit.pdf.

[2] *See* Rafi Goldberg, *Most Americans Continue to Have Privacy and Security Concerns, NTIA Survey Finds,* Aug. 20, 2018, NTIA, https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds.

[3] *See IBM Cybersecurity and Privacy Research,* at p. 21, The Harris Poll (April 13, 2018), https://newsroom.ibm.com/download/IBM+Cybersecurity+PR+Research+-+Final.pdf.

[4] *See, e.g.,* Alan McQuinn & Daniel Castro, *Why Stronger Privacy Regulations Do Not Spur Increased Internet Use,* ITIF (July 2018), http://www2.itif.org/2018-trust-privacy.pdf?_ga=2.165610170.480481664.1541076564-869707105.1534855862.

[5] As discussed in more detail below, significant financial incentives shape the behavior of tech platforms vis-à-vis consumers' data. This explains why Facebook, for example, has long sought to position itself as something akin to a utility service – *i.e.,* a "basic necessity" that users cannot live without. *See* Josh Constine, *Facebook Doesn't Want to be Cool, it Wants to be Electricity,* Sept. 18, 2013, TechCrunch, https://techcrunch.com/2013/09/18/facebook-doesnt-want-to-be-cool/.

[6] *See, e.g.,* Gina Pingitore et al., *To Share or Not to Share: What Consumers Really Think About Sharing their Personal Information,* Sept. 5, 2017, Deloitte Insights, https://www2.deloitte.com/insights/us/en/industry/retail-distribution/sharing-personal-information-consumer-privacy-concerns.html (highlighting a number of "punitive" actions – from disabling cookies to stopping their use of a particular site or service – that consumers have taken in the aftermath of data breaches).

[7] Consumer empowerment via public education has long been a goal of federal agencies like the Department of Commerce and the Federal Trade Commission. *See, e.g., Protecting Consumers Online,* at p. 16-17, A Report

Second, without explicit guardrails in place, consumers will remain at the mercy of rapacious, data-hungry tech firms, increasing the chances of harmful privacy intrusions. Indeed, those entities whose business models revolve around the monetization of consumers' data will continue to push the limits of intrusive data extraction if the federal government continues to drag its feet in the privacy context – and consumers will only know the true extent of these techniques when it's too late, *i.e.,* after the next data breach or privacy intrusion. The seemingly endless series of "revelations" about intrusive data collection techniques over the last few years could have likely been prevented, or, at a minimum, greatly curtailed had clear, consistent privacy rules been in place. Similarly, the inability – and, in some cases, unwillingness – of regulators to investigate and punish firms for their careless handling of user data fostered a status quo that did little to dissuade companies from engaging in data collection activities that many consider repugnant.[8]

Third, failure to act will negatively impact innovation. The race to monopolize data and the revenues that stem from its monetization has created a dynamic where dominant firms make it difficult for new competitors to enter a market or gain share.[9] This chills innovation by starving markets of new entrants, new ideas, and new business models. Similarly, as companies strive for data dominance across the myriad of devices, networks, and applications that consumers use every day, "firms are focused on building platforms that can span these various uses and tie the data together more cohesively. In many ways, this presages a new era of "walled gardens," where online firms seek to serve as the exclusive portal through which users navigate nearly all online services. The business practices surrounding the creation of such "gardens" and the ways in which companies direct their users into them could foster anticompetitive behavior."[10] Such behavior undermines innovation and ultimately harms consumers.[11]

---

from the FTC Staff (Dec. 1999), https://www.ftc.gov/sites/default/files/documents/reports/protecting-consumers-online/fiveyearreport.pdf; *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*, at p. iv, U.S. Dept. of Commerce (Dec. 2010), https://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf. As discussed below, these efforts have not been robust enough, due in large part to a lack of direction from Congress.

[8] *See Competition and Consumer Protection in the 21st Century Hearings*, Comments of the ACLP, at p. 5-6, FTC Project Number P181201 (Aug. 20, 2018), http://www.nyls.edu/advanced-communications-law-and-policy-institute/wp-content/uploads/sites/169/2018/08/ACLP-FTC-Filing-re-Competition-Issues-August-20-2018.pdf ("*ACLP FTC Comments*").

[9] *See, e.g., American Tech Giants are Making Life Tough for Startups,* June 2, 2018, The Economist, https://www.economist.com/business/2018/06/02/american-tech-giants-are-making-life-tough-for-startups ("Once a young firm enters [a market], it can be extremely difficult to survive. Tech giants try to squash startups by copying them, or they pay to scoop them up early to eliminate a threat.").

[10] *ACLP FTC Comments* at p. 11.

[11] *See, e.g.,* Maurice E. Stucke, *Should We Be Concerned About Data-opolies?,* 2 Geo. L. Tech. Rev. 275, 303-307 (2018), https://www.georgetownlawtechreview.org/wp-content/uploads/2018/07/2.2-Stucke-pp-275-324.pdf; David Wessel, *Is Lack of Competition Strangling the U.S. Economy?,* Harvard Business Review (March/April 2018), https://hbr.org/2018/03/is-lack-of-competition-strangling-the-u-s-economy ("…Facebook's relentless swallowing up of promising young firms effectively squashes the potential of upstarts to become competitors.

For these reasons, it is respectfully submitted that NTIA should advise the Executive Branch to push for meaningful federal legislative action – action that can deliver to consumers strong privacy protections while also preserving important incentives for private firms to continue investing in and experimenting with new offerings.

1.2 *Comments Overview*

These comments offer a range of observations and recommendations to NTIA in an effort to guide its work in developing a framework that will hopefully serve as the foundation for federal privacy legislation.

- **Section 2** highlights the need for federal action to provide certainty, predictability, and consistency in the administration of privacy rights and enforcement. To date, efforts to protect consumer privacy have been scattershot, with multiple actors at the federal level acting in an ad hoc manner in the aftermath of data crises. Consumer welfare suffers in such an environment.

- **Section 3** examines the importance of developing and implementing a national framework for consumer data privacy. Without federal action, states will continue to experiment with their own privacy laws. Such a Balkanized approach to data privacy risks undermining consumer welfare and chilling innovation.

- **Section 4** identifies several additional elements that must be part of any federal action on consumer privacy. These include: establishing clear consumer rights in their data; assuring a technology-neutral approach to the application of new privacy rules; and providing adequate guidance to the FTC vis-à-vis its implementation and enforcement of a national privacy framework.

