BEFORE THE

Federal Communications Commission

WASHINGTON, D.C.

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

COMMENTS OF COMCAST CORPORATION

COMCAST CORPORATION
300 New Jersey Avenue, N.W., Suite 700
Washington, DC 20001

WILLKIE FARR & GALLAGHER LLP
1875 K Street, N.W.
Washington, D.C. 20006

Counsel for Comcast Corporation

May 27, 2016

Table of Contents

Page

Table of Contents
(continued)

Page

Table of Contents
(continued)

Page

BEFORE THE

Federal Communications Commission

WASHINGTON, D.C.

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

COMMENTS OF COMCAST CORPORATION

Comcast Corporation ("Comcast") hereby responds to the above-captioned Notice of Proposed Rulemaking ("NPRM").[1] Comcast shares the Commission's stated goal of protecting the information consumers provide to their Internet service providers ("ISPs") and others in the Internet ecosystem, but what the Commission has proposed would actually be a net negative for consumers, who would realize no improvement in privacy. To the contrary, consumers would experience significant decreases in discounted offers, innovative services, and competitive alternatives. Rather than the ineffective and harmful privacy regime that the Commission has proposed, it should harmonize its framework with the technology-neutral privacy policies of the Obama Administration and the Federal Trade Commission ("FTC"), which have been very successful at protecting consumer privacy while also facilitating greater innovation, investment, and competition.

I. INTRODUCTION AND SUMMARY

"Any privacy framework should be technology neutral. ISPs are just one type of large platform provider [along with operating systems, browsers, social media, and other online

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, WC Docket No. 16-106 (rel. Apr. 1, 2016) ("*NPRM*").

services] that may have access to all or nearly all of a consumer's online activity."[2] So concluded the FTC in its comprehensive 2012 Privacy Report, after decades of rigorous study and oversight of the privacy practices of ISPs and all other service and content providers in the Internet ecosystem. The Obama Administration embraced a very similar approach in its 2012 Consumer Privacy Bill of Rights Report, recommending "a level playing field for companies, a consistent set of expectations for consumers, and greater clarity and transparency in the basis for FTC enforcement actions."[3] Chairman Wheeler also endorsed this approach, telling Congress and the public that "we work closely with the FTC[;] we will do our best to harmonize so that there is a common set of concepts that govern privacy,"[4] and "one of our challenges is to make sure we're consistent with the kind of thoughtful, rational approach that the FTC has taken."[5]

Comcast fully agrees with these statements. The best approach for the FCC to take in this proceeding would be to adopt rules that are consistent with the time-tested and highly successful technology-neutral privacy framework that the Administration has put forward and the FTC has maintained for decades for the entire Internet ecosystem – ISPs and non-ISPs alike. Several months ago, a wide cross-section of industry associations representing ISPs, technology

---

[2] *See Protecting Consumer Privacy in an Era of Rapid Change*, FTC Report, Federal Trade Commission, at 56 (Mar. 2012), https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers ("*2012 FTC Privacy Report*").

[3] Executive Office of the President, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, White House Report, at 36 (Feb. 2012), www.whitehouse.gov/sites/default/files/privacy-final.pdf ("*2012 White House Consumer Privacy Bill of Rights Report*"); *see also* Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015, https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf ("*2015 Consumer Privacy Bill of Rights Discussion Draft*").

[4] *Continued Oversight of the FCC: Hearing Before the Subcomm. on Communications & Technology of the House Energy and Commerce Comm.*, 114th Cong., Transcript at 107-108 (2015) (Statement of Tom Wheeler, Chairman, FCC).

[5] Margaret Harding McGill, *FCC, FTC Chiefs Zero In on Data Security, Privacy*, Law360 (Jan. 6, 2016) (reporting Chairman Wheeler's remarks during a conversation with Gary Shapiro, president and CEO of the Consumer Technology Association at the Consumer Technology Association show).

companies, equipment manufacturers, and others urged the Commission to exercise its newly-acquired jurisdiction over ISPs' privacy practices by adopting a privacy framework that maintains continuity with Administration policy and the FTC regime (the "Consensus Privacy Framework," attached hereto as Appendix B). Comcast strongly supports the Consensus Privacy Framework. It would allow the FCC to replicate the successful privacy policies advocated by the Administration and enforced by the FTC by focusing on transparency, choice, data security, data breach notification, and other key principles. This is a solution where everyone wins, most notably consumers, whose privacy would continue to be protected, and who would continue to benefit from lower-priced offerings, innovative new services, and increasing competitive alternatives.

