Before the

Federal Communications Commission

Washington, D.C. 20554

In the Matter of	)	
	)	WC Docket No. 17-108
Restoring Internet Freedom	)	

Privacy Comments

of the

International Center for Law & Economics

August 30, 2017

ICLE | 3333 NE Sandy Blvd., #207 | Portland, OR 97232 | 503.770.0652
icle@laweconcenter.org | @laweconcenter | www.laweconcenter.org

Introduction & Executive Summary 2
I. There is no basis for treating ISPs differently than the rest of the online economy with respect to privacy 6
A. ISPs do not present a unique threat 6
B. Broadband is sufficiently competitive to protect consumer choice, and getting more competitive by the day 9
II. The Failings of the FCC's *2016 Privacy Order* 12
A. The *2016 Privacy Order* did not evince understanding of the market 12
B. The FCC's 2016 approach did not mirror the FTC's approach 14
1. Opt-in 16
2. Consumer expectations 17
3. Other categories of data 19
C. The *2016 Privacy Order* fetishized technical possibilities without actually considering market realities 20
III. Good reasons to avoid overregulation of ISP privacy 22
A. Data and dollars: Online business models aren't fixed 22
B. Even where competition might be more limited, ISPs should not be discriminated against with more onerous rules 26
IV. Regulation of ISP Privacy Practices Should Revert to the FTC 28
A. The FTC's experience and expertise make it the best agency to oversee ISP privacy practices. 28
B. Preempting state regulation of ISP privacy practices will prevent the formation of a patchwork of privacy regulation that would be harmful to policy objectives 29
C. Concerns over Ninth Circuit's *AT&T Mobility* decision are misguided 31
Conclusion 33

Introduction & Executive Summary

As the Commission's *NPRM* notes, the *2015 Open Internet Order* "has weakened Americans' online privacy by stripping the Federal Trade Commission – the nation's premier consumer protection agency – of its jurisdiction over ISPs' privacy and data security practices."[1] The *Restoring Internet Freedom NPRM* further notes that:

[1] Notice of Proposed Rulemaking, *In the Matter of Restoring Internet Freedom*, WC Docket No. 17-108 (May 18, 2017) at ¶ 4 [hereinafter "*Restoring Internet Freedom NPRM*"].

> To address the gap created by the Commission's reclassification of broadband Internet access service as a common carriage service, the *Title II Order* called for a new rulemaking to apply section 222's customer proprietary network information provisions to Internet service providers. In October 2016, the Commission adopted rules governing Internet service providers' privacy practices and applied the rules it adopted to other providers of telecommunications services. In March 2017, Congress voted under the Congressional Review Act (CRA) to disapprove the Commission's *2016 Privacy Order*, which prevents us from adopting rules in substantially the same form.[2]

The *Restoring Internet Freedom NPRM* proposes to return to the status quo in place before the Commission adopted its *2015 Open Internet Order* with respect to privacy rules: not to adopt any new FCC rules, and leave regulation of privacy to the FTC.[3] We offer these comments in response to the Commission's request regarding that proposal.[4]

Getting regulation right is always difficult, but it is all the more so when confronting evolving technology, inconsistent and heterogeneous consumer demand, and intertwined economic effects that operate along multiple dimensions — all conditions that confront online privacy regulation:

> [S]ecuring a solution that increases social welfare[] isn't straightforward as a practical matter. From the consumer's side, the solution needs to account for the benefits that consumers receive from content and services and the benefits of targeting ads, as well as the costs they incur from giving up data they would prefer to keep private. Then from the ad platform's side, the solution needs to account for the investments the platform is making in providing content and the risk that consumers will attempt to free ride on those investments without providing any compensation—in the form of attention or data—in return. Finally, the solution must account for the costs incurred by both consumers and the ad platform including the costs of acquiring information necessary for making efficient decisions.[5]

Placing onerous restrictions upon ISPs alone would result in either under-regulation of edge providers or over-regulation of ISPs within the market, without any clear justification as to why consumer privacy takes on different qualities for each type of platform. But the proper method of regulating privacy is, in fact, the course that both the FTC and the FCC have historically taken, and which has yielded a stable, evenly administered regime: case-by-case examination of actual privacy harms and a minimalist approach to *ex ante*, proscriptive regulations.

---

[2] *Id.* at ¶ 66.

[3] *Id.* at ¶ 67.

[4] *Id.*

[5] David S. Evans, *Mobile Advertising: Economics, Evolution and Policy* (June 1, 2016) at 45, *available at* http://ssrn.com/abstract=2786123.

(cont.)

As the Commission itself has recognized, "[t]he intersection of privacy and technology is not new."[6] And yet in October 2016 the agency adopted a privacy regulatory regime for ISPs that was essentially disconnected from the collective wisdom of the agencies, scholars, and policy makers that have been operating in this space for decades. Eschewing consideration of business realities, and inadequately addressing consumer welfare effects, the *Order* was a prescriptive, invasive privacy regime inconsistent with "best practices" promoted by other agencies.

At the root of the *2016 Privacy Order* was the belief that "broadband is different," and should be regulated differently. But as even the Obama White House acknowledged, this just is not so.[7] And a significant risk of the FCC adopting privacy rules unique to ISPs is that it will, as former Chairman Wheeler did, contemplate a regime that insufficiently understands the consequences of its rules, especially upon the non-telecom markets they touch.

While former Chairman Wheeler's FCC paid lip service to the notion that mandated privacy and security protections must be designed to ensure that they do not undermine the larger goals of promoting broadband innovation and encouraging broadband access and use,[8] its *2016 Privacy Order* relied solely on hypothetical, *potential* harms that *could* arise. The "evidence" for these possible transgressions was a small subset of comments it received that described *not* ISPs' actual practices but merely the extent of ISPs' potential access to personal data.[9]

For the previous Commission, because ISPs' "position ***allows*** them to see every packet that a consumer sends and receives over the Internet while on the network, including, absent encryption, its contents,"[10] they ***would*** do so (and needed to be regulated accordingly). The Order asserted that, even with encryption, "encrypted web traffic ***can be used to infer***" what pages and resources users access.[11] But when it came to assessing actual practice, the Commission failed to address the business realities that dictate a far more circumscribed approach to ISP use of consumer data; instead, it asserted a need for special, heightened consumer protections against the presumed depredations of

---

[6] Notice of Proposed Rulemaking, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket 16-106 (Apr. 1, 2016), at ¶ 1 [hereinafter "*2016 Privacy NPRM*"].

[7] WHITE HOUSE,CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 6 (Feb. 2012) *available at* https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.

[8] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Report and Order, FCC 16-148 (rel. Nov. 2, 2016), at ¶ 1 [hereinafter "*2016 Privacy Order*"]. Of course, it is far from clear that the Commission in fact has a *legal* basis for applying CPNI rules drafted for switched-telephone networks to modern high-speed broadband networks. *See* Reply Comments of TechFreedom, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket 16-106 (Jul. 6, 2016) at 7.

[9] *2016 Privacy Order* at ¶¶ 29-35.

[10] *Id.* at ¶ 30 (emphasis added).

[11] *Id.* at ¶¶ 33-34 (emphasis added).

(cont.)

prying ISPs based on mere *ability*, rather than consideration of the market dynamics that guide their actual conduct.

Other U.S. privacy regulators evidence restraint and assess trade-offs, recognizing that the authorized collection and use of consumer information by data companies confers enormous benefits, even as it entails some risks. Indeed, the overwhelming conclusion of decades of intense scrutiny is that the application of *ex ante* privacy principles across industries is a fraught exercise as each industry — indeed each firm within an industry — faces a different set of consumer expectations about providing innovative services and privacy protections.[12]

Without engaging in this sort of reasoned analysis, the FCC's 2016 Order offered a selective presentation of the state of our knowledge about ISPs' *ability to access* personal data and asserts these potentialities as foregone conclusions. But a risk of harm cannot be inferred from mere ability — and the business realities do not support a more invasive, opt-in approach to privacy for ISPs. Instead, they counsel in favor of a case-by-case assessment of actual allegations of harm consistent with the FTC's approach and a balanced analysis of consumer welfare effects, rather than a restrictive, *ex ante* rule.

There is no reason to return to the flawed, FCC-enacted, broadband-specific privacy rules once Title II is rescinded. Even the Obama White House thought that ISP privacy regulation should be housed at the FTC.[13] Absent the FCC's classification of broadband internet access service ("BIAS") as a Title II service and the resulting lack of FTC authority over ISPs, there is nothing about ISPs that necessitates either different rules or different regulators.

To ensure consistent regulation of privacy practices on the Internet, the FCC should declare that BIAS is an interstate information service. Taking this step will have a number of salutary effects, including returning jurisdiction over ISPs' privacy practices to the FTC. Once this occurs, the FTC will again be able to take the lead in setting federal privacy policy for all entities participating in the Internet ecosystem.

Consistent with this action, the FCC should also make explicitly clear that, because BIAS is an interstate information service, state rules and regulations for BIAS that are inconsistent with federal policy governing the regulation of ISPs' privacy practices are preempted. This would not mean that generally-applicable consumer protections — like state data breach notification laws — would not apply; rather, it would mean only that states could not impose *ISP-specific* requirements in an attempt to undo or otherwise circumvent federal law and policy. A patchwork of ISP privacy regulations at

---

[12] *See, e.g.*, PETER SWIRE & KENESA AHMAD, FOUNDATIONS OF INFORMATION PRIVACY AND DATA PROTECTION: A SURVEY OF GLOBAL CONCEPTS, LAWS, AND PRACTICES (2012), at 76 ("The basic structure of fair information practices typically applies across… sectors, but the detailed rules and practices may vary.").

[13] CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY, *supra* note 7 at 29.

the state level would thwart the goal of having a unified privacy framework for ISPs that is consistent with the framework for all other participants in the Internet ecosystem.

I. There is no basis for treating ISPs differently than the rest of the online economy with respect to privacy

Key to properly regulating ISPs' and edge providers' collection and use of personal information is the reality that, in the truly relevant market — the market for advertising and data analytics — the distinction between edge and network is unimportant, and competition abounds.