2. CERTAINTY, PREDICTABILITY, AND CONSISTENCY ARE ESSENTIAL TO STRENGTHENING CONSUMER DATA PRIVACY

To date, efforts to address consumer data privacy have not been guided by any semblance of an overarching principle. Instead, data privacy "regulation" has been largely ad hoc at both the federal and state levels, creating significant uncertainty and unpredictability. As a result, outcomes have been disappointing from the vantage of protecting and empowering consumers in the digital ecosystem. This dynamic is poised to worsen for consumers as data collection and monetization become more prevalent in key sectors like education, healthcare, and transportation – sectors that have long been governed by separate laws regarding the collection and use of personal information. Overlapping authority and fragmented enforcement could greatly undermine consumer welfare.

We'll never know what TBH or Halli Labs or Orbitera or Instagram or WhatsApp or Oculus VR might have become had Facebook not absorbed them – or what companies might have been started had prospective founders not figured that it would be impossible to compete with Facebook.").

Section 2.1 examines the mechanics and practical consequences of this state of play.

Section 2.2 identifies how NTIA can address these issues and provide more certainty, predictability, and consistency.

2.1 *The Problem: Uncertainty Stemming From Inconsistent and Unpredictable Privacy Oversight and Enforcement in a Rapidly Changing Digital Ecosystem*

Analogizing data to oil illuminates the forces and incentives shaping the digital ecosystem, including the relationships between stakeholders working to gather consumers' information.

> "Data are to this century what oil was to the last one: a driver of growth and change. Flows of data have created new infrastructure, new businesses, new monopolies, new politics and—crucially—new economics. Digital information is unlike any previous resource; it is extracted, refined, valued, bought and sold in different ways. It changes the rules for markets and it demands new approaches from regulators. Many a battle will be fought over who should own, and benefit from, data."[12]

Like the oil sector, the commoditization of consumers' data and the significant revenues that can be derived from its monetization have prompted a diverse array of firms to explore the extraction of personal information.

- Any computing device linked to the Internet – a laptop used at home; a desktop used at work; a smartphone used on the go – generates data that can be collected and used in a range of ways, including via an operating system (*e.g.,* Apple iOS or Android); sensors built into smartphones (*e.g.,* accelerometers and gyroscopes); web browser (*e.g.,* Google Chrome); search engine (*e.g.,* Bing); data broker (*e.g.,* Acxiom); app developer (*e.g.,* Activision Blizzard); and content provider (*e.g.,* YouTube).[13]

- A range of new smart home products leverage sensors and other communications technologies to generate vast amounts of data that assist in optimizing particular

---

[12] *See Data is giving rise to a new economy,* May 6, 2017, The Economist, https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy.

[13] For an overview of the myriad of ways in which firms can use smartphones to track users and gather data, *see* David Nield, *All the Ways Your Smartphone and its Apps Can Track You,* Jan. 4, 2018, Gizmodo, https://gizmodo.com/all-the-ways-your-smartphone-and-its-apps-can-track-you-1821213704. *See also* Kashmir Hill and Surya Mattu, *Facebook Knows How to Track You Using the Dust on Your Camera Lens,* Jan. 11, 2018, Gizmodo, https://gizmodo.com/facebook-knows-how-to-track-you-using-the-dust-on-your-1821030620.

services and that provide more granular insights into individual and aggregate consumer behavior.[14]

- Ad-supported Wi-Fi networks that blanket large urban areas across the country rely on the data collected from users and passersby to demonstrate value to firms wishing to precisely target ads.[15] Billboards are increasingly leveraging similar kinds of data and collection techniques to ensure that ads are relevant.[16] And in addition to tracking online purchases, many retailers also track in-store shopping, browsing, and buying habits of customers by using facial recognition and tapping into data emanating from their smartphones.[17]

- In-home devices like smart TVs, voice assistants (*e.g.,* Amazon's Alexa), and hybrid offerings (*e.g.,* Facebook's Portal) actively listen to consumers, gather relevant information, respond to commands to purchase new products, change the channel, or search for the answer to a question. It is possible – and increasingly attractive to firms – to use the information gathered from these devices to target ads.[18] Similarly, wearable products like smart watches offer real-time portals into personal health data and other metrics that, in turn, help companies develop detailed portraits of users.[19]

- The continued improvement of artificial intelligence, the foundation upon which many of these new "smart" products is built, relies on a constant stream of data in

---

[14] *See* Kashmir Hill and Surya Mattu, *The House that Spied on Me,* Feb. 7, 2018, Gizmodo, https://gizmodo.com/the-house-that-spied-on-me-1822429852.

[15] *See, e.g.,* Benjamin Dean, *The Heavy Price We Pay for 'Free' Wi-Fi,* Jan. 25, 2016, The Conversation, https://theconversation.com/the-heavy-price-we-pay-for-free-wi-fi-52412 (articulating an array of concerns regarding the *quid pro quo* involved in providing "free" online services in exchange for the collection of granular personal information).

[16] *See, e.g.,* Grant Gross, *Billboards Can Track Your Location, and Privacy Advocates Don't Like it*, March 3, 2016, CSO, http://www.csoonline.com/article/3040607/security/billboards-can-track-your-location-and-privacy-advocates-dont-like-it.html; Marianna Kantor, *How Billboards are Challenging Digital Advertising,* June 13, 2018, ESRI, https://www.esri.com/about/newsroom/publications/wherenext/out-of-home-advertising-and-location-intelligence/.

[17] *See, e.g.,* Erin Griffith, *Consumers Hate In-Store Tracking (But Retailers, Startups and Investors Love it)*, March 24, 2014, Fortune, http://fortune.com/2014/03/24/consumers-hate-in-store-tracking-but-retailers-startups-and-investors-love-it/; Annie Lin, *Facial recognition is tracking customers as they shop in stores, tech company says,* Nov. 23, 2017, CNBC, https://www.cnbc.com/2017/11/23/facial-recognition-is-tracking-customers-as-they-shop-in-stores-tech-company-says.html.

[18] *See, e.g.,* Kurt Wagner, *It turns out that Facebook could in fact use data collected from its Portal in-home video device to target you with ads,* Oct. 16, 2018, Recode, https://www.recode.net/2018/10/16/17966102/facebook-portal-ad-targeting-data-collection.

[19] *See, e.g.,* Olga Kharif, *Coming Soon to Your Smartwatch: Ads Targeting Captive Eyeballs*, May 12, 2015, Bloomberg, http://www.bloomberg.com/news/articles/2015-05-12/coming-soon-to-your-smartwatch-ads-targeting-captive-eyeballs.

order to improve the underlying algorithms and make them more useful and responsive to consumers.[20]

- As broadband-enabled technologies (*e.g.*, wireless sensors, smart devices) seep further into key sectors like healthcare and transportation, even more firms will become engaged in the data trade. For example, the race to gain a first-mover advantage in the market for autonomous vehicles, which can generate upwards of 10 *terabytes* of data per car each day,[21] has resulted in a tech arms race among a number of firms, including legacy car manufacturers (*e.g.*, Ford), dominant tech firms (*e.g.*, Google), and new entrants (*e.g.*, Uber).[22] Insurance companies are relying more and more on "context-based" policies that adjust rates based on real-time information about customers' behavior.[23] Healthcare providers – doctors, hospitals, etc. – and insurers are increasingly using smart devices to collect mountains of data about patients.