Unfortunately, the FCC's NPRM proposes an entirely different – and entirely unjustified – path backwards. The NPRM would ignore the Administration's position and the FTC's framework and actually flip it on its head by adopting the most onerous and far-reaching privacy regulations ever devised in this country, and applying those regulations solely to ISPs despite the fact that "non-ISPs are increasingly gathering commercially valuable information about online user activity from multiple contexts, such as: (1) social networks; (2) search engines; (3) webmail and messaging; (4) operating systems; (5) mobile apps; (6) interest-based advertising; (7) browsers; (8) Internet video; and (9) e-commerce."[6] For example:

- While the FTC framework and Administration policies demonstrate a respect for context by applying opt-in consent only to highly-sensitive data (i.e., health, financial, and children's data, social security numbers, and precise geolocation data) and opt-out or implied consent to all other consumer data, the FCC's NPRM would do the exact

[6] Peter Swire, Justin Hemmings, & Alana Kirkland, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, Working Paper of The Institute for Information Security & Privacy at Georgia Tech, at 3-4 (Feb. 29, 2016), http://peterswire.net/wp-content/uploads/Online-Privacy-and-ISPs.pdf ("*Swire Paper*").

opposite by applying opt-out and implied consent to an extremely narrow set of activities and a blanket opt-in consent requirement to all other uses and disclosures.

- While the FTC framework and the Administration's Consumer Privacy Bill of Rights would allow companies to rely on implied consent to use and disclose information to market their and their affiliates' products and services to their customers, the FCC proposal would require that ISPs obtain opt-out consent for marketing a narrow set of "communications-related services" and opt-in consent for marketing all other services to their customers.

- While the Administration's Consumer Privacy Bill of Rights recognized that consumers today routinely benefit from free and innovative online services in exchange for allowing their data to be used for marketing and advertising, the NPRM proposes to prohibit ISPs from offering their customers price discounts or other value in exchange for the customer's consent to use her data for marketing and advertising. The FCC has no authority to prohibit or limit these types of programs, and such a prohibition would also be bad policy, since such offerings could result in significant benefits for consumers.

- While federal and state data breach laws typically limit companies' liability for breaches where circumstances warrant, such as where the data is encrypted or where consumers are not harmed, the FCC proposes a broad strict liability standard that would lead to over notification and, eventually, notice fatigue.

- While Section 222 only permits the FCC to regulate customer proprietary network information ("CPNI") and provides an exemption for subscriber list information, the FCC proposal would rewrite the statute by defining the data covered by the rules far more broadly than CPNI and outright eliminating the subscriber list information exemption.

There is no reasonable legal or policy basis for the FCC's proposed approach. Nothing has changed that would justify such a major departure from the flexible, technology-neutral approach endorsed by the FTC, the Administration, and Chairman Wheeler. Nothing in the marketplace, nothing in ISPs' behavior, nothing in consumers' views of ISPs or their privacy expectations – nothing, period. Although the 2015 Open Internet Order's reclassification of ISPs as common carriers shifted privacy jurisdiction over ISPs to the FCC from the FTC, that change does not mean the FCC can regulate ISPs without regard to the law or the facts.

The Commission's proposal will not enhance consumer privacy. The Commission's proposal will not enhance consumer privacy in any meaningful way. As explained in the Future of Privacy Forum's recent blog post, "[d]espite industry efforts, for many advocates and

consumers the comprehensive and pervasive nature of online tracking continues to be debated. But one thing is certain: it is not unique to ISPs."[7]

ISPs do not have widespread or unique access to customer information. In the post-Snowden world, encryption on the Internet is dramatically increasing, so that by the end of 2016 over 70% of all Internet traffic – and over 80% of the top-50 websites – will be encrypted, allowing ISPs to access and potentially use *even less* consumer data than they could when the FTC's and Administration's technology-neutral privacy approach for the Internet ecosystem was implemented. This is a key finding in the recent report of Peter Swire – a world-renowned privacy expert and the former chief privacy and policy advisor to Presidents Clinton and Obama – who concluded:

> In summary, based on a factual analysis of today's Internet ecosystem in the United States, ISPs have neither comprehensive nor unique access to information about users' online activity. Rather, the most commercially valuable information about online users, which can be used for targeted advertising and other purposes, is coming from other contexts.[8]

In other words, the FCC's proposed rules would apply to the entities that have less and less access to online customer information. Moreover, the non-ISPs to which the FCC's rules would *not* apply have access to the very same information to which ISPs have access – and often much more.