In the proper market — the market for informatics and advertising — ISPs are upstarts challenging the dominant position of firms like Google and Facebook. Placing uniquely onerous restrictions upon ISPs alone would result in either under-regulation of edge providers or over-regulation of ISPs within the advertising market, without any clear justification as to why consumer privacy takes on different qualities for each type of advertising platform.

This would (as the *2016 Privacy Order* did) create a barrier to competition by ISPs in other platform markets, without offering a defensible consumer protection rationale to justify either the disparate treatment or the restriction on competition.[14] Indeed, the paucity of evidence and analysis of the competitive dynamics of the advertising and broader informatics markets should have been fatal out of the gate to the *2016 Privacy Order*'s approach.

A. ISPs do not present a unique threat

It is incumbent upon proponents of privacy regulation, and especially *differential* regulation, to justify any particular proposed regime with evidence that demonstrates that consumer privacy, consumer welfare, and the public interest will be served. That showing has not been made with respect to ISPs.

First, even leaving aside this broader, combined market for the moment, the logic of the previous Commission's approach to broadband privacy regulation fails on its own terms. The Commission's approach — as well as that of a number of the commenters supporting it — reflected an unsubstantiated belief that ISPs present a unique (and uniquely substantial) threat to privacy, necessitating particular (and particularly onerous) regulation by the FCC. Public Knowledge and its co-authors, for example, claimed that

[14] *See, e.g.*, Comments of the International Center for Law & Economics and Scholars of Law & Economics, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106 (May 27, 2016) at 12-20, *available at* https://www.fcc.gov/ecfs/filing/60001975214/document/60002081125 [hereinafeter, "ICLE 2016 Privacy Comments"].

> BIAS providers are gatekeepers to the Internet. This position is unique to BIAS providers, and carries substantial implications for consumers, as the Commission has previously recognized. While traffic splinters among providers at the edge, all data — sensitive, non- sensitive, and everything in between — must pass through the hands of an ISP....
>
> The different ways that broadband providers can exploit the information that consumers must expose as part of receiving service — as well as the certainty that the most sensitive information will flow over the network — justify Congress' decision to design unique privacy protections for common carriers. As Senator Leahy recently noted in a letter to the Commission, "[t]he patchwork of state privacy laws and Federal Trade Commission enforcement are not adequate protections" for consumers.[15]

These breathless claims are inaccurate, however, and they are insufficient to justify disparate, more-invasive regulation for ISPs. As Howard Beales and Jeff Eisenach (among many others) have observed, "it is far from obvious which firms or types of firms currently have the most comprehensive view of consumers' online activities."[16] Further,

> consumers' access to the Internet is fragmented across multiple channels, meaning that no online service provider is in a position to collect a comprehensive record for any significant proportion of consumers, and there is no qualitative difference between the comprehensiveness of data available, for instance, to ISPs and what can be and is collected by other types of firms, such as firms that provide as search engines, browsers, operating systems and social media platforms, as well as data brokers and large advertising networks. Equally important, technologies and market conditions are constantly evolving. Thus, any attempt to categorize particular providers as uniquely engaged in "comprehensive data collection" about consumers' online activities would quickly prove outdated.[17]

Numerous limitations exist — and doubtless many more will continue to evolve in the market — upon ISPs' ability to access private data: increasingly popular encryption, multiple connections between work and home, and a shift to mobile apps all work to frustrate data gathering efforts.[18]

Second, even if ISPs have access to *some* unique data from which they can draw unique insights about consumers, they are still at a significant competitive disadvantage in the relevant (advertising)

---

[15] Comments of Public Knowledge, The Benton Foundation, Consumer Federation of American, and National Consumers League, *In the Matter of Protecting the Privacy of Consumers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106 at 3-4 (May 27, 2016), *available at* https://ecfsapi.fcc.gov/file/60002080037.pdf [hereinafter, "PK 2016 Privacy Comments"].

[16] Howard Beales and Jeffrey A. Eisenach, *Putting Consumers First: A Functionality-Based Approach to Online Privacy* 2 (Navigant Economics Paper, Jan. 2013), *available at* http://ssrn.com/abstract=2211540.

[17] *Id.*

[18] *See, e.g., id.*

(cont.)

market. Compared to ISPs, the scope of data available to edge providers is more pervasive, allowing them to gather data on users across devices and contexts.[19] True, all of these companies, including ISPs, have the ability to collect and use consumer data. But they are limited by the market dynamics that constrain them, including from interactions with each other.[20]

And in order to make use of the data to which ISPs *do* have access, in such a competitive environment, they would have to offer unique, valuable insights to potential advertisers in order to overcome the substantial value that the dominant networks offer — networks that are able to derive unique insights thanks to an ability to track individual users across devices, websites, and locations — and without being hogtied by encryption.[21]

Of crucial importance, it is not enough to have *access* to data; rather, it must be competitively valuable in order to make its collection and processing worthwhile. But "ISPs in many instances have access to data that is less revealing than content or other information about user activity available to the companies providing services to the user."[22] While ISP data may, in some cases, be unique, it is not generally uniquely valuable, and thus competitive pressures may deter ISPs from expending resources to access and process it in the first place.

Unless ISPs can replicate the benefits derived from this highly valuable cache of data, advertisers would have no reason to favor ISPs over current, dominant networks. But large data sets are so often filled with meaningless noise that is by no certain that ISPs can gain profitable insights from their

---

[19] *See, e.g., Dynamic Ads*, FACEBOOK BUSINESS (last accessed Aug. 30, 2017), *available at* http://bit.ly/2mutoRO; Marcelo Ballvé and Emily Adler, *The Atlas Explainer: Where Facebook's Atlas ad server fits in the digital-ad ecosystem, and how it works*, BI INTELLIGENCE (Apr. 10, 2015), *available at* http://read.bi/2muwup2.

[20] It must be noted that, according to the flawed argument that ISPs are "gatekeepers," so too would be many edge providers. Indeed, according to some — including many supporters of ISP privacy rules — many edge providers' positions as data aggregators are both more substantial and less apparent to consumers (and therefore less likely to be checked by competition). Facebook and Google, for instance, are able to track users across the majority of the web, and to do so in ways that are both more comprehensive than ISPs and that, according to some, afford users less opportunity to "opt-out" through the use of alternatives. *See, e.g.,* TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES (2010). Even though these claims regarding edge providers are similarly flawed, it is not accurate to assert, as the Commission did in its *2016 Privacy NPRM*, that ISPs "have the ability to capture a breadth of data that an individual streaming video provider, search engine or even e-commerce site simply does not." *2016 Privacy NPRM*, at ¶ 1. All told, and despite the bluster of some commenters, ISPs do not have access to the scope of advertising-relevant data that ad networks and many e-commerce platforms have. *See, e.g.,* ICLE 2016 Privacy Comments, *supra* note 14.

[21] *See* Jules Polonetsky and Stacey Gray, *Cross Device: Understanding the State of State Management*, Future of Privacy Forum (Nov. 2015), *available at* https://fpf.org/wp-content/uploads/2015/11/FPF_FTC_CrossDevice_F_20pg-3.pdf.

[22] Reply Comments of Peter Swire & Justin Hemmings, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket 16-106 (Jul. 6, 2016) at 9 [*hereinafter* "Swire & Hemmings Reply Comments"].

(cont.)

data.[23] Far from being juggernauts of potential ad sales, ISPs are much more like market upstarts: new entrants that can bring valuable and potentially innovative competition to the advertising marketplace — but that are more likely never to succeed in the market at all.

Moreover, to the extent that "sufficient competition" is a touchstone for adequate privacy protection, the Commission has not, to our knowledge, actually evaluated the extent of competition in the relevant markets, nor actually determined whether ISPs face more or less competition along the relevant dimensions than do, say, Google and Amazon.[24]

B. Broadband is sufficiently competitive to protect consumer choice, and getting more competitive by the day

Advocates of rules consistent with the Commission's *2016 Privacy Order* (to the extent permitted under the CRA) also proffer the misguided argument that there is less — and insufficient — competition in the broadband industry, which restricts consumers' choices and permits ISPs to abuse consumer data with impunity.[25] According to the *2016 Privacy Order* (citing the 2015 Open Internet Order), "[w]hile some customers can switch BIAS providers…, [b]roadband providers have the ability to act as gatekeepers even in the absence of 'the sort of market concentration that would enable them to impose substantial price increases on end users.'"[26] Yet in reality there is little indication that broadband access is lacking adequate competition, and strong indication that both current access and future development will ensure sufficient competition to protect privacy-sensitive consumers (assuming there are in fact enough of them to justify the cost of ISPs adopting different access models at all).[27]

---

[23] *See, e.g.*, James Glanz, *Is Big Data a Big Dud?*, NEW YORK TIMES (Aug. 17, 2013), *available at* http://www.nytimes.com/2013/08/18/sunday-review/is-big-data-an-economic-big-dud.html.

[24] *See generally* Peter Swire, Justin Hemmings & Alana Kirkland, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, Institute for Information Security & Privacy at Georgia Tech (May 2016), *available at* http://bit.ly/2lvRtsj [hereinafter "*Online Privacy And ISPs*"].

[25] *See, e.g.*, Open Technology Institute, *The FCC's Role in Protecting Online Privacy: An Explainer* 2, 3 (Jan. 2016) (characterizing ISP's as "gatekeepers" that "face little competition"), *available at* http://bit.ly/2lNRDXa.

[26] *2016 Privacy Order* at ¶ 36 (citations omitted).

[27] *Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable & Timely Fashion, & Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act*, 2015 Broadband Progress Report, 30 F.C.C. Rcd. 1375 (2015) [*hereinafter* "*2015 Broadband Progress Report*"]. The Commission, of course, changed the threshold for "broadband" access to 25 Mbps download speed in 2015, instantly wiping out some of this competition (on paper). But, presumably, for privacy-sensitive consumers, the possibility of a more protective ISP even at slightly slower speeds (in any case, well above those needed for the vast majority of Internet uses) would make 10 Mbps and 25 Mbps networks more directly competitive.

(cont.)