Unlike the oil sector, there is a distinct lack of regulatory clarity for the digital ecosystem, where data reserves are vast.[24] Protecting consumers' data and policing privacy violations is challenging given the surfeit of firms trafficking in data, the diversity of contexts where personal information is being collected, and, most importantly, the lack of a comprehensive privacy framework to guide the monitoring and enforcement of possible privacy intrusions. Indeed, the absence of such a framework has yielded an inefficient and confusing patchwork of approaches.

Numerous actors at the federal and state levels possess some measure of authority to police how personal information is collected and used. For many years, bright lines identified the boundaries of each entity's jurisdictional reach, with the FTC and state Attorneys General filling any gaps that might arise. Now, these lines are blurring as data collection migrates online and as incentives to monetize that information – either directly, in the form of ads,

---

[20] *See, e.g.*, Brian Feldman, *The Future of Tech is Artificial Intelligence and That's Just Fine for Google*, May 18, 2016, New York Magazine, http://nymag.com/selectall/2016/05/googles-back.html.

[21] *See, e.g., Autonomous Vehicles: The Race is On,* at p. 5, Accenture (March 2018), https://www.accenture.com/t20180309T093025Z__w__/us-en/_acnmedia/PDF-73/Accenture-Autonomous-Vehicles-The-Race-Is-On.pdf.

[22] *See, e.g.*, David Welch and Elisabeth Behrmann, *Who's Winning the Self-Driving Care Race?,* May 7, 2018, Bloomberg, https://www.bloomberg.com/news/features/2018-05-07/who-s-winning-the-self-driving-car-race.

[23] *See, e.g.*, Enrique Dans, *The Rise of Real-Time, Context-Based Insurance,* March 12, 2017, Forbes, https://www.forbes.com/sites/enriquedans/2017/03/12/the-rise-of-real-time-context-based-insurance/#68b419032ad6.

[24] This was not always the case for the oil sector. *See, e.g.*, Michael Santorelli, *Halo, Goodbye: Cleaning Up the Digital Ecosystem After the Facebook Data Spill*, April 24, 2018, Forbes, Washington Bytes, https://www.forbes.com/sites/washingtonbytes/2018/04/24/halo-goodbye-cleaning-up-the-digital-ecosystem-after-the-facebook-data-spill/#3d7e00a311eb ("*Halo, Goodbye*").

or indirectly, by selling that information to third-parties like data brokers – become attractive to more and more firms. Uncertainty stemming from novel questions of jurisdictional reach will likely emerge.

The following provides but a sampling of examples where jurisdictional overlap and uncertainty could arise (or has already arisen) among federal agencies (state-level regulatory and legislative efforts in this context are examined in section 3):

- In the *transportation* sector, both the FTC and the U.S. Department of Transportation's National Highway Traffic Safety Administration have authority over the collection and use of data stemming from autonomous cars.[25] These two entities "have coordinated on privacy issues related to connected vehicles," but because NHTSA has failed to "clearly define[] its roles and responsibilities as they relate to the privacy of vehicle data…some stakeholders may be uncertain about its authority to address privacy issues."[26]

- A similar dynamic is apparent in the *healthcare* sector, where the FDA, via the Federal Food, Drug and Cosmetic Act; the FTC, via its general UDAP authority; and the Department of Health & Human Services, via administration of HIPAA, each play a role in shaping the contours of health data collection and use.[27]

- Overlap is also evident in the *education* space, where tech companies like Apple, Google, and Microsoft are jockeying to put their offerings in front of as many students as possible.[28] For these firms, a primary driver is building brand loyalty at a young age. But these firms, along with content providers like Facebook, are also increasing their efforts in this space in order to collect data from students.[29] Both the FTC and the U.S. Department of Education have roles to play in protecting students' data: the FTC has authority to enforce the Children's Online Privacy Protection Act, while the DOE is responsible for overseeing schools' compliance

---

[25] *See Vehicle Data Privacy: Industry and Federal Efforts Under Way, But NHTSA Needs to Define its Role,* U.S. Govt. Accountability Office, GAO-17-656 (July 2017), https://www.gao.gov/assets/690/686284.pdf.

[26] *Id.* at p. 32.

[27] *See, e.g.,* FTC, Mobile Health Apps Interactive Tool, https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool (identifying the roles that the FDA, FTC, and HHS play in the mobile health app space).

[28] *See, e.g.,* Brian Heater, *Comparing Apple, Google and Microsoft's Education Plays,* March 27, 2018, TechCrunch, https://techcrunch.com/2018/03/27/comparing-apple-google-and-microsofts-education-plays/.

[29] *See* Natasha Singer, *How Google Took Over the Classroom,* May 13, 2017, N.Y. Times, https://www.nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html.

with the Family Educational Rights and Privacy Act.[30] However, there is significant uncertainty about whether and how both laws might apply to student data being collected by tech firms like Google.[31]

- In the *financial* sector, both the FTC and the Consumer Finance Protection Bureau possess overlapping authority, pursuant to several federal laws (*e.g.,* Dodd-Frank, FCRA), over the collection and use of personal financial information.[32] In many instances, these two agencies have coordinated their enforcement efforts vis-à-vis harms arising from the misuse of such data.[33] However, there is a risk that "such overlap also can lead to enforcement inefficiencies and inconsistencies," especially if one agency is more aggressive in policing a particular sector than the other.[34] Such could evolve over time if the agencies take different approaches to new and emerging digital services (*e.g.,* fintech; data brokers).[35]

- In the *telecommunications* sector, the Federal Communications Commission (FCC) has long protected "customer proprietary network information" (CPNI), which encompasses "some of the most sensitive personal information that carriers and providers have about their customers as a result of their business relationship (*e.g.*, phone numbers called; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting)."[36] This information was long generated exclusively by basic telephone providers, which, as common carriers,

---

[30] *See, e.g., Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*, U.S. Dept. of Education (Feb. 2014), https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf.

[31] *See, e.g.,* Henry Kronk, *In Light of Facebook and Cambridge Analytica, Will Anyone Revisit Google's Data Collection in G Suite for Education?*, April 22, 2018, ElearningInside News, https://news.elearninginside.com/another-case-data-collection-google-g-suite-education/ (highlighting data collection practices by Google that might run afoul of FERPA); Sarah Perez, *Over 20 advocacy groups complain to FTC that YouTube is violating children's privacy law,* April 9, 2018, TechCrunch, https://techcrunch.com/2018/04/09/over-20-advocacy-groups-complain-to-ftc-that-youtube-is-violating-childrens-privacy-law/ (highlighting an FTC complaint about alleged violations of COPPA by YouTube).