The Commission incorrectly assumes that consumers support its proposal. The Commission assumes that consumers desire tighter privacy regulations for ISPs than have existed under the FTC's regime, but there is no basis for this assumption. In fact, surveys conducted by the Pew Research Center, the Harvard Business Review, Columbia Business

---

[7] Stacey Gray, *Comprehensive Online Tracking is Not Unique to ISPs*, Future of Privacy Forum (May 20, 2016), https://fpf.org/2016/05/20/14382/ (emphasis added).

[8] *Swire Paper* at 3-4.

School, The National Cyber Security Alliance, and others show that consumers trust ISPs as much as or more than non-ISPs when it comes to collection and use of their online data. And a recent consumer survey conducted by Public Opinion Strategies & Peter D. Hart shows that (1) by an overwhelming 90%-8% margin, Internet users strongly agree that *all Internet companies should operate under the same set of privacy rules and regulations*; and (2) by a wide 83%-12% margin, Internet users say their online privacy should be protected *based on the sensitivity of their online data, rather than by the type of Internet company that uses their data*.[9] In other words, notwithstanding the NPRM's claims, the actual facts show that consumers support the current FTC and Administration technology-neutral, flexible approach to online privacy, not the radical departure from that approach being proposed by the Commission.

ISPs have a strong privacy track record. There is no evidence that ISPs have harmed consumers' privacy or present a greater threat to privacy than non-ISPs. At a recent Senate hearing on the FCC's broadband privacy proposal, FTC Chairwoman Ramirez and FTC Commissioner Ohlhausen both strongly indicated that the FTC privacy framework had been successful in protecting consumers and in regulating ISPs.[10] *In fact, the FTC has brought far more privacy enforcement actions against non-ISPs than ISPs*. This is not surprising as the ISP business model incentivizes the responsible treatment of consumer data, as the FCC itself has previously recognized.

---

[9] Neil Newhouse, Robert Blizzard, & Peter D. Hart, *Key Findings from Recent National Survey of Internet Users*, Progressive Policy Institute Memorandum, at 1-3 (May 26, 2016), http://www.progressivepolicy.org/wp-content/uploads/2016/05/Internet-User-National-Survey-May-23-25-Key-Findings-Memo.pdf (emphasis added).

[10] *Examining the Proposed FCC Privacy Rules: Hearing Before the Subcomm. on Privacy, Technology and the Law of the Senate Comm. on the Judiciary*, 115th Cong. (May 11, 2016) (statements of Edith Ramirez, Chairman, FTC and Maureen Ohlhausen, Commissioner, FTC), http://www.c-span.org/video/?409389-1/fcc-commissioners-testify-proposed-internet-privacy-rules (starting at 01:02:40 and 01:10:12).

The FCC's asserted rationales for applying onerous privacy rules only to ISPs have no basis in fact. In the same Senate hearing noted above, Chairman Wheeler suggested that the NPRM's onerous regulations may be warranted because ISPs control the broadband "network," and thus need to be restricted in similar ways to the voice CPNI rules that apply to the telephone companies that control the voice "network."[11] But this view is predicated on a series of false premises. The telephone network for which Section 222 was created collected unique data that was held only by the underlying network. No other entity could collect this data, and so Congress and the FCC were understandably focused on establishing rules to address the use, disclosure, and access to this unique consumer data. *But that is not at all the case with the Internet.* ISPs are part of a much different "network." As one commentator recently explained,

> [T]here's a difference between what Internet carriers know about what we do on the Internet and what PSTN carriers know about what we did on the telephone network for a very basic reason. The PSTN carrier is indistinguishable from the PSTN service provider because only the carrier can create a service. But the Internet allows anyone to create a service because Internet services are distinct from Internet carriage. The Internet takes apart the PSTN and rebuilds it partially on carriers and partially on service providers at the edge.[12]

The result is that ISPs are one of many parts of the Internet ecosystem in which ISPs and non-ISPs alike have access to much of the *same* consumer data – such as IP addresses and web-browsing history. Chairman Wheeler is, therefore, fundamentally mistaken in looking to the networks of the 20th century as a basis for privacy regulation of ISPs in the 21st century, and in his assumption that applying onerous privacy rules will enhance consumers' privacy in any way.

