

Before the  
**FEDERAL COMMUNICATIONS COMMISSION**  
Washington, DC 20554

In the Matter of )  
)  
Protecting the Privacy of Customers of Broadband ) WC Docket No. 16-106  
and Other Telecommunications Services )  
)

**Comments of ITIF**

The Information Technology and Innovation Foundation (ITIF)<sup>1</sup> appreciates this opportunity to comment on a challenging and important undertaking by the Federal Communications Commission’s (FCC or the Commission): the proposed creation of sector-specific privacy rules affecting virtually all aspects of broadband Internet access service (BIAS) providers’ collection and use of customer information.<sup>2</sup>

**INTRODUCTION AND SUMMARY**

Because this proceeding rests on a number of faulty assumptions about existing limitations on BIAS providers’ ability and incentives to collect information, the nature and direction of competition in BIAS and related markets, consumers’ willingness to make tradeoffs around privacy and other values, existing privacy safeguards, and the potential implications for international privacy discussions, this proceeding is fraught with unintended consequences.<sup>3</sup> However, the intended consequences are problematic as well, as the proposal seems less like a well-designed attempt to empower consumers to protect their privacy and more like a concerted effort to fence-in BIAS providers’ business practices.

---

<sup>1</sup> Founded in 2006, The Information Technology and Innovation Foundation, or ITIF, is a 501(c)(3) nonprofit, nonpartisan research and educational institute—a think tank—focusing on a host of critical issues at the intersection of technological innovation and public policy. Its mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

<sup>2</sup> *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, WC Docket No. 16-106, 31 FCC Rcd 2500 (2016) (*Privacy NPRM*).

<sup>3</sup> 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>.

The Federal Trade Commission (FTC) offers a categorically superior model for overseeing privacy. A uniform application of light-touch privacy oversight under the FTC’s deep experience with enforcement of unfair or deceptive trade practices would preserve an open field for competition and innovation. For all of these reasons, the Commission should abandon this proceeding and leave broadband privacy to the FTC.

If the Commission unwisely follows through on its proposal, it should take steps to ensure any regulations balance privacy protections with the beneficial uses of data and a uniform application of rules. The Commission should make its rules narrow, clear, and as consistent with the established FTC framework as possible.

## CONTENTS

Introduction and Summary.....	1
The Commission Should Not Regulate Broadband Privacy .....	3
The Proposal Rests on a Number of Faulty Premises .....	3
BIAS Access to Information Does Not Justify Sector-Specific Regulation .....	3
The Commission Ignores Existing Protections Offered by BIAS Providers.....	5
The Commission Mistakenly Assumes Future Competitive Dynamics.....	6
The Commission Under-appreciates the Benefits of Information Sharing and Use.....	8
The FTC Approach Better Promotes Innovation .....	10
The FTC Approach Likely Better Protects Privacy .....	11
The Section 706 “Virtuous Cycle” Supports Light-Touch Oversight.....	12
The Proposal is Inconsistent with U.S. Approach to Privacy Abroad .....	15
The Commission Can Lawfully Leave Privacy to the FTC .....	15
If The Commission Must Regulate, It Should Do So in a Way that Promotes Innovation .....	16
If the Commission Believes It Must Regulate, It Should Adopt an Approach Consistent with the FTC.....	16
An Opt-In Regime Stifles Innovation.....	17
De-identification Techniques Can Sufficiently Protect Privacy .....	18
The Commission Should Clarify, Narrow the Scope of its Jurisdiction.....	19
Conclusion .....	20

## THE COMMISSION SHOULD NOT REGULATE BROADBAND PRIVACY

The Commission's proposal does not present adequate justification for deviating from the successful FTC oversight of broadband privacy.

### The Proposal Rests on a Number of Faulty Premises

The Commission's proposal rests on a number of faulty assumptions to support some of the most extensive privacy regulations to date. First, BIAS provider's access to customer information does not rise to the level justifying sector-specific regulation. Second, the Commission assumes a particular industry structure and lines of competition.

#### BIAS Access to Information Does Not Justify Sector-Specific Regulation

As a threshold matter, the FCC should show unique risk of harm in the use of customer information by BIAS providers that justifies the greatly enhanced levels of protection proposed by the NPRM. The FCC has not and cannot show this risk because it does not exist. In addition to the rise of encryption and tools privacy-sensitive customers have at their disposal, every major BIAS provider already offers customers the ability to opt-out of practices they feel are intrusive.

Peter Swire in his report, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, lays out a number of ways in which BIAS providers generally have less visibility into users' online activity compared to other actors in the Internet ecosystem.<sup>4</sup> The report corrects a number of common factual misperceptions: There is a popular, but mistaken, belief that because BIAS providers operate the network connecting users to the rest of the Internet, these providers have a uniquely comprehensive view into consumers' online activities. While the paper itself does not make specific policy recommendations, the clear conclusion is that BIAS providers do not have anything near comprehensive access to consumer data. Especially after considering his examination of BIAS access compared to other Internet firms and advertisers, an eminently reasonable conclusion is that the risk of harm from BIAS use of data is no greater than others that continue operating under FTC oversight and does not justify a heightened level of regulation.

