ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Testimony of

Doug Brake

Telecommunications Policy Analyst

Information Technology and Innovation Foundation

Before the

House Committee on Energy and Commerce

Subcommittee on Communications and Technology

Hearing on

"FCC Overreach: Examining the Proposed Privacy Rules"

June 14, 2016

2123 Rayburn House Office Building

Washington, DC

Chairman Walden, Ranking Member Eshoo, and members of the Subcommittee, thank you for inviting me to share the views of the Information Technology and Innovation Foundation (ITIF) on the ongoing proceeding at the Federal Communications Commission (FCC) to regulate broadband privacy.

ITIF is a nonpartisan think tank whose mission is to formulate and promote public policies to advance technological innovation and productivity growth. The FCC's proposed privacy regime does a remarkably poor job of balancing those goals—innovation and productivity—with other policy interests. For this reason, and others explored below, ITIF has opposed the entire FCC privacy undertaking.[1]

There certainly is a role for government in protecting consumer privacy, but the oversight and enforcement provided by the Federal Trade Commission (FTC), along with existing industry practices and commitments, provide a superior framework for balancing privacy, consumer protection, and innovation. There is still time for Congress to direct the FCC to correct course.

BROADBAND PROVIDER ACCESS TO DATA DOES NOT JUSTIFY SECTOR-SPECIFIC REGULATORY SILOS

The FCC proposes strict data privacy regulations that will apply only to broadband Internet access providers.[2] In order to justify the FCC's sector-specific rules, one would expect an unusually high risk of consumer harm from consumer broadband data being shared inappropriately. After all, the only sector-specific privacy rules are for areas of the economy, such as healthcare or financial services, where there exists a heightened risk of harm from the disclosure of sensitive personal information. But, as a factual matter, that heightened risk does not exist with regard to broadband providers: their access to data is neither unique nor comprehensive.

In his report, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, Professor Peter Swire lays out a number of ways in which broadband providers generally have less visibility into users' online activity compared to other actors in the Internet ecosystem.[3] Broadband providers do not have anything near comprehensive access to consumer data for several reasons. One of the most prominent limitations on broadband providers' access to data is the growing use of encryption. When subscribers use encrypted protocols with their browsers, the broadband provider is unable to determine the content or information about the webpages that the user visits. And encryption adoption is on a sharp, recent rise: In 2014 a small percentage of traffic was encrypted, but by the end of 2016, it is estimated that 70

---

[1] *See* Doug Brake, Daniel Castro, & Alan McQuinn, ITIF, "Broadband Privacy: The Folly of Sector-Specific Regulation" (2016), http://www2.itif.org/2016-broadband-privacy-folly.pdf; Doug Brake, Daniel Castro, & Robert D. Atkinson, ITIF, "The FCC's Privacy Foray: Privacy Regulation Under Title II" (2015), http://www2.itif.org/2015-fcc-privacy.pdf; Doug Brake, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Comments of ITIF," WC Docket No. 16-106, *available at* http://www2.itif.org/2016-broadband-privacy-comments.pdf?_ga=1.25209844.812486504.1449157248; Doug Brake, "The FCC's Privacy Ruse," *Forbes* (April, 2016), http://www.forbes.com/sites/realspin/2016/04/27/the-fccs-privacy-ruse/#1c47825b10aa.

[2] The FCC's proposed rules apply only to Broadband Internet Access Services, or "BIAS" as defined at 47 CFR § 8.2(a).

[3] 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, Georgia Tech, Feb 2016, http://peterswire.net/wp-content/uploads/Online-Privacy-and-ISPs.pdf.

percent of traffic will be encrypted.[4] All of the top 10 websites now encrypt their traffic by default or on user log-in, and 42 of the top 50 do so as well.[5]

Broadband providers can still access high-level metadata even when consumer traffic is encrypted. For example, a broadband provider might be able to determine from metadata that a particular household is streaming video, but have no idea as to the actual content of the video. However, since encryption obscures most content, and virtually all sensitive content, the case for heightened rules applied only to broadband providers is extremely tenuous. The fact that consumers spread their Internet use over multiple broadband connections at home, work, and at various WiFi hotspots further reduces the risk of harm from any one provider's collection of information.