---

[11] *Examining the Proposed FCC Privacy Rules: Hearing Before the Subcomm. on Privacy, Technology and the Law of the Senate Comm. on the Judiciary*, 115th Cong. (May 11, 2016) (statement of Tom Wheeler, Chairman, FCC), http://www.c-span.org/video/?409389-1/fcc-commissioners-testify-proposed-internet-privacy-rules (starting at 01:21:14).

[12] Richard Bennett, *Privacy and the Internet: What the FCC Doesn't Get*, HighTech Forum (May 17, 2016), http://hightechforum.org/privacy-internet-fcc-doesnt-get/.

The claim by some that onerous ISP privacy rules are justified by the consumers' inability to easily switch ISPs also has no merit. This argument fails to acknowledge the following key facts:

- Comcast and other ISPs comply with the FTC's privacy framework on a *footprint-wide basis*, and all our broadband customers receive the same privacy policy that protects their data in the same compliant manner, so whether a broadband customer has one, none, or three other broadband competitive alternatives in their area does not change how ISPs use or protect their data or justify such unique ISP privacy rules.

- ISPs are not the only "large platform providers," and competitive alternatives for broadband are just as numerous as those for other such platforms. For example, there are two major mobile operating systems from which to choose, a few major social media platforms, and a few major email providers.

- And switching operating systems, social media platforms, email providers, and other online services is no less difficult than switching ISPs. For example, experts who have studied switching between iPhone and Android, or vice versa; switching to a new social media platform; or changing email service providers universally conclude the same thing – "Given the headaches of switching, most people avoid it."[13]

- In 2010, the FCC conducted a survey finding that one out of six customers switch wireline providers every year and that over the prior three years, 36% of Internet users had indicated that they had switched their provider, with 13% of users switching providers more than once, and almost one-third of those who had not switched providers having considered doing so.[14]

The Commission's proposal would affirmatively harm consumers. Not only is there no basis for the Commission's proposed rules, but they would also affirmatively harm consumers in numerous ways.

[13] Vindu Goel, *How to Switch to iPhone From Android: Patience and Persistence*, N.Y. Times (Apr. 6, 2016), http://www.nytimes.com/2016/04/07/technology/personaltech/how-to-switch-to-iphone-from-android-patience-and-persistence.html?smprod=nytcore-iphone&smid=nytcore-iphone-share&_r=0.

[14] FCC, *Broadband Decisions: What Drives Consumers to Switch—Or Stick With—Their Broadband Internet Provider*, FCC Working Paper, at 2-3 (Dec. 2010).

Cause Substantial Consumer Confusion. The rules would mislead and confuse consumers by creating a situation in which two very different sets of privacy standards apply to the same data that consumers provide to different entities participating in the Internet ecosystem.

- **EXAMPLE**: Imagine a consumer using her mobile device and ISP to connect to several websites to research some products or services. In the process she conducts various searches, emails her mom, launches a few apps, clicks on various Facebook "Like" buttons, and posts some comments to her social media page. While the limited data collected by the ISP in this example would be subject to an opt-in requirement before the ISP could use that data for marketing or other purposes, that very same data, plus much more data, collected by the websites, cookies, search engine, browser, mobile operating system, email service provider, apps, social media platform, ad networks, and other non-ISPs would all be subject to an opt-out consent regime. Thus, even if the consumer did not opt-in to the ISP's use of the data to send her tailored advertisements, she would still likely receive many tailored ads based on the data collected and used by the various *non-ISPs* in this example. This would confuse the consumer who thought she had prevented such tailored ads by not opting in to the ISP's use of her data.