One of the most prominent ways in which BIAS providers are limited in their access to consumer data is the growing use of encryption. When subscribers use encrypted protocols with their browsers, such as the Secure Sockets Layer (SSL) or Hypertext Transfer Protocol Secure (HTTPS), the broadband provider is unable to access the content or information about the detailed links that the user visits. The only information the ISP is

---

<sup>4</sup> 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>.

able to see is a limited set of metadata—data that describes information about the connection (e.g., the name of the website domain and the total volume of data transferred). As the cost of encrypting data has fallen, more websites have started to encrypt all traffic so that a third party cannot intercept exchanged information. As of April 2015, 29 percent of all Internet traffic in North America was encrypted, and that number is steadily rising.<sup>5</sup>

The rate of adoption has been augmented by prominent players in the web ecosystem supporting encryption. In 2014, Google started giving secure websites a small benefit in its search ranking algorithm and it has suggested it will weight this factor more in the future.<sup>6</sup> Similarly, the “Let’s Encrypt” program is a free, automated encryption service designed to encourage more websites to adopt secure Internet protocols.<sup>7</sup> The on-demand media provider Netflix—which by April 2015 accounted for 35.7 percent of all bandwidth consumed by North American web users daily—has also promised to adopt HTTPS.<sup>8</sup> The Electronic Frontier Foundation has long worked to expand encryption online with its “HTTPS Everywhere” project.<sup>9</sup> All Wikimedia sites, including Wikipedia, use encryption by default.<sup>10</sup> A number of news websites, with third-party advertising dependencies that historically made encryption more difficult, have recently announced they will encrypt by default.<sup>11</sup> Virtually all websites that hold sensitive user data enable encryption by default or on user login.

The trend is clear and strong in the direction of a reduction in BIAS access to consumer data. This is not to say encryption resolves all privacy questions. There are still plenty of websites that do not encrypt their traffic and metadata can still be revealing; there is still a need for oversight. But the question is not should BIAS providers have a total free-for-all with consumers’ data. Instead the question is between now-mature industry

---

<sup>5</sup> “Global Internet Phenomena Spotlight Encrypted Internet Traffic,” *Sandvine*, April 8, 2015,

<https://www.sandvine.com/downloads/general/global-internet-phenomena/2015/encrypted-internet-traffic.pdf>.

<sup>6</sup> “HTTPS as a ranking signal,” *Google*, August 6, 2014, [https://googleonlinesecurity.blogspot.com/2014/08/https-as-ranking-signal\\_6.html](https://googleonlinesecurity.blogspot.com/2014/08/https-as-ranking-signal_6.html).

<sup>7</sup> “About” *Let’s Encrypt*, February 12, 2016, <https://letsencrypt.org/about/>.

<sup>8</sup> “Global Internet Phenomena Spotlight Encrypted Internet Traffic,” *Sandvine*; Chris Welch, “Netflix will make browsing movies more secure within the next year,” *The Verge*, April 15, 2015, <http://www.theverge.com/2015/4/15/8422889/netflix-https-coming-within-one-year>.

<sup>9</sup> “HTTPS Everywhere,” *Electronic Frontier Foundation*, accessed May 2016, <https://www.eff.org/HTTPS-everywhere>.

<sup>10</sup> Yana Welinder et al., “Securing access to Wikimedia sites with HTTPS,” *Wikimedia Foundation*, June 2015, <https://blog.wikimedia.org/2015/06/12/securing-wikimedia-sites-with-https/>.

<sup>11</sup> See, for example, Jason Reich et al. “Buzzfeed And HTTPS” (May 2016), <https://www.buzzfeed.com/jasonreich/buzzfeed-and-https>.

best practices combined with the FTC's ex post oversight, on one hand, and on the other the FCC's expansive and restrictive regulatory scheme as proposed.

Beyond encryption, privacy-sensitive consumers have additional options to obfuscate their data from BIAS collection. They can use Virtual Private Networks (VPNs) to encrypt the Internet traffic a BIAS provider would otherwise see. If a broadband subscriber is using a VPN, the ISP can see only that the subscriber accessed that VPN, not traffic information. If consumers feel there is value in using VPNs to obfuscate their online habits from ISPs, they certainly can take that option. As of the second quarter of 2015, there were 45 million users running ad blocking software in the United States.<sup>12</sup> The fact that there is not a similar movement for adopting VPNs suggests that subscribers are not as concerned about the privacy of their data as some suggest.

To be sure, broadband providers could, and should, use their subscribers' information to create personalized services. Even considering the growing use of encryption, where users forego a VPN, broadband providers will be able to identify certain characteristics of their users based on metadata and other online tracking technologies, just as other actors in the Internet ecosystem can. However, this data is far less complete than advocates describe. Many do not take into account that many consumers subscribe to multiple ISPs for service. As of July 2015, 55 percent of U.S. adults report having both a smartphone and a home broadband subscription.<sup>13</sup> These adults may also connect periodically to the over 9 million Wi-Fi hotspots spread throughout the United States, and also spread their use over both work and come connections.<sup>14</sup> Furthermore, many households have multiple devices and ISPs do not always have the ability to link across devices. Therefore, each individual broadband provider sees only a portion of a user's online activity. And most of these customers use the same browser, search engines, social media platforms, and e-commerce sites across devices and service providers.

### The Commission Ignores Existing Protections Offered by BIAS Providers

Furthermore, all major BIAS providers already offer consumer's the ability to opt-out of existing targeted advertising programs.<sup>15</sup> In line with the FTC's guidance, broadband providers all offer notice of the data that is collected and the option for consumers to opt out of practices they feel are intrusive. The truth is users will

---

<sup>12</sup> "The 2015 Ad Blocking Report," *PageFair*, 2015, <https://blog.pagefair.com/2015/ad-blocking-report/>.

<sup>13</sup> John Horrigan and Maeve Duggan, "Home broadband adoption: Modest decline from 2013 to 2015," *Pew Research Center*, December 21, 2015, <http://www.pewinternet.org/2015/12/21/1-home-broadband-adoption-modest-decline-from-2013-to-2015/>.

<sup>14</sup> Wi-Fi Growth Map, iPass, <http://www.ipass.com/wifi-growth-map/>.

<sup>15</sup> 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>.

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 essence, the FCC is making the choice for consumers by mandating a largely opt-in regime, a regime that will reduce, not enhance consumer welfare, productivity, and innovation.

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 in the broadband marketplace that the FCC needs to correct. Broadband providers already give users privacy controls by offering the explicit ability to opt out of data use.