[32] *See, e.g.,* Thomas B. Pahl, *The Future of Financial Services Enforcement at the FTC,* at p. 3, Business Law Today (Sept. 2017), https://www.ftc.gov/system/files/documents/public_statements/1261473/pahl_blt_the_future_of_financial_services_enforcement_at_the_ftc.pdf (discussing how the two agencies have coordinated enforcement of certain requirements contained in the Dodd-Frank Act of 2010).

[33] *Id.*

[34] *Id.*

[35] *See, e.g.,* Maria Earley and Ashley Shively, *When Worlds Collide – Navigating Fintech/Traditional Bank Partnerships to Deliver Value to Consumers,* April 2, 2018, BNA, https://www.bna.com/worlds-collide-navigating-n57982090683/.

[36] *See* FCC, Customer Privacy, https://www.fcc.gov/general/customer-privacy.

were exempt from FTC oversight.[37] A recent attempt by the FCC to expand these rules to encompass internet access services was rebuffed by Congress.[38] However, as more and more non-telecom firms offer communications services that are similar to traditional telephone service – *e.g.,* IP-enabled voice; video calling – consumers find themselves with different rights and protections depending on the service they use and the provider delivering that service. Such could create confusion and ultimately undermine consumer welfare.

For consumers and those acting on their behalf, navigating this incoherent maze can be daunting. For innovators, the inconsistent and unpredictable nature of privacy enforcement can undermine incentives to invest, innovate, and enter new markets. As such, action must be taken to rationalize these regimes.

2.2 *How NTIA Can Address the Problem*

In the Request for Comment (RFC) that opened this docket, NTIA identified a number of important "high-level goals for federal action," including "harmoniz[ing] the regulatory landscape," providing "legal clarity," and assuring "comprehensive application" of privacy rules.[39] These elements and the larger proposed approach in the RFC are laudable but incomplete. For example, NTIA notes that it is not interested in proposing changes to "current sectoral federal laws" impacting consumer privacy in specific sectors like healthcare.[40] As discussed above, this makes little sense given the increasing uncertainty stemming from the overlapping jurisdiction of a number of federal and state agencies. Consumers are left increasingly worse off.

Ultimately, an even more comprehensive analysis would be beneficial. In addition to identifying the goals and values that should undergird federal privacy responses, NTIA should also put forward a vision – template of sorts – for comprehensive action that acknowledges and reflects the complex and ever-changing data collection dynamics in the digital ecosystem. Doing so will help NTIA and other federal actors develop a truly consistent, predictable, and harmonized framework that will provide consumers and industry with the certainty needed to efficiently address data-related harms.

To achieve such certainty, consistency, and predictability, NTIA should recommend the pursuit of a comprehensive rethink of federal privacy laws. As a first step, it should bring together stakeholders from all impacted sectors, as well as academics and consumer

---

[37] 15 U.S.C. § 45(a)(2).

[38] *See* David Shepardson, *Trump signs repeal of U.S. broadband privacy rules,* April 3, 2017, Reuters, https://www.reuters.com/article/us-usa-internet-trump-idUSKBN1752PR.

[39] *See Developing the Administration's Approach to Consumer Privacy,* 83 Fed. Reg. 48,600, 48,602 (Sept. 26, 2018), https://www.ntia.doc.gov/files/ntia/publications/fr-rfc-consumer-privacy-09262018.pdf ("*NTIA RFC*").

[40] *Id.* at 48,601.

advocates, in an effort to gather the data and insights needed to identify where inefficiencies exist and where gaps remain in the patchwork privacy regime that has developed. That information should be used to shape the development of federal legislation that provides a more coherent and predictable approach to consumer data privacy – an approach that can provide consumers with consistent rights and protections in their data regardless of where, how and with whom they share it (more specific parameters of federal action discussed below in sections 3 and 4).

3. A National Framework for Data Privacy Will Greatly Enhance Consumer Welfare & Support Continued Innovation

The confusion and uncertainty stemming from the fragmented approach to privacy monitoring and enforcement described in section 2 is greatly compounded by concomitant efforts at the state level to enforce equivalent laws and pass new data protection rules. These actions and the harms they cause are discussed in **Section 3.1**.

State action in this context is expected given the relative laxity of federal action on privacy. However, acting first or with more force does not legitimatize policies that conflict in numerous ways with fundamental tenets of the digital ecosystem – *i.e.,* the borderless nature of the networks transporting data; the global routes traversed by consumers' data; consumer expectations for consistent protections regardless of where they use a service; and the long track record of success in applying national frameworks to digital services. **Section 3.2** examines the roles that NTIA should play in building momentum toward a national regulatory regime for consumer data privacy.

3.1 *The Problem: State-Level Privacy Actions Are Counterproductive to the Task of Bolstering Consumer Data Protections & Supporting Continued Innovation*

Over the last few years, there has been a spate of state data privacy and security actions. Legislatures in about half the states have considered sweeping privacy rules aimed at policing the data collection activities of ISPs and other service providers in the digital ecosystem.[41] Several others have adopted laws specifically targeting data brokers,[42] while

[41] *See, e.g.,* NCSL, Privacy Legislation Related to Internet Service Providers, Oct. 15, 2018, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers-2018.aspx; NCSL, State Laws Related to Internet Privacy, July 25, 2018, http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx. For additional information on the range of state legislative efforts vis-à-vis data privacy, *see* NCSL, Digital Privacy and Security: Overview of Resources, http://www.ncsl.org/research/telecommunications-and-information-technology/telecom-it-privacy-security.aspx.

[42] *See, e.g.,* AJ Dellinger, *Vermont Passes First-of-its-Kind Law to Regulate Data Brokers,* May 27, 2018, Gizmodo, https://gizmodo.com/vermont-passes-first-of-its-kind-law-to-regulate-data-b-1826359383.

most have passed legislation in response to data breaches and other privacy intrusions.[43] Taken together, the vast majority of states have acted in some manner to address consumer data privacy. Meanwhile, state Attorneys General from across the country have launched investigations and pursued enforcement actions against a range of firms accused of harmful or negligent actions in the collection and use of consumers' personal digital information.[44] State AGs have been increasingly vocal in their defense of state authority to engage in these actions.[45]

There are several reasons why states have increased their efforts in this context.

