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 in Support of the Petitions for Reconsideration

The Information Technology and Innovation Foundation (ITIF) writes in support of the petitions for reconsideration in the above-captioned proceeding.[1] In the waning days of the Obama administration, the Federal Communications Commission (FCC) passed a set of rules that effectively shut broadband providers out of new data-driven business models. It is important that broadband consumers have choice and control over how their data is used, but the overly restrictive defaults imposed by the recent FCC rules come at a real cost to the economy and do not align with an average consumer's best interest, contrary to flawed assertions in the record.

Thankfully, the Commission now has an opportunity to revisit these flawed rules. The Commission should vacate these rules in their entirety or significantly revise the rules such that they "parallel the [Federal Trade Commission's] framework as closely as possible" as to not erect technology-based regulatory silos, unduly impede innovation, or diminish dynamic, cross-sector competition.[2]

[1] Founded in 2006, 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.

[2] In re Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Report and Order, FCC 16-148, WC Docket No. 16-106 (rel. Nov. 2, 2016), ("Report and Order"), Commissioner Pai Dissent at 1.

INTRODUCTION

The FCC's privacy rulemaking was initiated in part because of the classification of broadband as a common carrier under Title II of the Communications Act—a step taken to implement the particular net neutrality rules the FCC wanted. This common carrier status prevents the normal privacy cop, the Federal Trade Commission (FTC), from pursuing its usual privacy oversight duties when it comes to broadband providers. But sector-specific privacy rules for broadband providers are fundamentally misguided; broadband privacy belongs with the FTC. Under the FTC's enforcement of best practices and broadband provider policies, privacy protections are well balanced with other values, such as cost, usability, and innovation.

The FCC's sector-specific rulemaking underappreciated the impact of increasingly prevalent privacy-protecting technologies like encryption and virtual networks. What's more, all major broadband providers already allowed consumers to control how their information is used—a fact the FCC appears to have ignored. It is unfortunate that the FCC was convinced to dispose with FTC-style privacy oversight, as it comes with numerous benefits. The greater flexibility under the FTC enforcement framework allows room for new business models that could support expensive, next-generation networks with revenue other than consumers' monthly bills.

The FCC's deviation from the historical privacy protections of the FTC framework has the potential to significantly disrupt ongoing dynamic competition in innovative new uses of Internet data, ultimately slowing the rate of growth of broadband deployment and adoption. Beyond the obvious opportunities to put downward pressure on broadband prices through more targeted advertising, data is increasingly becoming a key fuel for innovation. Recent breakthroughs in artificial intelligence are predicated on "training" algorithms on large pools of data, so to effectively shut data collected by broadband providers out of this burgeoning field would be a mistake.

The FCC's rulemaking set a poor precedent for privacy rules touching other sectors of the economy, undermined the U.S. position when negotiating privacy issues abroad, dramatically deviated from the usual consensus-driven multistakeholder model of developing Internet rules, and unnecessarily expanded the scope of utility-style regulation of broadband. Indeed, it was an unfortunate step toward a European-style privacy regime based on the risk-averse precautionary principle. The FCC is right to begin dismantling these flawed rules.

THE COMMISSION SHOULD VACATE THE MISGUIDED PRIVACY RULES

Just as Title II is not the right home for broadband, Section 222 is not the proper source of authority for privacy oversight of broadband providers. Fundamental changes to broadband jurisdiction come with a tangled web—undoing these mistakes will be a delicate process. But the Commission should be undeterred by overblown claims from activists and vacate these rules in their entirety.

The Commission did not adequately consider many issues in the record. Many of the arguments familiar to those who have been following the proceeding were given short shrift, such as the dramatic, rapid adoption of

encryption that greatly diminishes the risk of privacy harm from broadband Internet access service (BIAS) provider use of data.

More fundamentally, judging from the privacy report and order, the Commission did not seek to balance the protection of privacy interests with countervailing benefits of additional data sharing and use. Instead, the Commission justified these heightened privacy restrictions through a combination of the supposed obligation to create rules in the FTC's stead (absent due to the common carrier exemption triggered by the misguided Title II classification) and the hypothetical harms from information sharing and use by BIAS providers. The report and order at times mentions a desire to "encourage the technological and business innovation that help drive the many benefits of our increasingly Internet-based economy" but sought to do so primarily through "bolstering customer confidence," which it thought would in turn "promote the virtuous cycle of innovation in which new uses of the network lead to increased end-user demand for broadband."[3]

This approach is severely misguided. First, it assumes a static system with unchanging competitive dynamics. It improperly seeks to secure BIAS as a static, common carrier utility that cannot experiment with new business models like other parts of the Internet ecosystem. If there is any doubt that the intention of these rules is to close off business model innovation, consider former Chairman Wheeler's initial notice of proposed rulemaking, which explicitly attempted to restrict data use based exclusively on the business purposes to which it would be put. This approach chills innovation, reduces the possibility of cross-sector innovation, and effectively erects technology-based regulatory silos.