### The Commission Mistakenly Assumes Future Competitive Dynamics

A fundamental error of this undertaking is the assumption about business models and the nature of competition in and across a number of platforms touched by the proposed regulations. There are a number of competitive dynamics that undermine any justification for sector-specific privacy rules. More troubling than the FCC overlooking these issues is the possibility that the proposed rules stem from a desire to lock BIAS providers out of data-driven business model innovation, consigning them to mere transport providers. Many of the problems with this rulemaking, and common carrier classification generally, stem from the Commission attempting to fit a square broadband peg into a round Title II hole.

The FCC proposes a three tier consent scheme consisting of implied consent for use of data in providing BIAS services, opt-out consent for marketing communications-related services, and opt-in consent for any other uses of data. This entire regulatory scheme is explicitly structured around the FCC controlling what business BIAS providers can be in. Granted, this is how common carriage worked in the 19<sup>th</sup> and 20<sup>th</sup> century, but if the FCC is honest about wanting a “Title II for the 21<sup>st</sup> century,” this proposal is deeply misguided.

The fact of the matter is broadband providers exist within a broader system of modular platforms competing along different fronts. The FCC tries to single out BIAS providers for special regulation without regard for how that could negatively impact dynamic competition across platforms.

A number of technology trends, particularly shifts toward software defined networking (SDN) in carrier networks and greater virtualization of network functionalities, are driving dramatic change throughout operators and vendors alike. Not only do these technologies make spinning up a network much cheaper and more flexible, but they will likely change traditional lines of competition and cooperation the Commission is assuming are static.

These advances in networking fit within a number of other technological developments that many think will see a growing diversity in network ownership and operation. Wireless analyst Dean Bubley, for example, points to a number of factors in addition to SDN, including the diversity of Internet of Things (IoT)

verticals, WiFi normalizing privatization of wireless connectivity, cheaper infrastructure, skilled network engineers employed by non-telecom companies, chip manufactures growing flexibility in connection modes, loss of ability to cross subsidize data connectivity with traditional telecom services such as voice or text, among others, that lead him to predict more “heterogeneity in network ownership.”<sup>16</sup> As he puts it, the “growing virtualization of technology will mean the number of ‘layers’ at which 3rd-parties can enter the market will grow.”<sup>17</sup>

A joint report from Arthur Little and Bell Labs explored the “double-edge sword” nature of cloud networking, explaining that there is real opportunity for carriers to build value through these shifts in technology, but it “could also result in a significant outflow of value across both consumer and business market segments, in favor of new competitors. Powerful new players could seek (and have the muscle) to drive a wedge between carriers and their customers in the long term,” pointing to high-value verticals, over-the-top providers, and web-scale companies.<sup>18</sup>

Even more intriguing are the ways in which edge providers could use their deep experience with advanced networking to support new broadband infrastructure deployment. This is not a wild hypothetical: Google Fiber is a clear example.<sup>19</sup> Facebook as well has been very active in the SDN space, and a major driver consolidating open-source hardware solutions under the Open Compute Project, which it has to expanded from the data center to carrier networks through the Telecom Infrastructure Project.<sup>20</sup> Last month, Facebook unveiled Terragraph and Project ARIES, a multiple input, multiple output (MIMO) wireless access system running on high-band unlicensed spectrum, that the company describes as “one of the lowest cost solutions to achieve 100 percent street-level coverage of gigabit Wi-Fi.”<sup>21</sup> Earlier this month, Facebook unveiled a

---

<sup>16</sup> Dean Bublely, “Telecoms is too important to leave to the telcos,” *Disruptive Analysis*, (May 2016) <http://disruptivewireless.blogspot.com/2016/05/telecoms-is-too-important-to-leave-to.html>.

<sup>17</sup> *Id.*

<sup>18</sup> Jesús Portal, et al, “Reshaping the future with NFV and SDN: The impact of new technologies on carriers and their networks,” *Arthur D Little & Bell Labs Alcatel Lucent*, [http://www.adlittle.com/downloads/tx\\_adlreports/ADL\\_BellLabs\\_2015\\_Reshapingthefuture.pdf](http://www.adlittle.com/downloads/tx_adlreports/ADL_BellLabs_2015_Reshapingthefuture.pdf).

<sup>19</sup> See Dan Pitt, “SDN Broadband Fast & Furious,” *ONF Blog* (May 2016), [https://www.opennetworking.org/?p=2194&option=com\\_wordpress&Itemid=316](https://www.opennetworking.org/?p=2194&option=com_wordpress&Itemid=316).

<sup>20</sup> See Jason Taylor, “Adopting an open approach to global networks with the Telecom Infra Project,” *Facebook* (Feb, 2016) <https://code.facebook.com/posts/973406756030104/adopting-an-open-approach-to-global-networks-with-the-telecom-infra-project/>.

<sup>21</sup> Neeraj Choubey & Ali Yazdan Panah, “Introducing Facebook’s new terrestrial connectivity systems — Terragraph and Project ARIES,” *Facebook* (April 2016) <https://code.facebook.com/posts/1072680049445290/introducing-facebook-s-new-terrestrial-connectivity-systems-terragraph-and-project-aries/>.

software-defined routing system to link these proto-5G antenna arrays, leading one analyst to claim “Facebook is getting ever closer to being a full-blown mobile service provider.”<sup>22</sup>

This is what cross-platform, dynamic competition could look like, and it should be encouraged. Yet, while much has been made of the potential impact of the Commission’s proposal on the targeted advertising market, the way in which heightened privacy restrictions would discourage potential new entry in network provision by historically data-center-focused companies seems little considered.

Chairman Wheeler acknowledged the importance of the “evolution from hardware-based networks to ones that are software-based” in a speech at The Brookings Institution.<sup>23</sup> At his most expansive, Wheeler asserted that that carrier SDN is not just about reducing costs and improving functionality for incumbent networks, but also “enable[s] LECs to become more fulsome competitors to cable operators’ dominant position in high-speed broadband.”<sup>24</sup> A view of broadband “competition, competition, competition” that is limited to telcos competing against cable companies is troublingly narrow.