First, like the federal government, states have long played a role in monitoring the collection and use of personal information. Every state in the nation has Unfair and Deceptive Acts and Practices (UDAP) laws on the books.[46] These laws "ban[] deceptive commercial acts and practices and unfair trade acts and practices whose costs exceed their benefits."[47] Such "mini-FTC" laws have been used on numerous occasions by state AGs to "seek civil penalties, injunctive relief, and attorneys' fees and costs" in the privacy context.[48] State legislatures have enacted a range of other privacy-related laws over the years (*e.g.*, data breach notification rules; FCRA equivalents) that have been interpreted as providing a solid foundation for enforcement actions impacting firms operating in the digital ecosystem.[49]

Second, many state actors – legislators, AGs, etc. – have felt compelled to act in light of a rise in practices and outcomes that negatively impact consumers' privacy and data protections. This dynamic has been particularly evident in the aftermath of major data

---

[43] *See, e.g., Protections for Consumer Data Privacy,* Colorado House Bill 18-1128 (signed May 29, 2018), https://leg.colorado.gov/sites/default/files/documents/2018A/bills/2018a_1128_signed.pdf.

[44] *See, e.g.,* Jonathan Mayer, *Data Protection Federalism,* Aug. 15, 2018, The Century Foundation, https://tcf.org/content/report/data-protection-federalism/?agreed=1 (providing an overview of state interests in protecting consumer data privacy and highlighting the myriad of roles that state AGs have played and are playing in this context). *See also* Danielle K. Citron, *The Privacy Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747 (2016), https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=4693&context=ndlr (providing a similar analysis, as well as historical context for state AG efforts in this space) ("*Privacy Policymaking of State AGs*").

[45] *See, e.g.*, Mike Litt, *32 State Attorneys General to Congress: Don't Replace Our Stronger Privacy Laws!*, March 27, 2018, U.S. PIRG, https://uspirg.org/blogs/blog/usp/32-state-attorneys-general-congress-dont-replace-our-stronger-privacy-laws (reporting on a letter, signed by 32 state AGs, pushing back on Congressional efforts to preempt state-level data security actions).

[46] For an overview of these laws, *see Consumer Protection in the States: A 50-State Evaluation of Unfair and Deceptive Practices Laws*, National Consumer Law Center (March 2018), http://www.nclc.org/images/pdf/udap/udap-report.pdf.

[47] *Privacy Policymaking of State AGs* at p. 754.

[48] *Id.*

[49] *Id.*

breaches by firms like Equifax and Yahoo, which exposed sensitive personal information of hundreds of millions of Americans.[50] Recently, AGs from 37 states sought more information regarding Facebook's data policies vis-à-vis Cambridge Analytica.[51]

Third, some states also feel compelled to act in this context because of a perception that the federal government is unable or unwilling to police consumer data privacy harms. This has been the case in the aftermath of Congress's roll back of the FCC's privacy rules aimed at ISPs and the European Union's implementation of its expansive General Data Protection Regulation (GDPR), activities that some states interpreted as creating a gap in privacy protections that needed to be filled.[52] The sweeping data privacy law recently signed into law in California was animated by these forces.[53] That law, billed by some as an American GDPR,[54] has been flagged by a diverse array of stakeholders – from privacy advocates to consumer groups and digital firms – as potentially harmful to consumers because it undermines incentives essential to further investment, experimentation, and innovation.[55]

Some fear that, in the absence of federal action to implement a national privacy framework, more states will follow California's lead and adopt their own version of consumer data privacy rules, adding to an already complex and overlapping patchwork of state and federal data privacy rules and regulations.[56] This would be problematic for several reasons.

First and foremost, the digital ecosystem is borderless, which makes it all but impossible to identify the precise locus of harmful activity. A consumer in state A might have her data exposed as a result of a hack perpetrated against a company's headquarters based in state B, which warehouses its data in cloud servers situated in states C, D, and E. Such an "impossibility exception" is understood at the network level where, even though the physical infrastructure of broadband systems is proximate to users, the information flowing

---

[50] *See, e.g.,* Alison Frankel, *State AG's Equifax case may portend big problems for data breach defendants,* April 5, 2018, Reuters, https://www.reuters.com/article/us-otc-equifax/state-ags-equifax-case-may-portend-big-problems-for-data-breach-defendants-idUSKCN1HC2KY.

[51] *See* Ali Breland, *State AGs press Facebook over Cambridge Analytica scandal,* March 26, 2018, The Hill, https://thehill.com/policy/technology/380374-state-attorneys-general-press-facebook-in-letter.

[52] *See, e.g.,* Caitlin Chin, *The U.S. Privacy Landscape Post-GDPR,* Aug. 1, 2018, Georgetown Public Policy Review, http://gppreview.com/2018/08/01/the-u-s-privacy-landscape-post-gdpr/.

[53] *See, e.g.,* Rachel Kraus, *3 ways California is leading the country in digital rights,* July 2, 2018, Mashable, https://mashable.com/article/california-consumer-privacy-act/#SWluTX.F3Oqk.

[54] *See, e.g.,* George P. Slefo, *Marketers and Tech Companies Confront California's Version of GDPR,* June 29, 2018, AdAge, https://adage.com/article/digital/california-passed-version-gdpr/314079/.

[55] *See, e.g.,* Marc Vartabedian, Georgia Wells and Lara O'Reilly, *Business Blast California's New Data-Privacy Law,* July 1, 2018, Wall St. Journal, https://www.wsj.com/articles/businesses-blast-californias-new-data-privacy-law-1530442800.

[56] *See, e.g.,* Nuala O'Connor, *Reforming the U.S. Approach to Data Privacy and Protection,* Jan. 30, 2018, Council on Foreign Relations, https://www.cfr.org/report/reforming-us-approach-data-protection.

over them lacks readily identifiable state-based components, a dynamic that has long undergirded the national regulatory framework for internet access services.[57] Accordingly, courts have routinely found that state-level regulation of such services is invalid.[58]

Second and related, consumers rarely consider the impact of where they use a particular service on the scope of privacy and data security protections available to them. Put another way, it is unrealistic to expect consumers to determine which protections might apply to their uses of digital services depending on where they are at a given point in time. In a country with 50 different privacy laws, consumers who leave their home state would be overwhelmed with information regarding the subtle ways in which other states' privacy regimes differ.

Third, the compliance costs stemming from a Balkanized state-by-state data privacy regime would be staggering and would greatly overshadow any benefits that might arise. In response, firms would likely opt to conform to the most exacting set of rules, which would unduly burden consumers who reside in states with less rigorous rules. In addition, compliance costs would in all likelihood be passed onto consumers, raising prices and chilling the use of digital services.[59] Innovation would be harmed as well as firms would be less inclined to experiment with new business models or new offerings in such a burdensome atmosphere.[60]

3.2 *How NTIA Can Address the Problem*

To mitigate against the emergence of a state-by-state patchwork of consumer data privacy laws, NTIA should ensure that any proposals – legislative and otherwise – stemming from this proceeding prioritize the development and implementation of a single national regulatory framework for consumer data privacy. NTIA recognizes the importance of such a standard, noting in its RFC that the "emerging patchwork of competing and contradictory baseline [privacy] laws" ultimately "harms the American economy and fails to improve

---

[57] *See, e.g., Restoring Internet Freedom*, Declaratory Ruling, Report, and Order, 33 FCC Rcd. 311, ¶198 (2018).