Privacy-sensitive consumers have additional options to protect their data if they choose. They can use virtual private networks (VPNs) to encrypt the Internet traffic a broadband provider would otherwise see. If a broadband subscriber is using a VPN, the broadband provider can see only that the subscriber accessed that VPN, not information about the user's end destination. If consumers want to use VPNs to obfuscate their online habits from their provider, they certainly can take that option.

Engineers have pointed out there is a significant gap between what information is technically available to Internet Service Providers (ISPs) and what is practically useful. Richard Bennett, a consultant with a thirty-year background in network engineering, points out that because of the numerous, diverse connections opened when a typical web page loads, "all the ISP can do with the all that information is guess what the important parts are…. As a practical matter, converting the raw information that ISPs can harvest from web requests made by users who aren't using VPNs is a very difficult task."[6]

Even given all that, provider access to data is simply not unique. As Jules Polonetsky, head of the Future of Privacy Forum, has put it, "[t]oday, data has been democratized"—large amounts of consumer data are already available to anyone with a credit card.[7] The ability to obtain data like that which broadband providers have access to is widely available and in no way unique to broadband providers. The proposed rules would lead to the strange and market-distorting result where broadband providers would not be allowed to share or use the exact same information that is readily available to others.

Moreover, as ITIF has demonstrated, all major broadband providers already offer consumers the ability to opt-out of existing targeted advertising programs, an important and often-overlooked point.[8] In line with the FTC's guidance, broadband providers all offer notice of the data that is collected and the option for

---

[4] *Id* at 29, *citing* "2016 Global Internet Phenomena, Spotlight: Encrypted Internet Traffic," Sandvine, Feb. 2016.
[5] *Id* at 28.
[6] Richard Bennett, "FCC Confused About Privacy," *HighTech Forum*, http://hightechforum.org/fcc-confused-about-privacy/.
[7] Jules Polonetsky, "Broadband Privacy and the FCC: Protect Consumers from Being Deceived and from Unfair Practices," *Future of Privacy Forum* (March 2016), https://fpf.org/2016/03/11/13938/.
[8] *See* Doug Brake, Daniel Castro, & Alan McQuinn, Information Technology and Innovation Foundation, Broadband Privacy: The Folly of Sector-Specific Regulation, (2016), http://www2.itif.org/2016-broadband-privacy-folly.pdf.

consumers to opt out of practices they are uncomfortable with. The truth is users will have no more and no less "control" over how companies use their broadband data under the proposed rules, as the FCC has asserted. What will change, however, is the ability of ISPs to responsibly experiment with new ways of supporting the expensive deployment and maintenance of broadband networks.

In addition, persistent confusion stems from the popular, but mistaken, belief that because broadband providers operate the network connecting users to the rest of the Internet—the actual location of broadband providers as in the middle between users and the online services they access—these providers have a special relationship with consumers' online activities. But this "gatekeeper" model is the wrong way to think about broadband providers' relationship to consumer data. As the FTC explained in its 2012 Privacy Guidelines, although ISPs serve as intermediaries, giving consumers access to other services, "[a]t the same time, the Commission agrees that any privacy framework should be technology neutral. ISPs are just one type of large platform provider" that have access to consumer data.[9]

Instead, of recognizing this fact, and treating broadband providers with the same light-touch approach that has seen such success with respect to other large platform providers, the FCC proposes a three-tier consent scheme. This framework consists of (1) implied consent for data used in actually providing broadband service, (2) opt-out consent for marketing "communications-related" services, and (3) opt-in consent required for any other uses of data. The entire regulatory scheme is explicitly structured around what business practices broadband providers can and cannot participate in. As such, this proceeding is less about enabling consumers to make choices about how their information is used by broadband providers—again, those choices already exist. Instead, it is more an ongoing effort to continually narrow broadband providers' businesses down to one of pure transport. It cuts off the possibility of targeted advertising-based models that would provide a revenue stream other than subscribers' monthly bills to support deployment of next-generation networks or consumer broadband discounts. Discounts offered in exchanged for access to browsing data would be especially helpful to price sensitive consumers, who may well not value their privacy as highly as some of the privacy advocates pressuring the FCC.