An even, uniform enforcement of light-touch privacy guidelines across the broadband ecosystem is not so much about preserving telecom companies’ ability to compete in targeted advertising, although that is important. It is more about having some humility about the direction that innovation will take the industry and not instituting what may before long become outdated silos of disparate regulations.

### The Commission Under-appreciates the Benefits of Information Sharing and Use

The Commission appears to focus almost exclusively on hypothetical harms from information sharing and use by BIAS providers, and fails to adequately recognize the significant upside to an additional source of data that can be put to innovative use. Any new regulations have to recognize there is a balance between the benefits additional sharing and use of data and the risk of privacy harms.<sup>25</sup> 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 Commission appears to under-appreciate this fact.

---

<sup>22</sup> Dan Jones, “Facebook Likes Software Routing for Its Gigabit Radios,” *Lightreading* (May 2016), <http://www.lightreading.com/mobile/5g/facebook-likes-software-routing-for-its-gigabit-radios/d/d-id/723293>.

<sup>23</sup> Prepared Remarks of FCC Chairman Tom Wheeler, The Brookings Institution, June 26, 2015, [http://transition.fcc.gov/Daily\\_Releases/Daily\\_Business/2015/db0626/DOC-334141A1.pdf](http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0626/DOC-334141A1.pdf).

<sup>24</sup> *Id.* at 2.

<sup>25</sup> 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.

The general point has been well recognized by a number of institutions. The President’s Council of Advisors on Science and Technology 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.”<sup>26</sup> As noted by the White House, “properly implemented, big data will become an historic driver of progress.”<sup>27</sup> 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.”<sup>28</sup> In our increasingly connected world, access to information is becoming more and more important, not just for businesses that solely operate on the Internet, but for traditional companies as well.<sup>29</sup> McKinsey estimates that about 75 percent of the value added by data sharing on the Internet accrues to “traditional” industries, especially via increases in global growth, productivity, and employment.<sup>30</sup>

But even those that recognize the benefits of data innovation often over-estimate what are speculative or hypothetical harms. For example, closely examining the harms listed in the White House’s 2014 report, “Big Data: Seizing Opportunities, Preserving Values,” only two cases of harm were concrete.<sup>31</sup> The proposal does not seem to anywhere recognize the benefit of BIAS providers as an important source of useful data, and instead only seeks comment on how that data source should be restricted. Consumers generally benefit from the ability of BIAS providers to more effectively use data, both directly from, for example, enjoying more relevant, less intrusive advertising, and indirectly from having advertisers pay more of the network costs. As long as consumers can opt out of these practices, which, as we note above, they already can, this is win-win, not a violation of a supposed fundamental right of privacy. By not exploring the current and potential

---

<sup>26</sup> 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](https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf)

<sup>27</sup> 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](https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf)

<sup>28</sup> 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](https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf).

<sup>29</sup> See Daniel Castro & Alan McQuinn, “Cross-Border Data Flows Enable Growth in All Industries,” ITIF (Feb 2015), <http://www2.itif.org/2015-cross-border-data-flows.pdf>.

<sup>30</sup> Matthieu Pélissier du Rausas et al., “Internet matters: The Net’s sweeping impact on growth, jobs, and prosperity,” McKinsey Global Institute, May 2011, [http://www.mckinsey.com/insights/high\\_tech\\_telecoms\\_internet/internet\\_matters](http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters).

<sup>31</sup> See Daniel Castro & Travis Korte, “A Catalog of Every ‘Harm’ in the White House Big Data Report,” (July, 2014), <https://www.datainnovation.org/2014/07/a-catalog-of-every-harm-in-the-white-house-big-data-report/>.

benefits of using data from BIAS providers before issuing new regulations, the Commission risks creating unintended consequences for consumers and the economy.

## The FTC Approach Better Promotes Innovation

The FTC model is a superior model to support innovation. The FTC has broad authority under Section 5 of the Fair Trade Act to oversee competition, and can take enforcement actions against unfair or deceptive trade practices.<sup>32</sup> If a broadband provider states that it will allow consumers to opt out of these data-driven services, and that provider does not follow that practice, then it would be subject to the FTC unfair and deceptive acts enforcement.<sup>33</sup> The FTC has also offered more specific guidance when it comes to privacy, putting forth a single, comprehensive, framework guided by three overarching principles: privacy by design, consumer choice, and transparency.<sup>34</sup>

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. Privacy oversight, with rules that apply an equal, light-touch approach, to different actors, would allow better allow for dynamic competition to occur across platforms. A uniform approach, 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 in providing BIAS services.

Beyond the basic protections against unfair or deceptive practices, the FTC has articulated a number of “recommendations for businesses and policy makers.”<sup>35</sup> There the FTC directly and effectively addressed many of the concerns animating the instant rulemaking: BIAS providers are a major gateway to using the Internet, there are switching costs associated with changing BIAS providers, and some areas offer a limited number of choices. Many of these issues are less concerning than when the FTC’s report was written. For example, BIAS switching costs are considerably lower, especially in mobile broadband where providers will pay users to switch to their network. In any event, an opt-out practices like those in use today allay any concerns.

---

<sup>32</sup> 15 USC § 45.

<sup>33</sup> *Id.*

<sup>34</sup> 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>.

<sup>35</sup> *Id.*

But, importantly, the FTC went on to recognize that “[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.<sup>36</sup> This is a widely agreed-upon point: privacy rules in particular, and rules governing technology-enabled practices and business models generally, should be technology-neutral and evenly applicable across different entities. Indeed, this was an animating motivation for the broad Consumer Privacy Bill of Rights proposed by President Obama.

The FTC model has other advantages beyond consistency. It generally attempts to focus narrowly on practices that are actually harming or likely to harm consumers, thus largely avoiding the all too common speculative predictions about how potential privacy risks will weigh against benefits. This gives new technology some space to grow, even where privacy advocates over-react.<sup>37</sup> Compare this to the FCC proposal, which is focused almost entirely on preventing hypothetical harms.