As of 2014, over 74% of homes had access to at least two wired ISPs able to deliver 10 Mbps download speed, and over 88% had access to at least two providers delivering 3 Mbps service.[28] Meanwhile, over 93% of consumers have access to at least three mobile broadband providers.[29] Looking forward, consumer choice at all download speeds is increasing at rapid rates due to extensive network upgrades and new entry in a highly dynamic market.[30]

The reasoning offered in the *2016 Privacy Order* to impose special rules rested, crucially, on the assertion that "BIAS providers are not, in fact, the same as edge providers in all relevant respects."[31] To support this claim, the Order repeatedly cited various commenters who claimed that ISPs have ***the ability*** to combine consumer data and Internet usage history into a "very unique, detailed and comprehensive view of their users."[32] The FCC used this language to make its case that ISPs' collection and use of consumer data creates unique concerns, that they should thus be regulated differently (and more onerously), and that doing so was consistent with the FTC's approach:

> While we recognize that there are other participants in the Internet ecosystem that can also see and collect consumer data, the record is clear that BIAS providers' gatekeeper position allows them to see every packet that a consumer sends and receives over the Internet while on the network, including, absent encryption, its contents.[33]

As we discuss in more detail below, the *2016 Privacy Order* was, in fact, *inconsistent* with the FTC's approach.[34] Moreover, ISPs' access to sensitive data is not unique, and, contrary to the *2016 Privacy Order*'s cherry-picked assertions, the latest comprehensive analysis suggests that ISPs' access is *more limited* than that of many edge providers.[35] Having "some" access is very different than having "comprehensive" access.

The claim that ISPs, uniquely among companies in the modern data economy, face insufficient competition in the broadband market is, as noted above, insufficiently supported.

---

[28] *Id.* at ¶ 83.

[29] *In re Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993: Annual Report and Analysis of Competitive Market Conditions with Respect to Mobile Wireless*, Seventeenth Report, 29 F.C.C. Rcd. 15311, at ¶ 51, Chart III.A.2 (2014).

[30] *See, e.g.*, Will Rinehart, *FCC Data Suggests Broadband Inequality Has Decreased* (May 11, 2017), *available at* https://www.americanactionforum.org/research/fcc-data-suggests-broadband-inequality-decreased/.

[31] *2016 Privacy Order* at ¶ 35; *see generally id.* at ¶¶ 28-37.

[32] *See, e.g., id.* at ¶ 32.

[33] *Id.* at ¶ 30.

[34] *See infra* Section II.B.

[35] *See Online Privacy And ISPs*.

(cont.)

The flawed manner in which the Commission has defined the purported relevant market for broadband distorts the analysis upon which the *2016 Order* was based, and manufactures a false scarcity in order to justify unduly burdensome regulations for ISPs. Even the Commission's own data suggest that consumer choice is alive and well in broadband. In 2010 the Commission observed that one sixth of customers switch broadband providers each year, and over a third switch every three years.[36] And on the wireless side, carriers experience an annual churn rate of between 12% and 24%,[37] while simultaneously adding on the order of 18 million new connections each year[38] — indicating that consumers readily switch wireless providers when it suits them.

The reality is that there is in fact enough competition in the broadband market to offer privacy-sensitive consumers options if they are ever faced with what they view as overly invasive broadband business practices.

And it still remains to be seen whether 25 Mbps — the arbitrary threshold selected by the Commission to define high-speed broadband — should be used as a benchmark. According to the *2015 Broadband Report*, less than 30% of all customers who were offered 25 Mbps service actually ordered it, a fact that suggests that the demand for this level of service may not actually have reached critical mass.[39] It is thus unsurprising that there has not been a ubiquitous rollout of 25 Mbps service when the revealed preference of over 70% of consumers indicates that such a service would be dramatically under-used.

The crabbed market descriptions that gives rise to the claims of insufficient competition also ignore the growth of wireless-only homes, which accounted for 13% of households in 2015.[40] But advertisers — a major driver of revenue online — have noticed this shift: By 2018 it is expected that mobile advertising revenue will outstrip fixed broadband advertising.[41]

---

[36] See Federal Communications Commission, *Broadband Decisions: What Drives Consumers to Switch – or Stick With – their Broadband Internet Provider* (2010) *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-303264A1.pdf.

[37] *In the Matter of Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, Annual Report and Analysis of Competitive Market Conditions With Respect to Mobile Wireless Including Commercial Mobile Services*, Eighteenth Report, WT Docket No. 15-125, at ¶ 20 (Feb. 24, 2015), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DA-15-1487A1.pdf.

[38] *Id.* at ¶ 18

[39] *2015 Broadband Progress Report* at ¶ 41.

[40] John B. Horrigan & Maeve Duggan, *Home Broadband 2015*, PEW RESEARCH CENTER (Dec. 21, 2015), *available at* http://www.pewinternet.org/2015/12/21/1-home-broadband-adoption-modest-decline-from-2013-to-2015/.

[41] Mark Hoelzel, *Mobile advertising is exploding and will grow much faster than all other digital ad categories*, BUSINESS INSIDER (Apr. 3, 2015) *available at* http://www.businessinsider.com/mobile-is-growing-faster-than-all-other-ad-formats-2014-10/.

And it is even easier for privacy-sensitive consumers to switch among wireless carriers. Many carriers will offer to buy out consumer contracts with competitors in order to attract new customers. Further, wireless consumers are significantly less limited by geography than are traditional fixed-broadband consumers; acquiring a new provider is as easy as signing up for new service, and consumers are able to retain those services as they move to new locations.

Moreover, it is important to remember that ISPs make decisions relating to investment, services offerings, etc. on the margins. Thus, even if a majority of consumers do not in fact have any incentive to switch providers in order to avoid collection of their data, the existence of even a critical number of consumers who *would* make that switch will operate as a constraint on ISPs that prevents them from engaging in harmful practices.

In short, proponents of special ISP privacy rules at the FCC fail to make out a coherent defense of their need based on the extent of broadband competition. Further, because of this competition, the market is likely robust enough to support a range of business models, from highly privacy-sensitive, fee-based services to the very common edge-provider model of subsidized or free access in exchange for use of consumer information.

II. The Failings of the FCC's *2016 Privacy Order*

A. The *2016 Privacy Order* did not evince understanding of the market

The *2016 Privacy Order*'s most basic claims purporting to differentiate ISPs from edge providers were paradigmatic examples of the misleading use of statistics.

First, the *2016 Privacy Order* asserted that ISPs "see every packet that a consumer sends and receives over the Internet while on the network, including, absent encryption, its contents."[42] Perhaps that is true "while on *the* network," but users rarely remain on a single network, and, just as they "multi-home" between multiple edge providers, they also move between ISPs throughout the day and over time.

[42] *2016 Privacy Order* at ¶ 30.

(cont.)

Moreover, despite its appendage by the *2016 Privacy Order* as if an afterthought, "absent encryption" describes a small and rapidly disappearing proportion of Internet traffic.[43] Put most charitably, the *2016 Privacy Order* relied on outdated data in order to claim that encryption was insignificant.[44]

The *2016 Privacy Order* then asserted that:

> By contrast, edge providers only see a slice of any given consumers Internet traffic. As explained in the record, edge providers' visibility into consumers' web browsing activity is necessarily limited. According to the record, only three companies (Google, Facebook, and Twitter) have third party tracking capabilities across more than 10 percent of the top one million websites, and none of those have access to more than approximately 25 percent of web pages.[45]

In truth, edge provider visibility *is*, of course, necessarily limited — but not by much. The assertion that companies like Google, Facebook and Twitter "have access to [no] more than approximately 25 percent of web pages" is disturbingly misleading, and dangerously close to an outright fabrication. The *fraction of all webpages* tracked is not the relevant metric in the slightest; rather, the *share of user visits* is. Thus, for example, the top 10 websites (an infinitesimal fraction of the total number of web pages) alone account for 33 percent of US website visits.[46] And in terms of visits (each of which has the potential to generate possible private data):

> There are over 1.1 billion websites on the internet, but the vast majority of all traffic actually goes to a very select list of them… The dropoff from [just] #1 to #100 is significant. Google.com has 28 billion visits, but a website like Citi.com (ranked #98) only has 53 million visits a month. That's a 500x difference!"[47]

Virtually all (if not all) of the top sites are tracked (most are *owned*, in fact) by the largest online platforms, and virtually all of them use encryption by default. On this measure, the ability of social media, search and e-commerce companies to track behavior and access data surely comprises an

---

[43] In just the time since the Order was drafted, the share of "top 100" sites with HTTPS encryption by default has gone from 21 percent to almost 40 percent, and 50 percent use HTTPS, either by default or after login. *Compare HTTPS on Top Sites*, GOOGLE TRANSPARENCY REPORT (last visited Aug. 26, 2017), https://www.google.com/transparencyreport/https/grid/, *with* Brian Barrett, *Most Top Websites Still Don't Use a Basic Security Feature*, WIRED (Mar. 17, 2016), https://www.wired.com/2016/03/https-adoption-google-report/. *See also Online Privacy and ISPs* at 36 ("All of the top 10 sites… [and] 42 of the top 50 sites either use HTTPS by default or shift to HTTPS when the user logs-in… [and] 24 of the top 50 sites use HTTPS by default, even without user log-in.").

[44] *See, e.g.*, Swire & Hemmings Reply Comments at 3-5.

[45] *2016 Privacy Order* at ¶ 30.

[46] *Most popular websites in the United States as of February 2016, based on share of visits*, STATISTA (last visited Aug. 28, 2017), http://bit.ly/2lTVXoR (based on calculations during the week ending February 27, 2016).

[47] Jeff Desjardins, *The 100 Websites That Rule the Internet*, VISUAL CAPITALIST (Mar. 7, 2017), http://www.visualcapitalist.com/100-websites-rule-internet/.

(cont.)

overwhelming share of the web — and not surprisingly, of course: These companies have an interest in prioritizing the tracking of the most trafficked websites.

When misleading, non-evidence "evidence" is offered as the only basis for a claim, there is reason to suspect that the actual evidence to support the contention simply doesn't exist.[48]

Similarly, on the basis of mere unsupported assertions by commenters, the *2016 Privacy Order* made a number of questionable, if not outright false, claims about ISPs' allegedly exceptional ability to view consumers' data.[49] In fact, non-ISP information collection practices are frequently far more robust than those of ISPs.