[58] *See Minn. Pub. Utils. Comm'n v. FCC*, 483 F.3d 570 (8th Cir. 2007); *Charter Advanced Servs. (MN), LLC v. Lange*, 259 F. Supp. 3d 980, 985 (D. Minn. 2017), *aff'd Charter Advanced Servs. (MN), LLC v. Lange*, No. 17-2290, slip op. at 4 (8th Cir. Sept. 7, 2018).

[59] *See, e.g., Outlook for State Data Security Laws: More than Breach Notification,* Dec. 16, 2014, IAPP, https://iapp.org/news/a/outlook-for-state-data-security-laws-more-than-breach-notification/.

[60] *See, e.g.,* Tony Clark and Michael Santorelli, *Federalism in Wireless Regulation: A New Model for a New World,* ACLP Scholarship Series, New York Law School (Feb. 2009), http://www.nyls.edu/advanced-communications-law-and-policy-institute/wp-content/uploads/sites/169/2013/08/Clark-Santorelli-Wireless-Federalism-February-2009.pdf (discussing this general dynamic and observing its impact in the wireless space).

privacy outcomes for individuals, who may be unaware of what their privacy protections are, and who may not have equal protections, depending where the user lives."[61]

The viability of national regulatory frameworks for digital services is well established. Indeed, a national approach to mobile and broadband services has yielded enormous gains for consumers and the country as a whole. Clarification by Congress that wireless services were to be regulated primarily at the federal level significantly hastened the construction of nationwide networks in the 1990s.[62] Since then, carriers have continued to invest billions each year in their networks, delivering to consumers faster and more affordable access to mobile services. The U.S. mobile sector now contributes $475 billion to the country's GDP and supports 4.7 million jobs.[63] A similar dynamic is evident in the broadband sector, which, for many years, was subject to a light-touch national regulatory regime, one that reflected Congress's clear statement in the 1996 Telecommunications Act's that the internet is to be "unfettered by Federal or State regulation."[64] Since 1996, ISPs have invested in excess of $1.6 trillion in their networks.[65]

NTIA should also make clear that a national privacy framework and robust state partnership on these issues are not mutually exclusive. To that end, NTIA should identify the contours of meaningful state roles in the administration of new federal guidelines for consumer data privacy. State AGs should be empowered to assist in the enforcement of federal privacy rules. Such already occurs. For example, in certain circumstances, state AGs can bring "civil actions on behalf of state residents for violations of the HIPAA Privacy and Security Rules."[66] However, state action is limited to instances when federal authorities have yet to bring suit; state AGs cannot act if their federal counterpart has done so, assuring a streamlined approach to enforcement.[67] This could serve as a model for state enforcement in the privacy arena. At a minimum, NTIA should encourage and spearhead ongoing dialogues with state AGs and other state actors in an effort to ensure that all available

---

[61] *NTIA RFC* at p. 48,602.

[62] *See, e.g.,* Charles M. Davidson & Michael J. Santorelli, *Seizing the Mobile Moment: Spectrum Allocation Policy for the Wireless Broadband Century*, 19 CommLaw Conspectus 1 (2010), http://www.nyls.edu/advanced-communications-law-and-policy-institute/wp-content/uploads/sites/169/2013/08/Davidson-Santorelli-Seizing-the-Mobile-Moment-CommLaw-Conspectus-2010.pdf.

[63] *See How the Wireless Industry Powers the U.S. Economy,* Accenture (April 2018), https://api.ctia.org/wp-content/uploads/2018/04/Accenture-Strategy-Wireless-Industry-Powers-US-Economy-2018-POV.pdf.

[64] 47 U.S.C. § 230.

[65] *See* Patrick Brogan, *U.S. Broadband Investment Rebounded in 2017,* U.S. Telecom Research Brief (Oct. 18, 2018), https://www.ustelecom.org/sites/default/files/documents/USTelecom%20Research%20Brief%20Capex%202017.pdf.

[66] *See* U.S. Dept. of Health & Human Services, State Attorneys General, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/state-attorneys-general/index.html.

[67] *See* 42 U.S.C. §1320d-5(d)(7).

resources are appropriately and efficiently leveraged in the pursuit of a stronger, more consistent and predictable national privacy regime.

4. ADDITIONAL CORE PRINCIPLES OF A NATIONAL CONSUMER DATA PRIVACY FRAMEWORK

As part of its efforts to build momentum toward federal legislative action on consumer data privacy, NTIA should provide specific guidance to the Executive and Congress about core principles that must be included in any bill that emerges. Two critical tenets were discussed above: the need to harmonize the myriad of existing consumer data laws by, among other things, establishing a single national framework for privacy. This section identifies several additional elements that must be part of any federal action on consumer privacy.

4.1 *Establish Clear & Strong Consumer Rights in Their Data*

The *quid pro quo* of exchanging personal information for free online services has driven incredible growth and innovation across the digital ecosystem. However, a major shift occurred when entities assisting consumers in the navigation of this vast new universe of content – primarily search firms – realized that advertisers were willing to pay more for ads that were actually clicked on by customers. This in turn resulted in an arms race among firms trying to develop algorithms and other approaches that could place online ads that were relevant to users.[68] This necessitated the development of platforms that could attract users and goad them into sharing more information about themselves – directly (*e.g.*, by filling out a form or buying a product), indirectly (*e.g.*, by typing in search terms), and surreptitiously (*e.g.,* by tracking users with cookies). The success of this business model – *i.e.,* of monetizing consumer data – coupled with an increase in consumers' interest in using the web to enhance real-world relationships, facilitated the rise of social media, a space currently dominated by Facebook.

Google spearheaded this shift in Internet economics. While it was not the first firm to develop an effective algorithm for sorting search results or enter the online advertising business, it produced an incredibly effective integrated system for doing both.[69] Ever since, a growing number of companies throughout the ecosystem have eagerly sought to compete for a slice of the online advertising market, which has grown from an industry that generated $9.6 billion in revenues in 2004 (the year of Google's IPO) to one that neared $90

[68] *See, e.g.,* JOHN BATTELLE, THE SEARCH: HOW GOOGLE AND ITS RIVALS REWROTE THE RULES OF BUSINESS AND TRANSFORMED OUR CULTURE (2006) (providing a detailed overview of how this aspect of the online market evolved in the late 1990s and early 2000s).