Regulation, and the concomitant focus on compliance, can slow the product development process. Second guessing each decision, running basic business choices through regulatory compliance, and analyzing the risk of running afoul of an unpredictable enforcement bureau, rapidly grinds innovation to a halt. Best practices, with effective oversight, better allows firms to focus on privacy practices that have an actual impact on consumers, instead of mere compliance.

Furthermore, splintering off sector-specific rules would create a troubling problem of inconsistent regulation as a wide variety of government agencies attempt to control their historical regulatory jurisdiction in an age of technological convergence. This problem is likely to be exacerbated as information technology is more tightly integrated with additional verticals, each of which have their own specialized regulator.

## **The FTC Approach Likely Better Protects Privacy**

The FTC has long been the primary agency for developing and enforcing privacy policy, and has done considerable work evaluating the competing values and costs and benefits to various privacy proposals.

Empirical evidence indicates that industries that operate under sector-specific regulations, like healthcare and banking, have less robust privacy practices than industries subject only to the FTC’s oversight. On average, firms without specific regulations invest more in internal privacy controls, and have a greater number of professional personnel focused on meaningful protections for consumers instead of lawyers focused on compliance.

---

<sup>36</sup> *Id* at 56.

<sup>37</sup> See Daniel Castro & Alan McQuinn, “The Privacy Panic Cycle: A Guide to Public Fears About New Technologies,” ITIF (September, 2015), <http://www2.itif.org/2015-privacy-panic.pdf>.

A survey conducted by the International Association of Privacy Professionals (IAPP) found that the median budget for privacy in unregulated firms (\$300,000) is more than double that of government (\$130,000) and 20 percent higher than that of regulated businesses (\$250,000).<sup>38</sup> Unregulated firms reported an average 17 employees working on privacy, compared to 10 employees for firms facing sector-specific regulation.<sup>39</sup>

This may seem counterintuitive, but companies that do not face sector-specific regulations are still face many incentives to devise effective privacy practices. As the IAPP explains “unregulated businesses report a greater focus than regulated businesses or government entities on enhancing the company’s brand and public trust, meeting consumer expectations and fulfilling the needs of business clients and partners.”<sup>40</sup> Regulated industries tend to focus narrowly on compliance and reducing the risk of a data breach, rather than focusing on how to design products and create internal policies that meet the privacy expectations of their consumers.<sup>41</sup>

Also note, interpreting this data as indicating FCC regulations should be preferred as being less costly than continued FTC oversight would be a mistake. Investment in delineating the acceptable data collection and use in new areas, positioning privacy as a competitive differentiator, and skilled privacy professionals working closely with marketing and product teams are all incredibly valuable services for a society tasked with the difficult challenge of balancing privacy and other values in the face of rapidly changing technology. On the other hand, compliance lawyers looking to reduce the risk of FCC fines are almost entirely a deadweight loss to the economy.

## **The Section 706 “Virtuous Cycle” Supports Light-Touch Oversight**

If the FCC regulates BIAS privacy it can be assured that it will do nothing to spur broadband deployment or use, and more likely will limit adoption because broadband revenues from advertising will fall, limiting BIAS providers’ ability to lower prices.

Section 706 of the Telecommunications Act requires the Commission to “encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans.”<sup>42</sup> The Commission has previously framed its Section 706 authority in terms of the so-called “virtuous cycle,” whereby new

---

<sup>38</sup> International Association of Privacy Professionals, IAPP-EY Annual Privacy Governance Report 2015 (2015) at 12, [https://iapp.org/media/pdf/resource\\_center/IAPP-EY\\_Privacy\\_Governance\\_Report\\_2015.pdf](https://iapp.org/media/pdf/resource_center/IAPP-EY_Privacy_Governance_Report_2015.pdf).

<sup>39</sup> *Id.*

<sup>40</sup> *Id.* at 15.

<sup>41</sup> *Id.*

<sup>42</sup> 47 U.S.C. 1302(a).

Internet applications and services, end-user demand for broadband, and network investment and innovation mutually reinforce one another to drive improvements throughout the broadband ecosystem.<sup>43</sup>

The Commission relies primarily on Section 222 of the Communications Act as legal authority for the proposed privacy regulations, but it also argues that “rules governing the privacy and security practices of BIAS providers...would be independently supported by Section 706” because privacy regulations would increase end-user “confidence” in using the Internet.<sup>44</sup> If the “virtuous cycle” theory is to hold any credence, policies the FCC adopts should have a reasonable connection to where limitations are actually restricting growth in Internet use. Simply noting that regulating will impact consumer confidence should not be sufficient for an independent grant of authority, especially given the lack of evidence that BIAS privacy practices have any impact on Internet adoption or use.

In making similar arguments, the FCC has previously pointed to the NTIA’s 2014 Digital Nation report, yet that report plainly states “only 1 percent of household expressed privacy concerns . . . as their primary reason for not using the Internet at home.”<sup>45</sup> The Pew Internet and American Society surveys of Americans’ use of broadband yielded similar results. When non-adopters were asked why they don’t own a smart phone, less than 1 percent of those surveyed listed “worried about privacy/tracking” as a reason. When non-adopters were asked why they don’t subscribe to broadband, privacy did not even make the cut of possible reasons.<sup>46</sup> Moreover, considering most privacy concerns are connected to the broader information ecosystem and the FCC’s professed attempt to keep a relatively narrow jurisdiction with this rulemaking, it is unlikely the FCC can concoct regulations that can allay the concerns of the 1 percent most privacy-sensitive Americans.