More fundamentally, the rules fail to adequately recognize the significant upside to additional sources of data that can be put to innovative use. Any new regulations must recognize there is a balance between the benefits of additional use of data and the risk of privacy harms.[4] 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 underappreciate this fact.

At a high level, this point has been well recognized by several 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."[5] As noted by the Obama White House, "properly implemented, big data will become

---

[3] Report and Order at 3.

[4] 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.

[5] 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.

an historic driver of progress."[6] 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.[7] 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.[8]

The rules do not seem to anywhere recognize the benefit of BIAS providers as an important source of useful data. Consumers generally benefit from the ability of BIAS providers to more effectively use data, both directly from enjoying more relevant, less intrusive advertising, and indirectly from having advertisers pay more of the network costs. But advertising is just one of many unpredictable uses for broadband data. For example, recent breakthroughs in artificial intelligence are predicated on "training" complicated algorithms on large pools of data, for which broadband data is potentially quite useful.

If consumers can opt out of practices they are not comfortable with, a choice architecture with defaults that encourage rather than restrain innovation would be a win-win. By not exploring the current and potential benefits of using data from BIAS providers, the Commission risks creating unintended consequences for consumers and the economy if these rules are not revisited.

Furthermore, the Commission did not adequately establish why an opt-out mechanism is not a sufficient protection of privacy in the face of the benefits of additional data sharing and use. All major BIAS providers already offer consumers the ability to opt-out of existing targeted advertising programs.[9] 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. Under former Chairman Wheeler, the Commission touted the new privacy rules as putting the consumer in control of their data. The truth is users will have no more and no less "control" over how companies use their broadband data if these rules go forward—a choice architecture of opt-in as the default instead of an opt-out removes data from being put to beneficial uses without empowering consumers with any additional control. What changes is the ability of ISPs to responsibly experiment with new ways of supporting the expensive deployment and maintenance of

---

[6] 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.
[7] *See* Daniel Castro & Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries," ITIF (February 2015), http://www2.itif.org/2015-cross-border-data-flows.pdf.
[8] Matthieu Pélissié 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.
[9] *See* Doug Brake, Daniel Castro, & Alan McQuinn, Information Technology and Innovation Foundation, "Broadband Privacy: The Folly of Sector-Specific Regulation," (March 2016), http://www2.itif.org/2016-broadband-privacy-folly.pdf.

broadband networks. The FCC is functionally making the choice for consumers by mandating an 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, further bolstering the case for revisiting these rules.

POTENTIAL HARM FROM VACATING THE PRIVACY RULES IS WILDLY OVERSTATED

Public interest filers, in their opposition to the petition for stay, assert that if the Commission grants reconsideration, "[a]s a practical matter. . . consumers will lack meaningful privacy protections for a significant period of time."[10] The hedging "as a practical matter" and "meaningful" are there for good reason: In a footnote to that assertion, the public interest groups rightly admit that "federal law would still require that ISPs protect consumer information."[11]

For however long the FTC is exempted from exercising their Section 5 authority over broadband providers, the Commission can fall back on its ability to enforce Section 222 without specific regulations. The Commission can return to something akin to the May 2015 enforcement advisory, which called on broadband providers to take "reasonable, good-faith steps to comply with Section 222."[12] The FCC could rely on that advisory, or issue a similar advisory if it has more specific policy guidance, such as an expectation that the Commission will enforce the statute in line with FTC Section 5 authority. This would see the Commission seek to hold companies to the privacy commitments they make to consumers. Industry has committed itself to just such a set of best practices.[13]

This is an imperfect, temporary solution, but a very workable one. An enforcement advisory expecting compliance with the broader statute, without specifying regulations, is admittedly an uncertain step forward. But the Commission should not allow privacy advocates to leverage this period of uncertainty into a one-way ratchet for stricter, less-balanced privacy regulations. Since the effective date of the Open Internet Order in June 2015, we have been without specific privacy regulation for broadband providers, and yet the parade of privacy horribles advocates now describe has not come to pass. There has been no breakdown in broadband privacy. Another period of similar uncertainty is justified as the Commission unwinds the unfortunate Title II classification and returns broadband privacy to FTC oversight.