[69] *Id. See also* Greg Lastowka, *Google's Law*, 73 Brook. L. Rev. 1327, 1335-1351 (2008) (discussing the development of these components of Google's business model).

billion in revenues in 2017.[70] The dominant format for digital ads is now mobile, revenue from which has grown at a compound annual rate of 71.4% since 2012.[71] Google and Facebook dominate this space, having acquired some 60% market share.[72] Search ads remain a popular format, but revenue growth in that segment has slowed a bit in recent years.[73] That said, it remains lucrative as it still comprises 44% of the overall digital ad market.[74] Google dominates the search market – "more than 90% of all [I]nternet searches are taking place through" Google and its subsidiaries like YouTube[75] – and extracts a tremendous amount of revenue from it.

These structural shifts in the economics underlying many Internet businesses have profoundly impacted personal privacy. In particular, they have created a self-reinforcing cycle of data generation and collection on the one hand and the provision and consumption of targeted services on the other. Consumers, although generally aware of the privacy risks implicated by this general dynamic and wary of certain types of intrusive practices, continue to consume these services and provide, knowingly or not, the increasingly granular data that is necessary to keep these firms afloat. The result is a race among content firms to create new ways for collecting ever-more detailed information and using that data to micro-target ads and other online offerings.

Action is needed to ensure that consumers are adequately protected from the kinds of intrusions that are becoming more and more frequent as a result of the perverse new incentives driving data collection and monetization. To that end, it will be necessary for Congress, with the input of NTIA and other stakeholders, to clearly identify the rights that consumers have in the various kinds of data they share when online and the acceptable means by which firms can collect that information.

There is an emerging consensus among stakeholders – including ISPs, content providers, consumers groups, and privacy advocates – that the ideal scope of privacy protections should correspond with the sensitivity of the data at issue and the context within which

---

[70] *See IAB Internet Advertising Revenues Report: 2017 Full Year Results,* at p. 2, Interactive Advertising Bureau (May 2018), https://www.iab.com/wp-content/uploads/2018/05/IAB-2017-Full-Year-Internet-Advertising-Revenue-Report.REV_.pdf ("*2017 IAB Report*").

[71] *Id.* at p. 9.

[72] *See* Rani Molla, *Google's and Facebook's share of the U.S. ad market could decline for the first time, thanks to Amazon and Snapchat*, March 18, 2018, Recode, https://www.recode.net/2018/3/19/17139184/google-facebooks-share-digital-advertising-ad-market-could-decline-amazon-snapchat.

[73] *2017 IAB Report*.

[74] *Id.*

[75] *See* Jeff Desjardins, *How Google Retains More than 90% of Market Share*, April 23, 2018, Business Insider, https://www.businessinsider.com/how-google-retains-more-than-90-of-market-share-2018-4.

that information is being collected.[76] This is a sensible approach. For example, digital health information shared with one's doctor is extremely sensitive and should be subject to strong protections so that it is not easily accessible or shareable except at the patient's direction. The same can be said for financial data like credit card information. Conversely, more prosaic information, like the fact that a person accesses a website at a certain time and views particular content, does not quite rise to the same level.

Sensitive data should be strongly protected and should only be collected from users if they give their affirmative consent (*e.g.,* via clear opt-in prompts). In other cases, consumers should have the ability to opt out of the kind of background collection of non-sensitive data that has long occurred online. In both cases, the consumer should have the ability to know what kind of information is being collected and how it is being used by the firm collecting it. There is considerable agreement on these parameters and should serve as a starting place for legislative efforts focused on defining what kinds of data falls into the sensitive and non-sensitive buckets.[77]

4.2 *Assure a Technology-Neutral Approach in the Application of Privacy Rules*

Without swift federal action, privacy will be weaponized and politicized by firms across the digital ecosystem seeking to wield the issue as a means of advancing their interests and undermining rivals. This has already happened. A few years ago, content firms and their surrogates convinced policymakers that it made sense to create a bifurcated privacy regime whereby ISPs are subject to exacting privacy rules enforced by the FCC, leaving all other digital firms to be subject to a much laxer standard enforced by a largely disinterested FTC.[78] Fortunately, Congress reversed this decision, but it has yet to take further steps to rationalize the fragmented set of rules for consumer data privacy that remains.

---

[76] *See, e.g.,* Kathy Grillo, *Privacy: It's time for Congress to do right by consumers,* Oct. 9, 2018, Verizon Policy blog, https://www.verizon.com/about/news/privacy-its-time-congress-do-right-consumers; Len Cali, *A Broad Consensus for Federal Privacy Legislation,* Sept. 28, 2018, AT&T Public Policy blog, https://www.attpublicpolicy.com/privacy/a-broad-consensus-for-federal-privacy-legislation/; U.S. Senate Commerce Committee, *Consumer Data Privacy: Examining Lessons from the EU'S GDPR and the California Consumer Privacy Act, Statement of Nuala O'Connor, President, CDT,* Oct. 10, 2018, Center for Democracy and Technology, https://cdt.org/files/2018/10/2018-10-09-FINAL-Nuala-OConnor-Written-Testimony-Senate-Commerce.pdf; *U.S. Chamber Privacy Principles,* Sept. 6, 2018, U.S. Chamber of Commerce, https://www.uschamber.com/sites/default/files/9.6.18_us_chamber_-_ctec_privacy_principles.pdf; *IA Privacy Principles for a Modern National Regulatory Framework,* Sept. 12, 2018, Internet Association, https://internetassociation.org/files/ia_privacy-principles-for-a-modern-national-regulatory-framework_full-doc/; U.S. Senate Commerce Committee, *Examining Safeguards for Consumer Data Privacy, Statement of Rachel Welch, SVP, Charter Communications,* Sept. 26, 2018, https://www.commerce.senate.gov/public/_cache/files/9cb79c7e-815c-4091-80d0-f425105b110b/2C25167C9296C00C1CBBEBD03171F49A.09-24-18welch-testimony.pdf.

[77] *Id.*

[78] *See, e.g., Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Comments of the ACLP, WC Docket No. 16-106 (May 27, 2016), http://www.nyls.edu/advanced-

The upside of these machinations is that it highlighted the real dangers – for consumers and for innovation – of maintaining separate privacy regimes for ISPs and everyone else. Creating different rules for different segments of the ecosystem would sow confusion among consumers. Having disparate privacy regimes will "confuse all but the savviest consumers" and ultimately "do little to promote the cause of "privacy.""[79] Innovation would also be harmed. Firms subject to more onerous privacy rules and enforcement would have fewer incentives to explore opportunities for generating new revenue streams stemming from digital advertising and related efforts.[80] In practice, this would starve the ecosystem of new business models and offerings that could serve as a competitive check on the dominant data collectors.

Ultimately, all firms in the digital ecosystem traffic in data: ISPs deliver data to consumers (they derive almost all of their revenue from voice, video, and data subscriptions); content producers create data for delivery to and consumption by consumers (these companies typically make money by placing ads based on these uses); and device manufacturers produce the hardware that consumers can use to access data (in many instances, these firms collect data, too). As such, it makes sense to have a single set of rules that applies to any firm engaged in the collection and monetization of consumer data.