As Peter Swire and coauthors note, "ISP access to user data is not *comprehensive* — technological developments place substantial limits on ISPs' visibility. Second, ISP access to user data is not *unique* — other companies often have access to more information and a wider range of user information than ISPs."[50] Compared to their edge-provider analogues, ISPs do not have particularly broad insight into consumer data that is not given to them in the course of subscribing.[51]

B. The FCC's 2016 approach did not mirror the FTC's approach

Among other things, the FCC's *2016 Privacy Order* imposed an opt-in requirement on ISPs without any meaningful evidence of harm or rigorous economic analysis of consumer welfare effects. Even as it *acknowledged* that opt-in may impose more cost, the Order never adequately addressed the trade-offs.[52] It also contemplated a significant expansion of what constitutes "sensitive" information requiring "opt-in" consent, well beyond what the FTC's framework embodies (and well beyond what the statute authorizes). And although it paid lip service to the possible benefits to consumers from ISPs' expanded use of data, it in fact addressed potential ISP use of data-sharing in exchange for

---

[48] As Commissioner O'Rielly noted:

> Now, today's *Order* tries to justify this new and complex approach by arguing that ISPs and edge providers see vastly different amounts of your online data. It recounts what it says is a vast sea of data that ISPs obtain. It then says that "By contrast, edge providers only see a slice of any given consumers Internet traffic." A "slice." Really? The era of Big Data is here. The volume and extent of personal data that edge providers collect on a daily basis is staggering. But because the *Order* wants to treat ISPs differently from edge providers, it asserts that the latter only sees a "slice" of consumers' online data. This is not data-driven decision-making, but corporate favoritism.

Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Notice of Proposed Rulemaking, Dissenting Statement of Commissioner Michael O'Rielly, WC Docket 16-106 (rel. Apr. 1, 2016).

[49] *See, e.g., 2016 Privacy Order* at n. 56, ¶ 29, and ¶ 33.

[50] *Online Privacy and ISPs* at 7.

[51] *See id.* at 23.

[52] *2016 Privacy Order* at ¶ 386 ("Although we recognize that opt-in imposes additional costs, we find that opt-in is warranted to maximize opportunities for informed choice about sensitive information.")

(cont.)

consumer discounts in a mere six paragraphs,[53] inexplicably adopting "heightened disclosure and choice requirements" (including opt-in consent)[54] that are at squarely odds with the FTC's approach in such circumstances.[55]

In these ways (as in others), the Order deviated from the FTC's data privacy regime. The FTC's 2012 Privacy Report, upon which the Order purported to rely as a guide for its rules,[56] tempers its concern that ISPs' have an exceptional ability to collect information, noting, with a nuance lacking in the *2016 Privacy Order*, that:

> [A]ny privacy framework should be technologically neutral. ***ISPs are just one type of large platform provider that may have access to all or nearly all of a consumer's online activity***. Like ISPs, operating systems and browsers ***may*** be in a position to track all, or virtually all, of a consumer's online activity to create highly detailed profiles.[57]

Taken as whole, the FTC's Privacy Report does not establish the proposition that ISPs should be held to a higher (or even a different) standard of regulation than edge providers.[58]

Rather than adopt the standards enforced by the FTC under Sections 5(a) and (n) of the FTC Act, import the FTC's Unfairness Policy Statement, and commit to the FTC's case-by-case approach to privacy enforcement, the Commission sought to impose a prescriptive privacy regime upon a small segment of the Internet ecosystem that is nowhere else replicated in the federal regulatory regime.

There is a world of difference between a regulatory regime based on suggested best practices, industry codes of conduct and overarching consumer protection standards in which businesses are free to

---

[53] *Id.* at ¶ 298-303.

[54] *Id.* at ¶ 301.

[55] *See* Statement of FTC Commissioner Maureen K. Ohlhausen Regarding Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106 (May 27, 2016) at 3 (noting the inconsistency and further noting that "the [FTC Privacy Report] observed [that] 'big data can create opportunities for low-income and under-served communities,' and cites a broad range of existing examples"). The *2016 Privacy Order* briefly acknowledged possible benefits but then adopted its "heightened" approach based solely on the *possibility* that the practice *may* present "possible benefits and harms." *2016 Privacy Order* at ¶ 301.

[56] *Id.* at ¶ 9 ("In adopting rules governing customer choice, we look to the best practices framework recommended by the FTC in its 2012 Privacy Report as well as the choice framework in the Administration's CPBR and adopt a framework that provides heightened protections for sensitive customer information.")

[57] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 26, 2012) at 56, *available at* http://go.usa.gov/csYRz (emphasis added) [*hereinafter* FTC Privacy Report].

[58] *Id. See also* Letter of Jon Leibowitz to the FCC, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106 (May 23, 2016) at 7.

(cont.)

experiment and compete within the general limits of "transparency, choice and data security,"[59] and a prescriptive regime that pays lip service to such standards but imposes aggressive constraints that fundamentally limit competition and choice.

1. Opt-in

The *2016 Privacy Order* deviated significantly from the FTC's regime by adopting "opt-in" requirements in multiple places and for a significantly expanded class of data — despite the fact that "'[o]pt-in' provides no greater privacy protection than 'opt-out' but imposes significantly higher costs with dramatically different legal and economic implications."[60] In staunching the flow of data, opt-in regimes impose both direct and indirect costs on the economy and on consumers,[61] reducing the value of certain products and services not only to the individual who does not opt-in, but to the broader network as a whole. Not surprisingly, these effects fall disproportionately on the relatively poor and the less technology-literate.[62]

Furthermore, empirical research shows that opt-in privacy rules reduce competition by deterring new entry. Thus, the seemingly marginal costs imposed on consumers by requiring opt-in can have a significant cumulative effect on competition: "[R]ather than increasing competition, the nature of transaction costs implied by privacy regulation suggests that privacy regulation may be anti-competitive.... [I]n some cases where entry had been profitable without regulation, [some firms] will choose not to enter."[63]

For these reasons, when data usage is consistent with "the context of the transaction or the company's relationship with the consumer," *regardless of the sensitivity of the data involved*, the FTC does

---

[59] *2016 Privacy Order* at ¶ 5.

[60] Fred H. Cate and Michael E. Staten, *Protecting Privacy in the New Millennium: The Fallacy of "Opt-In"* at 1, *available at* http://bit.ly/2lvZ9uz ("[C]onsider the experience of U.S. West, one of the few U.S. companies to test an 'opt-in' system. In obtaining permission to utilize information about its customer's calling patterns... the company found that an 'opt-in' system was significantly more expensive to administer, costing almost $30 per customer contacted."). *See also* Nicklas Lundblad and Betsy Masiello, *Opt-in Dystopias*, 7 SCRIPTED 155 (Apr. 2010), *available at* http://bit.ly/2lvKy2s.

[61] *Id.* at 5 ("[T]he 'opt-out' system sets the default rule to 'free information flow' and lets privacy-sensitive consumers remove their information from the pipeline. In contrast, an 'opt-in' system presumes that consumers **do not want** the benefits stemming from publicly available information, and thereby turns off the information flow, unless consumers explicitly grant permission to use the information about them.") (emphasis in original).

[62] *See, e.g.*, Lucas Bergkamp, *The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy*, 18 COMPUTER LAW & SECURITY REPORT 31, 38 (2002); *Opt-in Dystopias*, *supra* note 60, at § 5.1.

[63] James Campbell, Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Market Structure*, 24 J. ECON. & MGMT. STRATEGY 47, 48-49 (2015) (emphasis added).

(cont.)

not generally require choice (let alone affirmative consent) before a company collects or uses consumer data.[64] The sensitivity of the information is relevant only "[f]or practices requiring choice," meaning those that fall outside the context of the transaction.[65] For these uses, the FTC requires "affirmative express consent" (opt-in consent) only for uses of sensitive data.[66]

2. *Consumer expectations*

Despite its claims to the contrary, however,[67] the *2016 Privacy Order* ignored this critical component of the FTC's framework by focusing solely on the sensitivity of data, while virtually completely overlooking the context in which it was used. Instead, the Order claimed that "incorporating a sensitivity element into our framework allows our rules to be more properly calibrated to customer and business expectations. This approach is also consistent with the framework recommended by the FTC in its comments and its 2012 staff report."[68] But this is actually *inconsistent* with the FTC's approach. In fact, the FTC's framework explicitly *rejects* a "consumer expectations" standard: "Rather than relying solely upon the inherently subjective test of consumer expectations, the [FTC's] standard focuses on more objective factors related to the consumer's relationship with a business."[69]

Chairman Wheeler's "consumer expectations" framing, by contrast, was a transparent attempt to *claim* fealty to the FTC's well-developed standards while actually *implementing* a privacy regime that was flatly inconsistent with those standards.

The FTC's approach is an appropriately flexible one, aimed at balancing the immense benefits of information flows with sensible consumer protections. Thus it eschews an "inflexible list of specific practices" that would "risk[] undermining companies' incentives to innovate and develop new products and services...."[70]

Instead, the FTC's framework begins by establishing a sort of "safe harbor" for data use where its benefits may be presumed to exceed its costs and consumer consent may be inferred:

---

[64] FTC Privacy Report at 48.

[65] *Id.* at 60.

[66] *Id.*

[67] *2016 Privacy Order* at ¶ 173.

[68] *Id.*

[69] FTC Privacy Report at 38.

[70] *Id.* Nevertheless, the FTC does identify certain "illustrative" categories of interactions that would "not typically require consumer choice," including "fulfilment, fraud prevention, internal operations, legal compliance and public purpose, and most first-party marketing...." *Id.* at 39.

(cont.)

> Companies do not need to provide choice before collecting and using consumer data for practices that are consistent with the context of the transaction or the company's relationship with the consumer....[71]

To the limited extent that the *2016 Privacy Order* identified any categories of uses from which it would have inferred consent, by contrast, it adopted the "inflexible" approach that the FTC was expressly trying to avoid: a mechanical, "bright-line standard that freezes in place current practices and potentially could harm innovation and restrict the development of new business models."[72]

Not only did the *2016 Privacy Order* limit inferred consent to a narrow set of "Congressionally-Recognized Exceptions,"[73] but arguably these contemplated a smaller scope of activity than even the FTC's *illustrative* examples. While the *2016 Privacy Order* purported to incorporate implied consent for functions "necessary to, or used in, the provision of" broadband service,[74] it employed the agency's discretion to interpret the statute in such a way to narrow the scope of these allowable functions considerably beyond those contemplated by the FTC. Thus, for example, although the *2016 Privacy Order* included some first-party marketing within the scope of implied consent, it limited it (without sufficient) to services already purchased or "commonly bundled together with the subscriber's telecommunications service."[75]

In short, the *2016 Privacy Order* did not heed the FTC's call for humility and flexibility regarding the application of privacy rules to ISPs (and other Internet platforms):

---

[71] *Id.* at 48. The framework does *also* infer consent when practices "are required or specifically authorized by law." *Id.*

[72] *Id.* at 36.