---

[10] Public Interest Organizations opposition to petition for stay, WC Docket No. 16-106 (February 3, 2017), at 6.
[11] *Id.*
[12] Federal Communications Commission, "Enforcement Bureau Guidance: Broadband Providers Should Take Reasonable, Good Faith Steps to Protect Consumer Privacy."
[13] "Protecting Consumer Privacy Online," *NCTA,* (January 27, 2017 press release), https://www.ncta.com/news-and-events/media-room/content/protecting-consumer-privacy-online.

Various commenters have pointed to a Ninth Circuit opinion of last summer as reason to leave broadband privacy under the purview of the FCC.[14] For instance, Harold Feld of Public Knowledge, in reaction to this case wrote "help us FCC, you're the consumer's only hope."[15] In their opposition to the stay petition, public interest advocates wrongly advance the blanket claim that "because of the Ninth Circuit decision, the FTC cannot require ISPs to comply with their voluntary privacy policies."[16]

As we at ITIF have previously explained, many of the initial reactions to this case were way overblown.[17] While this case merits attention by policymakers, its ultimate impact is likely small. The case is pending a rehearing, and a reversal seems possible if not likely. The Communications Act, the law to regulate commerce in question here, is clearly "activity-based" in its scope, only regulating common carriers insofar as they are engaged in common carriage. In the *AT&T Mobility* case, the Ninth Circuit ended its analysis prematurely. The court need only hold on rehearing that when determining the scope of the common carrier exemption, whether it is activity-based or status-based, simply look to the act in question. Regardless, this is a case of limited jurisdiction, and it contains limiting language in its own decision (albeit phrased in the negative). Furthermore, there is bipartisan support for removing the common carrier exemption, if not a broader bill to ground broadband privacy and net neutrality issues in clear legal authority.

To allow these broadband privacy rules to move forward out of fear of the jurisdictional implications of the Ninth Circuit decision would allow the tail to wag the dog. Given the tenuousness of the impact of this case, and the myriad ways in which any policy ills resulting from it can be cured, it would be foolish for the Commission to hesitate in dismantling these rules.

---

[14] *FTC v. AT&T Mobility LLC*, No. 3:14-cv-04785-EMC (9th Cir. 2016).
[15] Harold Feld, "Understanding the Ninth Circuit's Decision in AT&T Mobility v. FTC," *Public Knowledge* (August 2016), https://www.publicknowledge.org/news-blog/blogs/understanding-the-ninth-circuits-decision-in-att-mobility-v-ftc.
[16] Public Interest opposition to stay at 7.
[17] Doug Brake, "Ninth Circuit Throws Wrench into Jurisdictional Boundary Between FCC and FTC" *Innovation Files* (September 2, 2016), https://itif.org/publications/2016/09/02/ninth-circuit-throws-wrench-jurisdictional-boundary-between-fcc-and-ftc.

ALTERNATIVELY, THE COMMISSION SHOULD ALIGN ANY RULES WITH THE FTC ENFORCEMENT MODEL

Short of vacating the rules entirely, if the Commission hopes to promote continued flourishing of innovation throughout the Internet ecosystem, it would be wise to revisit these rules to truly align them with the FTC model. 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.[18] 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.[19] 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.[20]

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 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.

The FTC model has other advantages beyond consistency. It generally attempts to focus narrowly on practices that are 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 overreact.[21] Compare this to the FCC rules, which are 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,

---

[18] 15 USC § 45.
[19] *Id.*
[20] 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.
[21] *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.

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.

Throughout this proceeding the 2012 FTC privacy report, "Protecting Consumer Privacy in an Era of Rapid Change," has been continually conflated with its actual enforcement authority. That report was a set of unenforceable guidelines, whereas Section 5 is fundamentally an ex post, harm-based mechanism. The Commission did not adequately consider the benefits to innovation of a truly flexible oversight model that holds companies to their commitments and steps in where harm occurs, but otherwise allows for new uses of data to take shape. Instead the Wheeler Commission claimed to align its rules with the 2012 report, with a few notable departures.

Removing web browsing and app usage from the category of sensitive information would be a small step in the right direction. It would help align FCC regulations with FTC identified best practices, but it is worth recognizing that even this would be significantly more restrictive than actual FTC practice.

CONCLUSION

Far and away the best course forward for the Commission is to vacate these rules in their entirety. The Commission did not consider several important arguments in the record, and did not adequately consider the benefits of putting additional broadband data to use in the economy. Claims advanced by privacy advocates are overstated, and the Commission should reconsider these rules. Ideally, the rules should be vacated in their entirety as the Commission also seeks comment on the appropriate legal framework for broadband generally.

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

March 6, 2017