Advocates pushing the FCC to act on broadband privacy generally have far higher sensitivity to privacy than the consumers they claim to represent. In reality, most consumers are quite willing to disclose personal

---

<sup>43</sup> The 2010 Open Internet Order first framed the cycle: “The Internet’s openness...enables a virtuous circle of innovation in which new uses of the network—including new content, applications, services, and devices—lead to increased end-user demand for broadband, which drives network improvements, which in turn lead to further innovative network uses.” *Preserving the Open Internet, Broadband Industry Practices*, Report and Order, 25 FCC Rcd 17905, 17910-11, para. 14 (2010)

<sup>44</sup> Privacy NPRM 31 FCC Rcd 2597, para 309.

<sup>45</sup> Protecting and Promoting the Open Internet, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 para. 464 (2015), *citing* the 2015 Broadband Progress Report at paragraph 104, *citing*, NTIA, Exploring the Digital Nation: Embracing the Mobile Internet (Oct. 2014), [http://www.ntia.doc.gov/files/ntia/publications/exploring\\_the\\_digital\\_nation\\_embracing\\_the\\_mobile\\_internet\\_1016\\_2014.pdf](http://www.ntia.doc.gov/files/ntia/publications/exploring_the_digital_nation_embracing_the_mobile_internet_1016_2014.pdf).

<sup>46</sup> John B. Horrigan & Maeve Duggan, “Home Broadband 2015,” *Pew Research Center*, Dec. 21, 2015, <http://www.pewinternet.org/files/2015/12/Broadband-adoption-full.pdf> p. 15

information in exchange for something of value.<sup>47</sup> Most of us are willing to give up location data for more accurate weather predictions or to hail a ride-share. We are willing to give up biometric data to better track our health and fitness. We give up fingerprint data to more easily unlock our phone. The FCC should not be driven to overly-broad regulation by advocates who may well be in that most privacy-sensitive category.

The FCC should especially avoid this outcome when a much more substantial impediment to broadband adoption than privacy concerns is broadband cost—which could potentially be addressed through ad-supported broadband. Instead of taking business models off the table under dubious pretenses, we should be nudging consumers towards allowing innovative uses of broadband data that could help make service cheaper.

There is a real possibility that advertising-supported broadband could make for a cheaper alternative to one that is supported by monthly bills alone. As well-covered in the press, AT&T has experimented with one of its “GigaPower” products in Austin, TX that offers a lower monthly fee if users agree to allow tracking of online activity.<sup>48</sup>

Others have shown data collection and targeting advertising can allow for broad deployments of free, public WiFi. Beyond WiFi deployments in cafes and coffee shops (which collect user data) that the FCC explicitly excluded from its definition of “BIAS provider,” Both New York City and Kansas City have deployed kiosks that provide free Internet connection.<sup>49</sup> These services are offered conditional to accepting the sharing of data, so the FCC’s proposal, if adopted, would make them unlawful.

An automatic presumption against these new kinds of pricing practices is remarkably anti-consumer. To the extent broadband user data can be monetized, there is a significant opportunity to reduce the cost of broadband service and thus expand broadband adoption. Recent research indicates that the cost of service may play more of a role in broadband non-adoption than initially thought (as compared to questions of relevance or digital literacy).<sup>50</sup> The opportunity to offer variable pricing based on data collection policies is

---

<sup>47</sup> Lee Rainie & Maeve Duggan, “Privacy and Information Sharing: Many Americans Say they might provide personal information, depending on the deal being offered and how much risk they face,” *Pew Research Center* (Jan 2016), <http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/>.

<sup>48</sup> See e.g., Elizabeth Dwoskin & Thomas Gryta, “AT&T Offers Data Privacy—for a Price,” *Wall Street Journal*, <http://blogs.wsj.com/digits/2015/02/18/att-offers-data-privacy-for-a-price/>.

<sup>49</sup> See Stacey Higginbotham, “In Kansas City you trade your data for Wi-Fi,” *Medium* (May 2016) <https://medium.com/@gigastacey/in-kansas-city-you-trade-your-data-for-wi-fi-5ef26e8bed54#.8ddlm3pvs>; Kaveh Waddell, “Will New York City’s Free Wi-Fi Help Police Watch You?” *The Atlantic* (Apr. 2016), <http://www.theatlantic.com/technology/archive/2016/04/linknyc-new-york-wifi-privacy-security/477696/>.

<sup>50</sup> See, e.g. Amina Fazlullah, “Research Shows Cost is Biggest Barrier to Broadband Adoption,” *Benton Foundation*, Jan. 11, 2016, <https://www.benton.org/blog/research-shows-cost-biggest-barrier-broadband-adoption>.

potentially a boon for those looking for a lower-cost option to either get online or move towards a faster speed connection. Advertising supported broadband or other platforms will drive further broadband adoption and use.

## **The Proposal is Inconsistent with U.S. Approach to Privacy Abroad**

The FCC's proposal undermines the position of the United States in its advocacy around the world for privacy regimes that more closely mirror our own. Privacy concerns can vary considerably from culture to culture, and not everyone shares U.S. values. Some countries are eager to promote their own information technology companies, and privacy offers a convenient lever to ratchet up those protections.

The FCC, in singling out a single class of market participants for heightened regulations, emboldens and legitimizes similar efforts around the world. A consistent, uniform privacy regime would be much easier to promote to countries. Of course, the FTC already enforces a wide variety of privacy laws much narrower than its Section 5 authority, but the Commission's proposal represents a significant splintering of an important portion of the broadband ecosystem, significantly complicating what can already be a confusing area of the law and undermining the cohesiveness of FTC oversight.

## **The Commission Can Lawfully Leave Privacy to the FTC**

Generally speaking, the FTC Act precludes the FTC from addressing common carrier practices, leaving these to the specialized regulator—the so-called “common carrier exemption.”<sup>51</sup> The FCC asserts that “FTC lacks statutory authority to prevent common carriers from using such unfair or deceptive acts or practices.”<sup>52</sup> Some have argued that this exemption creates a vacuum obligating the FCC to act on broadband privacy.<sup>53</sup> But the FCC need not regulate privacy, and can lawfully leave broadband privacy to the FTC.