[73] *2016 Privacy Order* at ¶¶ 10, 201-220. *See also* 47 U.S. Code §§ 222(c)(1) & (d).

[74] *Id.* at ¶ 201.

[75] *2016 Privacy Order* at ¶ 199-200, 204. By contract, the FTC identifies most first-party marketing as a use "consistent with the context of the transaction," and thus not requiring consent. The FTC does note that companies should enable opt-in consent for the use of *sensitive data* in first-party marketing (as did the FCC) — but, for the FTC, even this limitation is flexible. The FTC Privacy Report notes that "the risks to consumers may not justify the potential burdens on general audience businesses that *incidentally collect* and use sensitive information," for example. FTC Privacy Report at 46-47 (emphasis in original). Moreover, and tellingly, the FTC notes a specific exception from inferred consent for ISPs *using deep packet inspection* for marketing purposes — although, even then, it recommends only some opportunity for choice, and not necessarily affirmative consent. FTC Privacy Report at 40-41 & 56. The implication is clear, however: ISPs' first-party marketing that does *not* use deep packet inspection does *not* automatically trigger a choice obligation under the FTC's framework. The 2016 Privacy Report, by contrast, adopts a much more rigid and detailed set of constraints. *See also Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Notice of Proposed Rulemaking,* Dissenting Statement of Commissioner Michael O'Rielly, WC Docket 16-106 (rel. Apr. 1, 2016) ("In another departure from the FTC framework and widespread consumer expectations, the order limits inferred consent [with respect] to first party marketing.... Here again, there is no rational reason to place undue restrictions on broadband providers.").

(cont.)

> These are complex and rapidly evolving areas, and more work should be done to learn about the practices of all large platform providers, their technical capabilities with respect to consumer data, and their current and expected uses of such data.[76]

3. Other categories of data

As noted, under the FTC's regime, the sensitivity of data matters essentially only for transactions inconsistent with context. But the FTC's approach contemplates a further distinction, between data uses that require "express affirmative" (opt-in) consent and those that do not (requiring only "other protections" short of opt-in consent[77] — *e.g.*, opt-out). In the FTC's framework, it is *this* distinction that generally turns on the sensitivity of the data involved.

Because the distinction is so important — because opt-in consent is much more likely to staunch data flows — the FTC goes to great pains to provide guidance as to what data should be considered sensitive, and to cabin the scope of activities requiring opt-in consent. Thus, the FTC agrees that "information about children, financial and health information, Social Security numbers, and precise geolocation data [should be treated as] sensitive."[78] Beyond those instances, however, the FTC does not consider any other type of data as inherently sensitive.[79]

By contrast, and without explanation, the *2016 Privacy Order* added to this list several additional categories of information. In particular, it designated "web browsing histories," "application usage histories," and "content" as sensitive data.[80] Treatment of these categories of information as sensitive and requiring opt-in consent is flatly inconsistent with the FTC's approach and would deter consumer-welfare-enhancing uses of data.[81]

---

[76] FTC Privacy Report at 56.

[77] *Id.* at 60.

[78] *Id.* at 59.

[79] It should be noted that the FTC Privacy Report would also impose an opt-in requirement when companies adopt "material retroactive changes to privacy representations." *Id.* at 57-58.

[80] *2016 Privacy Order* at 167.

[81] *See, e.g.*, Comments of the International Center for Law & Economics and Scholars of Law & Economics, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106 (May 27, 2016) at 12-20, *available at* https://www.fcc.gov/ecfs/filing/60001975214/document/60002081125.

Nor is this result required by the statute. Seemingly, even for those uses of information that the statute specifically authorizes only "with the approval of the customer," it requires opt-in consent only for disclosure of proprietary information to third-parties. The basic rule in § 222(c)(1) is that disclosure or use is limited "[e]xcept as required by law **or with the approval of the customer**" (emphasis added). But "approval of the customer" is not necessarily "affirmative express consent," and can be effected by notice and *non-choice* — *i.e.*, by an informed consumer's decision not to opt-out. By contrast, § 222(c)(2) requires that "[a] telecommunications carrier shall **disclose** customer proprietary network information, **upon affirmative written request by the customer**, to any person designated by the customer" (emphasis added). Although this is couched in terms of a provider's obligation to share information when a (cont.)

It is telling that when the FTC sought public input on its own privacy framework, *only a single commenter* would have "characterized as sensitive information about consumers' online communications or reading and viewing habits."[82] The FTC explicitly rejected this suggestion.

Instead, the FTC treats web browsing history as information that raises "special concerns," often requiring some form of consumer *choice*, but not as sensitive information requiring *opt-in consent*.[83] Similarly, nothing in the FTC Privacy Report (or elsewhere) suggests that "app usage history" or "the content of communications" should necessarily be treated as sensitive or encumbered by opt-in requirements.

In fact, to the extent that the FTC has supported the use of do not track (DNT) mechanisms (for both web browsing,[84] as well as app usage[85]) in order to provide consumers some choice regarding use of their web browsing and app usage histories, it recommends DNT only in the form of consumer *opt-out*, not opt-in, and only when inconsistent with context.[86]

By treating virtually *all* useful information accessible by ISPs as "sensitive,"[87] and by making the sensitivity of data the primary determinant for opt-in consent, the *2016 Privacy Order* would have dramatically expanded the constraints on data collection and usage for ISPs well beyond those espoused by the FTC — without any evidence of a corresponding benefit.

C. The *2016 Privacy Order* fetishized technical possibilities without actually considering market realities

To begin with, the FCC made clear throughout the Order that its initial acknowledgement that privacy protections and innovation may be at odds was an empty one. Instead, the FCC fell back on

---

customer requests it, it also indicates that Congress was fully cognizant of the different degrees of consumer consent, and saw fit to impose a heightened, affirmative consent standard only in the case of disclosure, rather than first-party use.

[82] FTC Privacy Report at 59 (citing to Comment of Electronic Frontier Foundation, cmt. #00400, at 7).

[83] Such usage is discussed not in the section of the Report on "Practices Requiring Affirmative Express Consent," IV.C.2.e, but rather in the section on "Large Platform Providers That Can Comprehensively Collect Data Across the Internet Present Special Concerns," IV.C.2.d. *See id.* at 41.

[84] *Id.* at 52-55.

[85] *See* FTC Staff Report, *Mobile Privacy Disclosures: Building Trust Through Transparency* (2013) at 20-21, *available at* https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf [hereinafter "FTC Staff Mobile Privacy Report"].

[86] FTC Privacy Report at 53 ("[A]n effective Do Not Track system should… [enable consumers to] opt out of collection of behavioral data for all purposes other than those that would be consistent with the context of the interaction…"); FTC Staff Mobile Privacy Report at 21 (adopting the DNT standards described in the FTC Privacy Report).

[87] *2016 Privacy Order* at ¶ 167.

(cont.)

the faulty logic of the Open Internet Order's "virtuous circle" to claim, in effect, that only regulation could preserve the Internet's immense success:

> The risk of privacy harms directly affects behavior and activity by eroding trust in and use of communications networks. As the Commission has found, if "consumers have concerns about the privacy of their personal information, such concerns may restrain them from making full use of broadband Internet access services and the Internet, thereby lowering the likelihood of broadband adoption and decreasing consumer demand."[88]

In a microcosm of the poverty of the "virtuous circle" theory, that section of the Open Internet Order, in turn, cited to a Pew study that claims that, of the 15 percent of American adults who didn't use the Internet in 2013, three percent pointed to "worried about privacy" as their main reason for not doing so.[89] Six percent, however, pointed to "too expensive" as their main reason[90] — something that could only have been *exacerbated* by the Order. The notion that mitigating (in theory) a problem impeding three percent of users while exacerbating a problem that impedes six percent will *increase* consumer demand is an absurd one, of course.

Further emblematic of the Order's lack of careful analysis, the Order asserted that "requiring opt-in approval for the use and sharing of sensitive customer PI reasonably balances burdens between carriers and their customers."[91] Yet this assertion was made without pointing to any cost-benefit analysis indicating whether, as an *ex ante* rule, it makes sense in every case to impose notice requirements between ISPs and consumers. To point out just one problem with this approach, it is well known in the literature that consumers often suffer from "information overload"[92] such that it will not always be frictionless — or, on net, helpful — for consumers to be aware of the "costs and benefits of participation in these programs." Instead, in many cases, consumers will evaluate the services of ISPs *as a whole*, treating their privacy — which for different consumers will have a different value — as just one component of their relationship with an ISP which includes, among other things, convenience, overall cost, speed, and reliability.

Moreover, the Order would have harmed consumers who do not view privacy protections through the same, maximalist lens as the Commission. The net result of the rules would have been that, on the margin, consumers would be presented with a narrower range of pricing and product options,

---

[88] *2016 Privacy Order* at ¶ 380 (quoting *Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5821, ¶ 464 (2015)).

[89] *Who's not online and why,* PEW RESEARCH CENTER (Sep. 2013) at 2, *available at* http://pewrsr.ch/2lO0gks.

[90] *Id.*

[91] *2016 Privacy Order* at ¶ 193.

[92] *See, e.g.,* Troy A. Paredes, *Blinded by the Light: Information Overload and Its Consequences for Securities Regulation*, 81 WASH. U. L. Q. 417 (2003).

(cont.)

meaning that fewer consumers — who have a wide range of heterogeneous preferences — would be offered their preferred options. Consumer welfare would consequently decrease.