Equally as important for consumers will be the zealous enforcement of these rules. In practice, enforcers need to be aware of where consumer harms are likeliest to occur and deploy resources accordingly. Harm (*e.g.*, a breach) is possible anywhere in the ecosystem, but intrusions and "creepy" behavior is more probable in those segments where data collection is the primary means of revenue generation. As previously noted, significant financial incentives drive digital firms like Google and Facebook to extract more and more data from users, including sensitive information. Conversely, ISPs play a very small role in data collection, due mostly to the fact that consumers' online activities increasingly span multiple devices and locations, making it is nearly impossible for a single ISP to glean as much information about a particular user's online behavior as, say, Google.[81] In addition, more and more data that flows over broadband networks is being encrypted, a dynamic that greatly limits the visibility an ISP might have into a customer's data.[82] Moreover, even

---

communications-law-and-policy-institute/wp-content/uploads/sites/169/2013/08/ACLP-Privacy-Comments-WC-Docket-No-16-106-052716.pdf.

[79] *See* Jon Leibowitz and Jonathan Nuechterlein, *The New Privacy Cop Patrolling the Internet*, May 10, 2016, Fortune, http://fortune.com/2016/05/10/fcc-internet-privacy/.

[80] *See FCC's Broadband Privacy Proposal Credit Negative for Linear TV and Wireless Providers,* March 14, 2016, Moody's Investor Service, http://www.netcompetition.org/wp-content/uploads/FCC%E2%80%99s-broadband-privacy-proposal-credit-negative-for-linear-TV-and-wireless-providers.pdf.

[81] *See* Peter Swire et al., *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less Than Access by Others*, The Institute for Information Security & Privacy at Georgia Tech (Feb. 2016), http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf.

[82] *Id.*

though some ISPs use customer data to develop and market ancillary services, the financial growth of these companies remains almost exclusively tied to subscription fees for Internet access, video and telephone service, not advertising revenue.

4.3 *Provide Adequate Guidance Regarding the Implementation and Enforcement of the National Consumer Data Privacy Framework*

A key part of meaningful federal action to protect consumers' data will be clear direction from Congress that FTC will be the primary cop on the privacy beat. To that end, it will be necessary for Congress to provide sufficient guidance to the Commission vis-à-vis how the rules are to be implemented and enforced. Striking the right balance will be critical. A law that is too specific will quickly become antiquated (as has been the case with the sectoral laws described above). On the other hand, legislation that is too imprecise will expose privacy to political gamesmanship, a dynamic that has been evident in other contexts (*e.g.,* net neutrality) due to substantial deference extended to agency interpretations of vague enabling statutes by federal courts.[83]

One way to ensure that the Commission hews closely to Congressional intent in the implementation and enforcement of privacy rules is to require cost-benefit analyses as part of any action the FTC might take in this context. Such analyses are typically undertaken by federal agencies as part of "major" rulemakings,[84] which include proceedings that are "likely to result in an annual effect on the economy of $100 million or more."[85] The FTC currently lacks the ability to engage in the kind of rulemaking that most other agencies engage in, but if it is granted authority to do so by federal legislators, then the law should require cost-benefit analyses as part of any action the Commission takes in this context.[86] Such a requirement will help to ensure that the FTC efficiently allocates resources in furtherance of its oversight and enforcement (see section 4.2 for a discussion of the benefits of focusing Commission attention on areas where harms are likeliest to occur).

---

[83] *See, e.g.,* Emily Hammond Meazell, *Super Deference, The Science Obsession, and Judicial Review as Translation of Agency Science*, 109 Mich. L. Rev. 733 (2011) (observing that courts are increasingly inclined to be more deferential to agency actions involving scientific or technical analyses); Kent Barnett & Christopher J. Walker, *Chevron in the Circuit Courts*, 116 Mich. L. Rev. 1 (2017), https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1667&context=mlr (tracking so-called *Chevron* deference extended to federal agencies by federal courts).

[84] *See, e.g., New Developments in Regulatory Cost-Benefit Analysis,* April 23, 2018, The Regulatory Review, https://www.theregreview.org/2018/04/23/new-developments-in-regulatory-benefit-cost-analysis/.

[85] *See Executive Order 12291 of Feb. 17, 1981*, https://www.archives.gov/federal-register/codification/executive-order/12291.html.

[86] *See, e.g.,* Adam Thierer, *A Framework for Benefit-Cost Analysis in Digital Privacy Debates,* 20 Geo. Mason L. Rev. 1055 (2013), https://www.mercatus.org/system/files/Benefit-Cost-Analysis-for-Online-Privacy---Adam-Thierer-[2013-George-Mason-Law-Rev].pdf.

Another way Congress can shape FTC efforts vis-à-vis the implementation of a new privacy framework is to carve out safe harbors for digital firms in the statute. Safe harbors provide a means for legislators to identify specific activities that do not violate a particular law. These provisions are relatively common in the tech space, providing innovators with certainty regarding the extent to which a particular service or business model might be subject to or immune from legal action.[87] Privacy safe harbors could encompass a set of practices – *e.g.,* data collection techniques; transparency measures; opt-in and opt-out for certain kinds of sensitive and non-sensitive information; breach notifications – that would be presumptively in line with Congress's expectations for consumer empowerment and protection in the digital ecosystem. Including such carve-outs would greatly streamline FTC oversight and enforcement, allowing it to focus on areas where harm is probable.

5. CONCLUSION

The output of this docket is critically important to building momentum in support of long overdue federal action to protect consumers in the rapidly evolving digital ecosystem. Without comprehensive action, firms will deploy ever more invasive data extraction techniques, greatly increasing the odds of more regular privacy intrusions. Consumer welfare and innovation are significantly worse off in such an environment. For these reasons, NTIA must urge the Executive to push for a legislative solution that formalizes a national regulatory framework, one that can deliver the certainty and predictability needed to protect consumer privacy while also assuring continued investment and business model experimentation.

The ACLP looks forward to serving as a resource to the NTIA as it develops the Administration's approach to these critical issues. Should you have any questions, please do not hesitate to contact us.

Respectfully submitted,

/s/ Charles M. Davidson
CHARLES M. DAVIDSON, DIRECTOR

/s/ Michael J. Santorelli
MICHAEL J. SANTORELLI, DIRECTOR

[87] *See, e.g.,* 17 U.S.C. § 512 (aka the Digital Millennium Copyright Act safe harbors); Martin A. Weiss and Kristin Archick, *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield,* Congressional Research Service, CRS R44257 (May 19, 2016), https://fas.org/sgp/crs/misc/R44257.pdf.