The FCC has broad authority to interpret its statute, and is clearly within its power to forebear from Section 222 as applied to BIAS providers. The Commission can acknowledge the fact that BIAS privacy practices are non-common carrier activities, and thus the FTC is not precluded from acting with regard to broadband

---

<sup>51</sup> 15 U.S.C. § 45(a)(2).

<sup>52</sup> Privacy NPRM, 31 FCC Rcd at 2596, para 306.

<sup>53</sup> See e.g., Harold Feld et. Al, “Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World,” Public Knowledge, Feb. 2016, [https://www.publicknowledge.org/assets/uploads/blog/article-cpni-whitepaper\(1\).pdf](https://www.publicknowledge.org/assets/uploads/blog/article-cpni-whitepaper(1).pdf)

privacy.<sup>54</sup> In addition to forbearing from 222 as applied to BIAS, the Commission should clarify the existing memorandum of understanding between the two agencies that broadband privacy is the province of the FTC.

## **IF THE COMMISSION MUST REGULATE, IT SHOULD DO SO IN A WAY THAT PROMOTES INNOVATION**

If the Commission feels it is obligated to regulate broadband privacy, it should attempt to do so in a way that best promotes innovation. It can do this most expediently by adopting an approach consistent with the FTC and avoiding an overly-broad opt-in requirement. The Commission should keep its regulations clear and narrow, and relax its requirements for sharing aggregate or otherwise de-identified data.

### **If the Commission Believes It Must Regulate, It Should Adopt an Approach Consistent with the FTC**

As discussed above, an application of FTC style enforcement evenly across the Internet ecosystem will best allow for innovation and dynamic competition across traditional industry boundaries. For this reason, if the FCC feels it must continue with this rulemaking, it should seek to harmonize its framework with the FTC's practices to the greatest extent possible. The FTC's privacy regime has worked well to find the balance of necessary privacy protections and innovation-enhancing information sharing over time.

The hallmarks of the FTC's method, transparency, notice, and choice, do much of the heavy lifting in this area, informing customers of their options and allowing BIAS providers flexibility to find beneficial uses of data while retaining consumers' trust. The FTC model can also guide the Commission in deciding when to take enforcement action: when there is actual consumer harm.<sup>55</sup> BIAS providers already follow FTC guidelines, offering consumers the ability to opt-out of data sharing, so the FCC can, and should, take the option to institute protections while doing little disruption to current practice.

The Commission should also encourage the continued formation of enforceable industry best practices. The case of Verizon's so-called "super-cookie" shows how best practices, concern for preserving reputation and respect for consumer trust, can guide privacy policies without specific regulatory constraints. In October 2014, news stories described a practice by Verizon Wireless of modifying some of its cellular web traffic to

---

<sup>54</sup> At least one court has ruled the common carrier exemption of Section 5 should be narrowly read as "activity based," triggering only when ISPs are engaged in common carrier activities, rather than a simple question of status. *See Federal Trade Commission v. AT&T Mobility*, Order Denying Defendant's Motion to Dismiss, No. C-14-4785 EMC, March 31, 2015, <https://www.ftc.gov/system/files/documents/cases/150331attmobilityorder.pdf>.

<sup>55</sup> *See* Daniel Castro & Alan McQuinn, "How and When Regulators Should Intervene," ITIF (Feb 2015), <http://www2.itif.org/2015-how-when-regulators-intervene.pdf>.

insert a Unique Identifier Header (UIDH), dubbed a “super-cookie,” that helped create profiles for targeted ads.<sup>56</sup> Listening to the concerns of the privacy community, Verizon voluntarily changed its policy in March 2015, and began allowing users to opt out of the tracking program.<sup>57</sup>

This clearly shows that BIAS providers are indeed informed and guided by public reaction to these practices. Some advocates attempt to paint this as an area where BIAS providers are unconstrained, which simply is not true. By promoting a dynamic process whereby consumers can inform the particular shape of privacy consent processes, in combination with existing “opt out” possibilities, concerns around BIAS data collection disappear. Consumers that object to a broadband provider’s CPNI policy would not have to switch carriers if they can simply opt out.

### **An Opt-In Regime Stifles Innovation**

At a minimum, the FCC should do away with its broad opt-in requirement for use and sharing of data by BIAS providers. The United States has generally gone with opt-out privacy frameworks, and only applies opt-in requirements for especially sensitive information. As the research of Catherine Tucker at MIT has shown, the more lightly regulated and flexible privacy regime in the United States is a key factor in why we lead the world in the Internet economy.<sup>58</sup> The FCC proposes a wildly over-broad opt-in regime that is clearly designed to lock BIAS providers out of building business practices around sharing data to market non-communications products and services. This is a severe departure from the FTC’s established practices that cannot be reasonably grounded in any possible risk of harm or affording consumers additional control.

An opt-out regime would adequately give consumers control over how their data is treated, even though the percentage of those who care to exercise it is small. An opt-out approach would be consistent with a technology-neutral approach, preserves carriers’ and third-parties’ ability to innovate with this data, and could ultimately lower cost for consumers. At most, obtaining consumers’ affirmative express consent should be required only for sensitive information.

---

<sup>56</sup> Robert McMillan, “Verizon’s ‘Perma-Cookie’ is a Privacy-Killing Machine,” *Wired*, October 27, 2014, <http://www.wired.com/2014/10/verizons-perma-cookie/>.

<sup>57</sup> Brian Chen, “Verizon Wireless Customers Can Now Opt Out of ‘Supercookies,’” *New York Times*, March 31, 2015, <http://bits.blogs.nytimes.com/2015/03/31/verizon-wireless-customers-can-now-opt-out-of-supercookies>.