It is possible that the privacy-sensitive among us might be willing to pay for ad-free (and other non-tracking) versions of today's apps and other online services (including, potentially, broadband access), just as it is possible that they would be willing to bear the cost of finding and using ad- and cookie-blockers. But most people prefer to access apps, content, and services for free,[93] and do not care much about privacy except with respect to the most sensitive information (e.g., healthcare data, children's educational records),[94] so long as the personal data they provide is secure and they get something of value in return.[95] The FCC's prescriptive and onerous rules simply did not address the heterogeneity of consumer preference and its effect on these markets.

III. Good reasons to avoid overregulation of ISP privacy

A. Data and dollars: Online business models aren't fixed

Commenters have also opined that it would be inappropriate for ISPs (as opposed to other companies with access to consumer data) to trade broadband access for the use of consumer information.[96] But there is no basis for this claim. Although ISPs may, in the past, have typically required cash payment for their services, there is simply no reason to think that this will — or should — persist as the dominant business model.[97] In fact, left with the freedom to innovate, it very well may be the case that ISPs discover some menu of different options that work for both a wider range of consumers and the ISPs. Such a menu could easily include the option of "paying" for broadband access via

---

[93] *See, e.g.*, Mary Ellen Gordon, *The History of App Pricing, and Why Most Apps are Free*, THE FLURRY BLOG (Jul. 18, 2013), http://bit.ly/2muGBdn.

[94] Thus certain sector-specific privacy regimes do impose opt-in requirements in certain cases. *See, e.g.*, 45 CFR 164.508 (HIPAA); 34 CFR 99.30 (FERPA). But these are outliers, and they arise in clearly exceptional areas. The sort of data with which the FCC is concerned are decidedly not of this sort.

[95] *See, e.g.*, Jens Grossklags & Alessandro Acquisti, *When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information*, *in* PROCEEDINGS OF SIXTH WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY (2007), *available at* http://weis2007.econinfosec.org/papers/66.pdf.

[96] *See, e.g.*, Comments of the American Civil Liberties Union, *In the Matter of Protecting the Privacy of Consumers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, at 6-7 (May 27, 2016), *available at* http://apps.fcc.gov/ecfs/document/view?id=60002089529.

[97] Further, ISPs *have* actually experimented with offering ad-supported, free service. In 1999, for example, NetZero made waves by announcing just such a service with its dial-up option. *See* Bob Sullivan, *Free Net access gains steam*, ZDNET (Feb. 9, 1999) *available at* http://www.zdnet.com/article/free-net-access-gains-steam/.

(cont.)

targeted advertising. If *both* consumers and ISPs are satisfied with such an arrangement, it would be the height of hubris for the Commission to declare such a business model unfit for consumers.[98]

Moreover, finding alternative revenue channels helps promote investment in broadband itself:

> For both the edge and the core… the common currency of the [Internet] is information — that is, the ability to collect, track and ultimately monetize a plethora of information to provide enhanced online experiences for consumers. Moreover, it is the ability to monetize information successfully that will encourage, at least in part, the investments by both the edge and core to support the [Internet].[99]

Without this monetization, ISPs face a possible revenue shortfall as a result of the increased commoditization of broadband instigated by the FCC's prior regulatory decisions.[100] And as even the Commission itself has observed, investment in infrastructure suffers when "service providers… cannot earn enough revenue to cover the costs of deploying and operating broadband networks, including expected returns on capital, [such that] there is no business case to offer broadband services."[101]

Data often powers commerce, especially online, as the NPRM recognizes: "[I]t is not unusual for consumers to receive perks in exchange for use of their personal information."[102] Some commenters clearly believe, however, that the trade-off of data for dollars is outside of consumer expectations when it comes to broadband access, despite the fact that "[i]n the broadband ecosystem, 'free' [or reduced price] services in exchange for information are common."[103]

The commonly employed, multi-sided platform model allows Internet users to access an enormous amount of content at zero nominal price. Nevertheless, the NPRM and many of the supporting comments appear to treat the use of consumer data to drive platform subsidization through ad sales

---

[98] On the Google Play Store, for example, over 90% of apps are nominally "free" to users and rely on data and advertising for revenue while less than 10% are subscription based without such tracking. *See API App Market Data*, 42 MATTERS (last accessed Aug. 27, 2017), *available at* https://42matters.com/app-market-explorer/android.

[99] George S. Ford & Lawrence J. Spiwak, *Information, Investment and the Internet of Everything*, US CHAMBER OF COMMERCE FOUNDATION (Sept. 22, 2015), https://www.uschamberfoundation.org/article/information-investment-and-internet-everything.

[100] *See* T. Randolph Beard, George S. Ford, Thomas M. Koutsky, & Lawrence J. Spiwak, *Network Neutrality and Industry Structure*, 29 HASTINGS COMM. & ENT. L.J. 149 (2007), *available at* http://www.phoenix-center.org/papers/CommEntNetworkNeutrality.pdf.

[101] FED. COMMC'N. COMM'N, CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN 136 (Mar. 16, 2010), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-296935A1.pdf.

[102] *2016 Privacy NPRM* at ¶ 242. The *NPRM* does also assert, however, that "it is not clear that consumers generally understand that they are exchanging their information as part of those bargains."

[103] *Id.*

(cont.)

as an unalloyed negative. But exchanging information that is used for advertising purposes for discounted or free products and services is common in the Internet ecosystem and has underwritten its development in significant ways. Not only is there no evidence that subsidizing content access has negative effects, studies on multi-sided platforms suggest that the very success of online platforms depends upon actually adding value for all participants, especially consumers.[104]

Online intermediaries (like Google, Amazon, etc.) use data collected from users to more effectively target advertisements. In order to be successful, users must value the services provided (including the advertisements) more than the cost they incur (which may include the psychic cost of trading personal information for access). Building a search engine, email service, or ISP is not costless. If a multi-sided platform cannot recoup costs by charging one side of the platform (e.g., advertisers), then it will charge another side of the platform (e.g., consumers). Far from helping those with less disposable income,[105] a rule like the one proposed by the FCC will likely harm them the most by inflating broadband access prices and precluding pricing models that could subsidize access pricing.

If ISPs opt for differentiated business models that include providing nominally "free" access in exchange for serving targeted ads to consumers, there is no reason to expect consumer harm. Similarly, despite the bare assertions of the NPRM's supporters that "consumer expectations"[106] do not include trading data for access, there is no reason to believe this to be true. Overall consumer welfare could easily increase as a result of ISPs shifting more of the cost of broadband access to advertisers by charging them more in exchange for more accurate consumer targeting.

---

[104] *See generally* DAVID S. EVANS, PLATFORM ECONOMICS: ESSAYS ON MULTI-SIDED BUSINESSES (2011), *available at* http://www.marketplatforms.com/wp-content/uploads/Downloads/Platform-Economics-Essays-on-Multi-Sided-Businesses.pdf.

[105] *See* PK 2016 Privacy Comment, *supra* note 15, at 32 ("We are deeply concerned about the effects of 'pay for privacy' regimes on minority communities, low income neighborhoods, the elderly, and other vulnerable groups. While the current availability of such service (namely AT&T's $30 per month "discount" gigabit service) is limited to middle- to high-income areas, such practices in low-income or other vulnerable communities could quickly become prohibitively priced. In households with low income elasticity, even moderate price discrimination between privacy and no-privacy offerings can become coercive inducements. Such inducements could force low-income consumers to choose between exercising their privacy rights, and having a broadband connection at all. This is a choice that no consumer should be required to make, particularly in light of the Commission's mission of universal access to broadband communications.").

[106] *See, e.g.*, *2016 Privacy NPRM* at ¶¶ 104-05 ("FTC best practices counsel that consumer choice turns on the extent to which the practice is consistent with the context of the transaction or the consumer's existing relationship with the business. Consistent with this and our existing rules, we propose that, except as permitted above in Part III.C.1.a, BIAS providers must provide a customer with notice and the opportunity to opt out before they may use that customer's PI, or share such information with an affiliate that provides communications-related services, to market communications- related services to that customer. We seek comment on this proposal… This approach is similar to the approach taken by our current Section 222 rules, and **we believe it is consistent with customers' expectations**.") (emphasis added).

(cont.)

The reliance on "consumer expectations," moreover, rests upon an imagined snapshot of reality held static. OTI argues, for instance, that

> The context in which broadband customers share private information with BIAS providers is specific and accompanied by cabined expectations: the customers share the information with BIAS providers to facilitate provision of a service for which they have contracted. The information is therefore most appropriately thought of as on loan to, rather than transferred to, broadband providers. OTI agrees with the FCC's characterization of private information shared by customers for the purpose of receiving broadband service as a "possession" belonging to the customer.[107]

OTI attempts to substitute its own judgment of what consumers (should) believe about their data for that of consumers themselves. And in the process it posits a "context" that can and will never shift as new technology and new opportunities emerge. Such a view of consumer expectations is flatly anti-innovation and decidedly anti-consumer, consigning broadband users to yesterday's technology and business models. The rule OTI supports could effectively forbid broadband providers from offering consumers the option to trade data for lower prices. The sad implication of this paternalistic impulse is that consumers are incapable of making choices about their own data, and are further incapable of revising their understanding of the bargains they make. The FCC should forcefully reject such a view.

Of course consumers *could* be harmed if they are not aware of the nature of this tradeoff, but such a speculative harm does not justify invasive rules that strongly deter such transactions entirely;[108] at most it justifies disclosure — notice and choice. And, given that some consumers remain without an Internet connection — many for reasons of price[109]— it remains at least a reasonable presumption that a reduced price service, subsidized by targeted advertising, would yield a net increase in consumer welfare.

Online business models are constantly in flux. Even otherwise-similar companies take different approaches to revenue generation. For instance, there are apps that are subscription-based and others

---

[107] Comments of New America's Open Technology Institute, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket 16-106, at 7 (Mar. 31, 2016), *available at* https://ecfsapi.fcc.gov/file/60002081381.pdf.

[108] As the FCC seems to recognize. *See 2016 Privacy NPRM* at ¶ 245.

[109] John B. Horrigan & Maeve Duggan, *Barriers to broadband adoption: Cost is now a substantial challenge for many non-users*, PEW RESEARCH CENTER (Dec. 21, 2015), http://www.pewinternet.org/2015/12/21/3-barriers-to-broadband-adoption-cost-is-now-a-substantial-challenge-for-many-non-users/.