Deprive Consumers of Discounted Bundles, Lower Prices, and Innovative Services and Depress Broadband Investment. The proposed rules would also diminish ISPs' incentive and ability to market and advertise to customers valuable, lower-priced bundled offerings, innovative services, and other discounted products that benefit consumers. For example, Comcast bundles broadband services in a "quadruple play" that includes home security services. To the extent services like home security are subject to opt-in consent, Comcast would be effectively foreclosed from using customer information from broadband services to market its quadruple play bundle. Many customers that would benefit from that offer would likely never become aware of it. The same is true for many new services that ISPs may wish to launch. The result will be to discourage ISPs from investing in such innovative services, and to reduce their incentives to invest in broadband, as the FCC has previously recognized when it touted the importance for broadband investment of affording flexibility to companies to offer product bundles to their customers.

Block New Competition. The proposed rules would also increase the barriers to ISP entry into the highly-concentrated market for online advertising, thereby depriving consumers of the greater competition and innovative products and services ISP insurgents could unleash in this market in which the top-10 players are edge providers that control over 70% of the market.[15] A leading industry analyst recently concluded, "We can't think of any other media marketplace with this level of dominance."[16]

This is significant, since ISPs are some of the few companies with the resources to enter this market. By reinforcing the market power of these *non-ISP incumbents*, the Commission would essentially ensure that online advertising prices remain artificially high. Given that online advertising is becoming an essential input for retail offerings, consumers will end up paying too much for a wide range of products and services across the economy. It is therefore unsurprising that a coalition that includes virtually every major trade association representing advertisers and retailers, including the American Advertising Association, the American Association of Advertising Agencies, the Direct Marketing Association, the National Retail Federation, the U.S. Chamber of Commerce and many more, has publicly opposed the sweeping ISP rules proposed by the Commission.[17]

Harm Network Security. The proposed rules would also make it harder for ISPs to deliver a secure, reliable service. For example, the Commission's proposal for detailed, highly

[15] *See, e.g.*, David Shepardson, *FCC Internet privacy proposal could harm broadband providers - Moody's*, Reuters (Mar. 15, 2016), http://www.reuters.com/article/usa-fcc-internet-moodys-idUSL2N16N19H ("Moody's said Internet providers could be 'severely handicapped' in their ability to compete with digital advertisers such as Facebook Inc. and Google").

[16] MoffettNathanson, *Digital Duopoly*, at 3 (May 3, 2016).

[17] Letter from American Advertising Federation et al., to Senators Jeff Flake and Al Franken (May 10, 2016), http://thedma.org/wp-content/uploads/Industry-Hill-Letter-re-FCC-Privacy-NPRM.pdf.

prescriptive security requirements runs completely counter to years of Administration cybersecurity policy, and even Chairman Wheeler's policy of allowing industry – as the first line of defense – to take the lead in developing and implementing robust cybersecurity practices. Relatedly, the extremely broad definition of data security breach, and the absence of any reasonable exceptions for consumer harm, encryption, inadvertent recipients, or the like, will lead to the massive over-notification of consumers and their desensitization to serious breaches, thus further undermining security and increasing consumer harms.

The Commission's proposal is unlawful. The Commission's proposal is unlawful in at least three respects. First, the Commission does not have the authority to adopt the proposed rules. Section 222 of the Communications Act was intended to apply to telephony providers, not ISPs, and there is no evidence that Congress intended it to apply in any context in the draconian fashion that the NPRM proposes. Nor can the Commission rely on Sections 201, 202, 705, 706, or any other provision to "supplement" its authority here. As the Commission has previously held, Section 222 occupies the field in the regulation of telecom carrier privacy. Moreover, if the Commission were to ignore this well-established precedent and rely on these other provisions, it would also undermine its position that it cannot regulate edge providers, since some of these provisions are not limited to telecommunications carriers.

Even assuming Section 222 applies to ISPs, the NPRM improperly attempts to contort and expand the plain language of Section 222 in ways that are clearly beyond Congress's intent and the Commission's authority. For example, the Commission proposes to expand the data covered by its rules to go far beyond "CPNI," including to data not obtained from the ISP customer and to data that is not "individually identifiable" under any reasonable interpretation of that term.