In essence, the FCC is making the wrong up-front choice for consumers by mandating an opt-in process that will reduce consumer welfare, productivity, and innovation. Most people are happy to make trade-offs around privacy and other values, such as convenience or price, but requiring them to go out of their way and take the extra step of opting in would sharply reduce participation rates. For the small share of consumers who truly worry about broadband information practices, they have strong motivations to opt out, and are already able to do so under current practice. But the FCC proposal would effectively shut off innovative practices that would benefit the majority of broadband consumers who would otherwise likely be willing to participate.
It is a widely agreed-upon point that privacy rules in particular, and rules governing technology-enabled practices and business models generally, should be technology-neutral and evenly applicable across different

[9] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," at 56 (March 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

entities.[10] Instead, the FCC is looking to build new regulatory silos based on what business practices it thinks broadband providers should and should not be engaged in.

FTC ENFORCEMENT AND EXISTING CONSUMER CHOICE BETTER BALANCES PRIVACY AND INNOVATION

The tremendous value of innovation stemming from new sources of data has been well recognized by a number of respected institutions. The President's Council of Advisors on Science and Technology, for example, outlined a number of benefits in its recent report on privacy and big data, ultimately stating their strong belief that "the positive benefits of big-data technology are (or can be) greater than any new harms."[11] As noted by the White House, "properly implemented, big data will become an historic driver of progress."[12] And as the White House noted more recently, "big data provides opportunities for innovations that reduce discrimination and promote fairness and opportunity, including expanding access to credit in low-income communities, removing subconscious human bias from hiring decisions and classrooms, and providing extra resources to at-risk students."[13]

The FCC, however, focuses exclusively on hypothetical harms from information sharing and use by broadband providers, and fails to adequately recognize the significant upside to an additional source of data that can be put to innovative use. By helping individuals and organizations make better decisions, data has the potential to spur economic growth and improve quality of life in a broad array of fields—the FCC appears to under-appreciate this fact.

Any new regulations should recognize there is a balance between the benefits additional sharing and use of data and the risk of privacy harms.[14] The research of Catherine Tucker at MIT has shown the light-touch privacy regime in the United States is a significant factor in why this country leads in the Internet economy compared regions under more restrictive privacy regimes, such as the European Union.[15] There is a significant

---

[10] Indeed, this was a motivating concern behind the Administration's proposed Consumer Privacy Bill of Rights. In supporting that proposed legislation, the White House explained that "[i]t is important that a baseline statute provide a level playing field for companies, a consistent set of expectations for consumers…." The White House, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," at 36 (February 2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[11] President's Council of Advisors on Science and Technology, "Big Data and Privacy: A Technological Perspective" (May 2014), at 14, https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf

[12] Executive Office of the President, "Big Data: Seizing Opportunities, Preserving Values" (May 2014), https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

[13] Executive Office of the President, "Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights" (May 2016), https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

[14] On this balance, *see* Avi Goldfarb & Catherine Tucker, "Privacy and Innovation," in *Innovation Policy and the Economy, Volume 12* U. of Chicago Press (2012), 65-89.

[15] Catherine Tucker, "Empirical Research on the Economic Effects of Privacy Regulation," 10 *J. on Telecomm. & High Tech. L* 265 (2012) *available at* http://jthtl.org/content/articles/V10I2/JTHTLv10i2_Tucker.PDF

risk that privacy advocates will seek to use the FCC's more restrictive model to ratchet up rules across the rest of the Internet ecosystem in a way that would do significant harm to the online economy.

We should prefer the FTC model as simply superior in supporting data innovation compared to that proposed by the FCC. The FTC oversees fair competition and has broad authority under Section 5 of the Fair Trade Act to take enforcement actions against unfair or deceptive trade practices.[16] The FTC also offers specific guidance when it comes to privacy, having put forth a single, comprehensive framework guided by three overarching principles: privacy by design, consumer choice, and transparency.[17]

By allowing flexibility for industry to develop best practices within these guidelines, and stepping in ex post where problems develop, the FTC does not have to predict the direction technological advancements or changes in business practices will take us. This allows firms to internalize or outsource different functions in fast-paced industries with a focus on efficiency rather than compliance. This type of privacy oversight, with rules that apply an even, light-touch approach to different actors, would be a better environment for dynamic competition to occur across platforms. A uniform oversight framework, with low regulatory barriers to entry, would not only allow carriers to explore further entry into areas like advertising, but would avoid discouraging new entrants from providing broadband services.