(cont.)

that are ad-supported.[110] The same is true of email providers,[111] search engines,[112] and all manner of other content online.[113] Some popular companies started out without utilizing ads but developed strong advertising networks over time, and others started with an ad-supported model, but moved towards subscriptions. Still others use combinations of both models.[114] The idea that ISPs in particular should be locked into one model because it is how they have tended to operate in the past is completely at odds with the larger reality of the online economy.

B. Even where competition might be more limited, ISPs should not be discriminated against with more onerous rules

Not only has the Commission failed to offer any support for the idea that ISPs' use of data would change as a result of competition, a number of market realities undermine ISPs' ability to pervasively gather information on their users.

First, as Peter Swire has noted, the increasing prevalence of encryption correspondingly limits ISPs' access to much consumer data.[115]

Further, as users increasingly access the web through mobile devices, consumer data to which ISPs have access is curtailed. Mobile users overwhelmingly access online content through apps and not web pages.[116] Even without encryption on a mobile app, an ISP would have a steep hill to climb to piece together all of the data about users of apps. The reality, however, is that much of the mobile ecosystem is moving toward pervasive, end-to-end encryption, further frustrating any hope of data gathering that ISPs may have had.[117]

---

[110] *See, e.g.*, Ron Medlin, *How Do Apps Make Money: A Complete Guide to App Monetization*, ZAPPOROO (Mar. 14, 2016), https://zapporoo.com/blog/app-monetization-guide/.

[111] *See, e.g.*, Wikipedia, *Comparison of webmail providers*, https://en.wikipedia.org/wiki/Comparison_of_webmail_providers (as of Aug. 26, 2017 at 11:54 am).

[112] *Cf.* Google & Westlaw.

[113] *See, e.g.*, Wikipedia, *Website monetization*, https://en.wikipedia.org/wiki/Website_monetization (last visited Aug. 26, 2017).

[114] Medlin, *supra* note 110 ("Remember, these app monetization methods are not exclusive. You can combine two or more of them, or even change from one to another at a later date depending on what is working.").

[115] *Online Privacy and ISPs* at 7.

[116] Greg Sterling, *Apps Eat Digital Media Time, With Top 3 Capturing 80 Percent*, MARKETING LAND (Sep. 23, 2015), http://marketingland.com/apps-eat-digital-media-time-with-top-3-capturing-80-percent-143555.

[117] Apple, for instance, added a whole suite of encryption tools as well as a basic level of device encryption to iOS 8. *See* Cyrus Farivar, *Apple expands data encryption under iOS 8, making handover to cops moot*, ARS TECHNICA (Sep. 18, 2014), http://arstechnica.com/apple/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/.

(cont.)

Additionally, many mobile developers rely on common resources — for instance Amazon Web Services — to power the backend of their apps.[118] Thus, much of the traffic from mobile apps appears to ISPs to be traveling to and from generic services on broadly used infrastructure, which would frustrate any attempt to develop a profile on even a particular app's usage, let alone on what a given user is doing with that app. The edge providers that develop the apps, on the other hand, *will* have a complete view of all relevant user data.

Some comments in support of the proposed rules attempt to cast ISPs as all powerful by virtue of their access to apparently trivial data — IP addresses, access timing, computer ports, etc. — because of the power of predictive analytics.[119] These commenters assert that the possibility of predictive analytics coupled with a large data set undermines research that demonstrates that ISPs, thanks to increasing encryption, do not have access to any better quality data, and probably less quality data, than edge providers themselves have.[120]

But this is a curious bit of reasoning. It essentially amounts to the idea that, not only should consumers be permitted to control with whom their data is shared, but that all other parties online should be proscribed from making their own independent observations about consumers. Such a rule would be akin to telling supermarkets that they are not entitled to observe traffic patterns in their stores in order to place particular products in relatively more advantageous places, for example. But the reality is that most data is noise; simply having more of it is not necessarily a boon, and predictive analytics is far from a panacea. In fact, the insights gained from extensive data collection are frequently useless when examining very large data sets, and are better employed by single firms answering particular questions about their users and products.[121]

And, although it is possible to conceive of a future in which ISPs may be able to connect the dots between the various random data points found in their access logs, the fact still remains that any edge provider with a relationship with a third-party data aggregator could basically obtain the same insights. Supporters of the proposed rules yet again have failed to demonstrate not only why it is that this sort of access should be disfavored (or deterred), but also why such a restriction should apply only to ISPs.

---

[118] Sharon Gaudin, *The cloud gets mobile apps moving*, COMPUTERWORLD (Aug. 17, 2015), http://www.computerworld.com/article/2971519/cloud-computing/the-cloud-gets-mobile-apps-moving.html.

[119] PK 2016 Privacy Comments, *supra*, note 15, at 6–8.

[120] *Id.* at 9.

[121] *See, e.g.*, James Glanz, *Is Big Data a Big Dud?*, *supra* note 23.

(cont.)

IV. Regulation of ISP Privacy Practices Should Revert to the FTC

As the NPRM recognizes, "[w]hen the [FCC] reclassified broadband Internet access service as a common carriage telecommunications service in 2015… that action stripped FTC authority over Internet service providers."[122] The FTC Act prohibits the FTC from regulating common carriers.[123] Reversing Title II reclassification will restore jurisdiction over ISP privacy and data security practices to the FTC – the agency with the most experience and expertise in the privacy area. And preempting state-level regulation of ISP privacy practices will ensure that consumers enjoy strong, consistent, and comprehensive privacy protections while providers have the flexibility and certainty to innovate.

A. The FTC's experience and expertise make it the best agency to oversee ISP privacy practices.

One of the primary reasons cited in the legislative record supporting Congress's resolution of disapproval of the FCC's flawed 2016 privacy rules was Congress's intent to have a single privacy standard for the players in the Internet ecosystem that is administered by the FTC.[124] In the NPRM, the FCC seeks to implement that goal by "propos[ing] to respect the jurisdictional lines drawn by Congress whereby the FTC oversees Internet service providers' privacy practices."[125] This is the right decision.

Given the FTC's widely recognized expertise in this space, it is appropriate to return jurisdiction over ISPs' privacy practices to the agency to ensure a consistent privacy framework for all participants in the online economy. Officials from both the FTC and FCC strongly favor having a single uniform privacy standard for Internet companies that is administered by the FTC as the expert agency in the privacy space. Chairman Pai has repeatedly stated his preference for this outcome. For example, in his statement commending Congress on passing its joint resolution of disapproval of the FCC's *2016 Privacy Order*, Chairman Pai reiterated that "the FCC will work with the FTC to ensure that consumers' online privacy is protected through a consistent and comprehensive framework. In my view, the best way to achieve that result would be to return jurisdiction over broadband providers' privacy practices to the FTC, with its decades of experience and expertise in this area."[126] Similarly,

---

[122] *Restoring Internet Freedom NPRM* at ¶ 66.

[123] *See* 15 U.S.C. § 45(a)(1).

[124] *See* 163 Cong. Rec. at H2489 (Mar. 28, 2017) (statement of Rep. Blackburn) (stating that "having two privacy cops on the beat will create confusion within the internet ecosystem and will end up harming consumers"); 63 Cong. Rec. at S1954 (Mar. 23, 2017) (statement of Sen. Cornyn) ("The FCC privacy rules are just another example of burdensome rules that hurt more than help and serve as another example of the government's picking winners and losers. They unreasonably target internet service providers and, ultimately, make our internet ecosystem less efficient by adding more redtape.") .

[125] *Restoring Internet Freedom NPRM* at ¶ 67.

[126] Ajit Pai, Chairman, FCC, Statement on Congressional Resolution of FCC Broadband Privacy Regulations (Mar. 28, 2017), https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0328/DOC-344116A1.pdf.

(cont.)

Chairman Pai and Acting Chairman Ohlhausen issued a joint statement in the wake of the FCC's stay of its disapproved data security rules noting their joint belief that jurisdiction over ISPs' privacy practices should be returned to the FTC, noting that "[t]he FTC has a long track record of protecting consumers' privacy and security throughout the Internet ecosystem."[127]

Acting Chairman Ohlhausen and senior FTC staff have also expressed the belief in this proceeding that returning jurisdiction over ISPs' privacy practices to the FTC is the right course of action to ensure a consistent privacy framework for all online entities.[128] Acting Chairman Ohlhausen and the FTC staff both described at length "the FTC's powerful tools to protect consumers and competition" and the FTC's significant expertise in handling privacy issues.[129] Among the reasons the FTC staff provided in support of returning jurisdiction to the FTC, the staff rightly recognized that,"[a]s a matter of consistency, it makes little sense to exclude only BIAS providers from the FTC's privacy and data security jurisdiction, which covers virtually all other entities in the Internet ecosystem."[130] These statements are consistent with the conclusions drawn by the FTC in its 2012 Privacy Report, in which it set forth a privacy framework that "applies to all commercial entities" (with certain limitations related to the type and amount of data collected).[131]

B. Preempting state regulation of ISP privacy practices will prevent the formation of a patchwork of privacy regulation that would be harmful to policy objectives

In addition, the FCC should expressly clarify that state laws regulating the collection and use of customer information by ISPs that conflict with the FTC's privacy framework are preempted. Declaring that BIAS is an interstate information service that is not subject to certain forms of state regulations — like conduct regulations that prescribe how ISPs can use their networks — would be consistent with the FCC's treatment of BIAS in the past.[132] The FCC has an established history of

---

[127] Ajit Pai, Chairman, FCC, & Maureen K. Ohlhausen, Acting Chairman, FTC, Joint Statement on Protecting Americans' Online Privacy (Mar. 1, 2017), https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0301/DOC-343702A1.pdf.

[128] Comments of Acting FTC Chairman Maureen K. Ohlhausen, WC Docket No. 17-108, at 14 (Jul. 17, 2017) [hereinafter "Ohlhausen Comments"]; Comment of the Staff of the Federal Trade Commission, WC Docket No. 17-108, at 12 (Jul. 17, 2017) [hereinafter "FTC Staff Comments"].

[129] Ohlhausen Comments at 8-13; FTC Staff Comments at 2-12.

[130] FTC Staff Comments at 18.

[131] FTC Privacy Report at 22.