<sup>58</sup> 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](http://jthtl.org/content/articles/V10I2/JTHTLv10i2_Tucker.PDF)

## De-identification Techniques Can Sufficiently Protect Privacy

The proposal, in considerably broadening of the CPNI statute and even other sector-specific privacy rules, aims to require BIAS providers “ensure the aggregated customer PI is not reasonably linkable to a specific individual or device.”<sup>59</sup>

Several scholars have argued that we should not over-react to the risks of re-identification, and, furthermore, common sense tells us that we can get a great deal of utility out of anonymized data with reasonable privacy safeguards. In justifying this broad requirement, the Commission cites Latanya Sweeney’s famous study showing that 87% of the U.S. population could be uniquely identified by gender, ZIP code, and date of birth.<sup>60</sup> This research, and other similar studies, provides a good grounding for understanding the balance between re-identification risk and utility of data sets. Researchers at Palo Alto Research Center have since replicated this study using 2010 census data, finding that only 63% of the population is uniquely identifiable given those data categories.<sup>61</sup> More importantly, the risk of unique identification drops off sharply when given slightly more abstract data. For instance, if the data is limited to gender, ZIP code, and the month and year of birth (instead of the full birthday), the percentage of those uniquely identifiable drops to 4.2%.<sup>62</sup> Similarly, if one replaces the ZIP code with the county in which a man or woman with a particular birthday lives, only 0.2% of the population is unique.<sup>63</sup>

This simple example illustrates that there is a balance between the utility of data and the privacy risk. The more granular data is, the more useful it may be to researchers, but the greater the risk of re-identification. Some types of data can have remarkably long tails—for example, the oldest living person can easily be picked out of the world’s population given only a dataset of birth year. There will always be a risk of targeted re-identification against statistical outliers.

The goal of the Commission should not be eliminating the risk of identification, but instead balancing the risk of harm from re-identification with the tremendous benefits that would flow from innovative uses of anonymized and/or aggregate data. For, as explored by Jane Yakowitz, the risk of privacy harm from re-identification is significantly lower than many risks we all take without concern, such as throwing out our

---

<sup>59</sup> Privacy NPRM, 31 FCC Rcd 2554, para 157.

<sup>60</sup> Privacy NPRM, 31 FCC Rcd 2554, note 263, *citing* Latanya Sweeney, Abstract, Uniqueness of Simple Demographics in the U.S. Population (Carnegie Mellon Univ., Lab. for Int’l Data Privacy 2000), <http://dataprivacylab.org/projects/identifiability/index.html>.

<sup>61</sup> Phillippe Golle, Revisiting the Uniqueness of Simple Demographics in the US Population, Palo Alto Research Center, available at <http://crypto.stanford.edu/~pgolle/papers/census.pdf>.

<sup>62</sup> *Id.* at 2.

<sup>63</sup> *Id.*

trash.<sup>64</sup> Felix Wu, a professor at Benjamin N. Cardozo School of Law, claims that there is not much support for the “strongly pessimistic view” that no useful data can be anonymous.<sup>65</sup> He explains that “[a] closer look at the computer science ... reveals that several aspects of that literature have been either misinterpreted, or at least overread, by legal scholars.”<sup>66</sup> Despite the misleading headlines and assertions made by some of those reporting on this topic, de-identification continues to be a valuable and effective mechanism for protecting personal information.<sup>67</sup>

The FTC framework generally allows flexible use of de-identified data that cannot be reasonably linked to an individual. The FCC proposal goes considerably further, putting the burden on BIAS providers to prove that aggregate data cannot be re-identified, contractually prohibit third parties from attempting to re-identify data, and even monitor those third parties to ensure that those contracts are not violated.<sup>68</sup> The FCC should relax these requirements to facilitate the use of aggregate or otherwise de-identified data. Instead of affirmatively requiring BIAS providers to prove data cannot be re-identified, and tailor those practices to each particular dataset, the FCC should follow the FTC approach.

### **The Commission Should Clarify, Narrow the Scope of its Jurisdiction**

The FCC has defined BIAS provider as “[a] mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service....”<sup>69</sup> This is potentially a broad set of services, especially if this Commission or a future Commission decides to read the term “capability” broadly. The potential for the Commission’s regulations to creep into other areas of the broadband ecosystem will create confusion and discourage innovators from offering products that integrate with the open Internet. Again, it would be far and away best for the Commission to refrain from regulating broadband privacy, absent that, it should regulate in a way that is consistent with FTC practices. But if the FCC must regulate BIAS providers differently, it should be done as narrowly and clearly as possible to avoid unnecessary confusion.

---

<sup>64</sup> Jane Yakowitz, Tragedy of the Data Commons, 25 HARVARD J. OF L. & T. 1, 40, 2011.

<sup>65</sup> Felix T. Wu, Defining Privacy and Utility in Data Sets 84 U. OF COLO. L. REV. 1118, 1124.

<sup>66</sup> *Id.*

<sup>67</sup> Ann Cavoukian & Daniel Castro, “Big Data and Innovation, Setting the Record Straight: De-identification *Does Work*” *Information and Privacy Commissioner of Ontario* (June 2014), <http://www2.itif.org/2014-big-data-deidentification.pdf>.

<sup>68</sup> Privacy NPRM 31 FCC Rcd 2553-4, para 154.

<sup>69</sup> 47 CFR § 8.11(a).

## CONCLUSION

The proposed regulations would reduce the efficiency of the broadband industry, with resultant loss of broadband network investment and higher prices for broadband consumers. The basic structure of the Commission's proposal is fundamentally flawed. It attempts to constrain specific companies from innovating with new advertising-supported broadband offerings, reifies a static industry structure, under-appreciates the value of data innovation.

The best option is for the Commission to leave broadband privacy with the FTC's enforcement of established framework and guidelines, but to the extent it feels it must act, it should do so in a way that best promotes innovation.

Doug Brake  
Telecommunications Policy Analyst  
Information Technology and Innovation Foundation  
1101 K Street NW, Suite 610  
Washington, DC 20005

May 27, 2016