The FCC proposal deviates from the well-tested FTC enforcement model in several significant ways, most egregiously in structuring its opt-in choice architecture around the services broadband providers seek to engage in, instead of consumers' expectations of privacy or risk of harm. It also imposes significant burdens around ensuring data not be re-identifiable, and data security requirements.

Both current FTC staff and the former FTC Chairman, Jon Leibowitz filed comments outlining the ways in which the proposal deviated from the FTC approach. As Leibowitz put it, "in many important areas [the FCC's proposal] overshoots the mark, proposing regulations for broadband providers that go well beyond those imposed upon the rest of the Internet economy and which, if adopted, would undercut benefits to the very consumers it seeks to protect."[18] Current FTC staff commented as well, writing that aspects of the proposed rules "[do] not reflect the different expectations and concerns that consumers have for sensitive and non-sensitive data. As a result, it could hamper beneficial uses of data that consumers may prefer...."[19] Former

---

[16] 15 USC § 45.

[17] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," March 2012, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[18] Jon Leibowitz, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Comments of Jon Leibowitz," at 2, WC Docket No. 16-106, *available at* http://apps.fcc.gov/ecfs/document/view?id=60002014604.

[19] Staff of the Bureau of Consumer Protection of the Federal Trade Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Comments of FTC Staff," at 22, WC Docket No. 16-106, *available at* https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf.

FTC Commissioner Josh Wright specifically called out the negative impact on innovation, characterizing the proposal as one that "fails to consider the economic costs affecting consumers, ISPs, and innovation."[20]

A uniform set of light-touch privacy oversight tracking the FTC approach would preserve the flexibility needed for innovation and incentives for cross-platform competition.

PRIVACY POLICIES SHOULD BE ADDRESSED AT A CONGRESSIONAL LEVEL, IF AT ALL, NOT THROUGH NOVEL FCC STATUTORY INTERPRETATION

Privacy policies, especially those proposed by the FCC, impact a substantial portion of the Internet economy, and should be developed at a national level through Congress. Instead, the FCC is improvising, twisting a statute that was clearly developed for a different time. The FCC took this step backwards in time when forced to classify broadband providers as Title II common carriers in order to impose its ill-advised net neutrality rules. Many of the problems with this rulemaking, and common carrier classification generally, stem from the FCC attempting to fit a square broadband peg into a round Title II hole. The political and popular support for open Internet rules provided cover for the FCC to attempt to usurp jurisdiction over broadband privacy from the FTC, who had successfully overseen the privacy practices of broadband provider prior.

In its proposal, the FCC overwhelmingly relies on Section 222, within Title II of the Communications Act. Section 222 was written as a tool to prevent anti-competitive use of telephone records by rival phone companies as a part of the 1996 Telecommunications Act's introduction of competition into the local telephone market. This was a time when only one type of company—telephone providers—had unique, and uniquely valuable, data about customers. The FCC now intends to repurpose this statute into a broad mandate to police virtually all aspects of broadband providers' collection and use of customer data—even broader than it had interpreted the statute when regulating telephone records—in an economic system that is far more complex and dynamic.

This proceeding, and privacy generally, is an area of significant national concern, and policy here should be set through an open and democratic legislative process in Congress, not creative statutory re-interpretation by an independent agency. Congress is better suited to ascertain the implications of broadband privacy regulations on areas outside the FCC's jurisdiction and balance the numerous policy goals implicated by this proceeding.

CONCLUSION

Some of the policy goals animating the FCC's proposal are legitimate, but simply given undue weight. There is certainly an interest in ensuring customers have transparent notice and choice over how their information is used and collected when navigating the Internet ecosystem, but, consumers already have this choice and the FTC framework better balances competition, innovation, and consumer protection.

---

[20] Joshua D. Wright, "An Economic Analysis of the FCC's Proposed Regulation of Broadband Privacy" (May 2016), *available at* http://apps.fcc.gov/ecfs/document/view?id=60002077298.

Given the advent of tools for users to protect their privacy and the fact ISPs provide consumers with meaningful control over the use of their data, there is no specific consumer harm occurring that the FCC needs to correct, and no justification for specific, heightened rules peculiar to the FCC's jurisdiction. Congress should direct the FCC to correct course, and adopt rules in line with the existing FTC framework.

Thank you again for this opportunity to appear before you today.