[132] *See Vonage Holdings Corp. Petition for Declaratory Ruling Concerning an Order of the Minnesota Public Utilities Commission*, Memorandum Opinion and Order, 19 FCC Rcd. 22404, ¶¶ 22-32 (2004), *aff'd sub nom. Minn. Pub. Utils. Comm'n v. FCC*, 483 F.3d 570 (8th Cir. 2007).

(cont.)

preempting state regulation to ensure that information services, including Internet access, are regulated exclusively at the federal level or are subject to a federal policy that these services "should remain free of regulation."[133]

Under federal law, state regulations may be preempted expressly or implicitly to the extent that they "stand[] as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."[134] This authority to preempt state law extends beyond Congress to federal agencies acting within the scope of their authority.[135] Like a decision by Congress or a federal agency to adopt particular regulations, a decision *not* to regulate in a particular way also has preemptive effect.[136]

Privacy rules such as those adopted in the FCC's rescinded *2016 Privacy Order*, if adopted by some selection of states, would serve to constrain, if not dictate, how ISPs may provide BIAS and their use of customer information derived therefrom. As we have discussed above, such rules can have a very real and negative effect on ISPs' provision of BIAS to the detriment of their customers and the economy. A patchwork of state privacy laws that mandate various, and inevitably contradictory, technical or operational requirements regarding the provision of BIAS would frustrate congressional and FCC intent to have a single uniform privacy framework for ISPs and other entities in the Internet ecosystem.

This is not an idle concern. Many states have already shown an interest in stepping in to fill the perceived void left when Congress adopted its joint resolution of disapproval to rescind the *2016 Privacy Order*.[137] Some states have even attempted to adopt rules mirroring the very FCC rules already rejected by Congress. These attempts at state privacy legislation unique to ISPs would create a patchwork of regulation that would frustrate the Commission's intent to return to a regulatory state of affairs under which "every online company's privacy practices [would be policed] consistently" by the FTC as the expert agency in this area.[138]

---

[133] *See Petition for Declaratory Ruling that pulver.com's Free World Dialup Is Neither Telecommunications Nor a Telecommunications Service*, Memorandum Opinion and Order, 19 FCC Rcd. 3307 ¶ 16 (2004); *see also id.*

[134] *Crosby v. Nat'l Foreign Trade Council*, 530 U.S. 363, 373 (2000) (citations and quotation omitted).

[135] *See City of New York v. FCC*, 486 U.S. 57, 63-64 (1988).

[136] *See Bethlehem Steel Co. v. N.Y. State Labor Relations Bd.*, 330 U.S. 767, 774 (1947).

[137] *See, e.g.*, Jon Brodkin, *California May Restore Broadband Privacy Rules Killed by Congress and Trump*, ARS TECHNICA (June 21, 2017), https://arstechnica.com/tech-policy/2017/06/california-may-restore-broadband-privacy-rules-killed-by-congress-and-trump/; Aaron Nicodemus, *States Step in to Fill Rescinded FCC Web Privacy Rule Void*, Bloomberg BNA (Apr. 18, 2017), https://www.bna.com/states-step-fill-n57982086800/.

[138] *Restoring Internet Freedom NPRM* at ¶ 66.

(cont.)

Moreover, the privacy laws that states have already proposed vary significantly — from those that seek to adopt the FCC's rescinded rules to others that propose new and sometimes more onerous requirements for ISPs.[139] As Commissioner Clyburn has acknowledged, such variations in privacy protections is problematic. Thus she noted in testimony before the House Energy and Commerce Subcommittee on Communications and Technology that "I don't think the American public would be very comforted to know that depending on who they call or who their provider is or whether they go online that they might have different levels of expectations or protections."[140]

This is not to say that states have no role in privacy regulation. Such an approach would prevent states from adopting *ISP-specific* regulations, but it would not prevent states from imposing and enforcing laws of general applicability that do not contravene federal policy. Thus, for example, general data breach notification laws would still apply to the extent that an ISP is the victim of an incident that triggers such laws, and state attorneys general would contionue to be able to enforce their state consumer protection laws against deceptive privacy policies.

As discussed above, however, there is no basis for treating ISPs differently than other companies that provide Internet-based services, and doing so could harm consumers and the economy by creating of consumer confusion, limiting options and information available to consumers, and constraining ISP innovation and investment.

C. Concerns over Ninth Circuit's *AT&T Mobility* decision are misguided

Some have raised concerns that the FTC's jurisdiction over ISP privacy practices may be limited due to a ruling by a panel of the Ninth Circuit in *FTC v. AT&T Mobility* that the common-carrier exemption is status-, not activity-based.[141] Simply put, these concerns are misguided.

---

[139] Legislators in Washington, for example, proposed a bill that would enact rules largely tracking those disapproved of by Congress, whereas legislators in Maryland and Minnesota proposed to adopt legislation requiring ISPs to obtain opt-in consent before using the IP address of a customer's *router* for any purpose, including providing broadband access. But without such IP addresses, it is impossible to render BIAS. At the same time, these proposed bills would prohibit providers from refusing BIAS for non-consent, even though it is impossible to provide the service without such information.

[140] *Oversight and Reauthorization of the Federal Communications Commission: Hearing Before the Subcomm. on Communications and Technology of the H. Comm. on Energy and Commerce*, 115th Cong. (Jul. 25, 2017) (statement of Mignon Clyburn, Commissioner, FCC), https://www.c-span.org/video/?431676-1/fcc-commissioners-testify-oversight-hearing&start=9179 (at 02:31:42).

[141] *See, e.g.*, *Restoring Internet Freedom NPRM* at 73 (Dissenting Statement of Commissioner Mignon L. Clyburn) ("The item proposes to quietly ensure that broadband customers have no privacy protections whatsoever, shirking our privacy responsibilities under the Communications Act. The majority knows that we cannot simply let the Federal Trade Commission (FTC) take the helm on broadband provider privacy practices while there is still a chance that if a provider offers legacy voice their broadband service—irrespective of classification—is likely out of bounds for the FTC. (cont.)

As an initial matter, the panel decision is no longer good law. The Ninth Circuit decided to grant *en banc* rehearing of the panel's decision, and in so doing nullified the panel's ruling.[142] In its order granting *en banc rehearing*, the Ninth Circuit explicitly clarified that "[t]he three-judge panel disposition in this case shall not be cited as precedent."[143] Therefore, unless and until the *en banc* Ninth Circuit upholds the panel's ruling on its interpretation of the common-carrier exemption, the ruling has no legal effect on the FTC's ability to address the non-common-carrier activities of ISPs.

Moreover, the *AT&T Mobility* panel's decision is unequivocally in error. The common-carrier exemption has long been understood as activity-based,[144] and to treat it otherwise "would leave no federal agency able to protect millions of consumers across the country from unfair or deceptive practices or obtain redress on their behalf," a problem that "is especially severe in the area of consumer data privacy and security."[145] Similarly, the FCC has also historically understood the common-carrier exemption to be activity-based: "In [the FCC's and FTC's] coordinated efforts to protect American consumers, the agencies have historically understood the FTC to have jurisdiction over non-common-carrier services of entities that also engage in common carriage services within the exclusive jurisdiction of the FCC and have concentrated their consumer protection accordingly."[146] The FCC and FTC memorialized this mutual understanding in a Memorandum of Understanding between the two agencies regarding consumer protection oversight.[147]

Finally, even if the panel's decision is upheld on rehearing, the ruling would apply only within the Ninth Circuit and would not have binding precedential effect in any other circuit. In fact, at least one other circuit has taken a position contrary to the misguided *AT&T Mobility* panel's ruling by indicating that the common-carrier exemption is activity-based.[148]

While it is heartening for consumers that the case that limits the FTC's authority is slated for rehearing, it is still unclear whether the FTC can enforce broadband privacy until the full 9th Circuit opines.").

[142] *FTC v. AT&T Mobility LLC*, 864 F.3d 995 (9th Cir. 2017).

[143] *Id.*

[144] Petition of the Federal Trade Commission for Rehearing *En Banc*, *FTC v. AT&T Mobility LLC*, No. 15-16585, at 5 (9th Cir. Oct. 13, 2016) ("[t]he FTC has long interpreted the exception as activity-based.").

[145] *Id.* at 1-2.

[146] Amicus Curiae Brief of the Federal Communications Commission in Support of the Federal Trade Commission's Petition for Rehearing *En Banc*, *FTC v. AT&T Mobility LLC*, No. 15-6585, at 3 (9th Cir. Oct. 24, 2016).

[147] *FCC-FTC Consumer Protection Memorandum of Understanding*, at 2 (Nov. 16, 2015), *available at* https://www.ftc.gov/policy/cooperation-agreements/memorandum-understanding-consumer-protection-between-federal-trade ("[T]he scope of the common carrier exemption in the FTC Act does not preclude the FTC from addressing non-common carrier activities engaged in by common carriers.").

[148] *See, e.g.*, *FTC v. Verity Int'l, Ltd.*, 194 F. Supp. 2d (S.D.N.Y. 2002), *aff'd* on other grounds, 443 F.3d 48 (2d Cir. 2006); *see also* Petition of the Federal Trade Commission for Rehearing *En Banc*, *FTC v. AT&T Mobility LLC*, No. 15-16585, at 6.

Conclusion

Re-imposing restrictive privacy rules on ISPs would stifle robust competition between ISPs and other platforms and suppress ISPs' investment in new lines of business, thereby depriving consumers of new and innovative services, greater choice in the marketplace, and lower prices. The FTC's mode of regulation of ISPs has been perfectly sufficient, and relatively few complaints emerged during its tenure. At the same time, the FCC engages in its own case-by-case analysis of privacy harms and further bolsters the effective regulation of the use of data by ISPs. There is no reason to return to the Wheeler-FCC's flawed, broadband-specific privacy rules once Title II is rescinded.

Rather, in order to ensure consistent regulation of privacy practices on the Internet, the FCC should declare that BIAS is an interstate information service and thereby return primary jurisdiction over ISPs' privacy practices to the FTC.

Consistent with this action, the FCC should also make explicitly clear that, because BIAS is an interstate information service, state rules and regulations for BIAS that are inconsistent with federal policy governing the regulation of ISPs' privacy practices are preempted. A patchwork of ISP privacy regulations at the state level would thwart the goal of having a unified privacy framework for ISPs that is consistent with the framework for all other participants in the Internet ecosystem.