Second, the proposals are unconstitutional, because they violate ISPs' commercial speech rights under the First Amendment. Specifically, the government does not have a substantial interest in regulating the speech implicated by the Commission's proposal, the proposed rules do not directly and materially advance the government's purported interest in promoting customer privacy, and the proposed rules are not narrowly tailored. Thus, the proposed rules would be rejected by any reviewing court under the Supreme Court's well established *Central Hudson* test.

Finally, the proposed rules are arbitrary and capricious because they are unnecessary, unlikely to advance the Commission's stated goal of enhancing consumer privacy, and would be affirmatively harmful to consumers, ISPs, and others in the Internet ecosystem.

The Commission may not impose the proposed rules on cable services under Section 631. There is no basis for the Commission to extend any new privacy rules it adopts for ISPs to cable services under Section 631. The structure and terms of the Communications Act make clear that Congress intended for the privacy rules applicable to telecommunications services and cable services to be different. Congress enacted two very different statutory sections addressing these entities. In addition, various statutory provisions, such as 621(c), 624(f), and 621(b)(3)(A)(ii), expressly preclude application of telecommunications carrier rules to cable services and vice versa. Finally, any perceived need for rules governing ISPs' use of customer data can in no way be said to apply in the video marketplace, where the Commission has acknowledged there is robust competition and choice, and where the privacy regime has been in effect and working well for over 30 years.

* * *

In summary, assuming Section 222 authorizes the Commission to regulate broadband privacy, the FCC should:

- Adopt the Consensus Privacy Framework. This will continue to protect consumers' privacy consistent with the well-established and highly successful FTC and Administration privacy framework, while promoting continued competition, innovation, and investment in the vibrant Internet ecosystem.

- Limit Scope to CPNI. The Commission should limit its rules to the use, disclosure, and access to CPNI, as it did in the voice context, consistent with the plain language and intent of the statute.

- Limit Opt-In Consent to Sensitive Data. As set forth in the Consensus Privacy Framework, ISPs and their affiliates should be permitted to market or advertise any of their services to their customers based on implied consent, or at most opt-out consent where the affiliate relationship is not clear to the customer. Opt-in consent should be required only with respect to the use or disclosure of sensitive data (e.g., financial, health, children's data, Social Security Numbers, and precise geolocation data).

- Implement a Reasonable De-Identification Standard. ISPs should be permitted to use, disclose, and provide access to CPNI that has been stripped of information that could reasonably be used to identify any individual customer ("de-identified information") without obtaining prior customer approval. Information should be able to qualify as de-identified regardless of whether it is aggregated. The rules should also make clear that de-identification is only required with respect to sharing information with unaffiliated third parties, not with respect to internal uses or sharing with affiliates or contracted agents/vendors.

- Clarify Use of Vendors/Service Providers. The rules should make clear that an ISP may hire and provide CPNI to an agent/vendor based on implied consent, provided the ISP has an agreement with the vendor requiring it to safeguard the CPNI and to use it solely on behalf of and as directed by the ISP and not for the vendor's own purposes.

- Permit Use of Lower Pricing and Other Benefits in Exchange for Consent to Use CPNI. The Commission should allow ISPs to offer their customers lower prices or other benefits in exchange for their permission to use or disclose their data for marketing purposes. Such an approach is consistent with the statute and with common marketplace practices, and would significantly benefit consumers.

- Adopt Sensible Data Breach Rules. The data breach rules should (1) apply only to sensitive personal information; (2) incorporate reasonable exceptions that are commonplace in other breach rules for encryption, substantial consumer harm, and inadvertent disclosures; and (3) allow at least 30 days after discovery of the breach to send the notification.

- Refrain from Restrictions on Arbitration Clauses. The Commission has no authority or sound policy basis to restrict these clauses, which Congress clearly authorized in the Federal Arbitration Act and which the Supreme Court and many other courts have

consistently upheld. These provisions benefit both consumers and providers by offering them a less expensive and more convenient means of settling disputes.

- Refrain from Applying the Broadband CPNI Rules to Cable Services. The FCC has no authority to do so. Rather, Congress purposefully created separate privacy statutes for cable services and telecommunications services, and the Commission is not at liberty to ignore that clear congressional intent.

II. THE PRINCIPLES UNDERLYING THE ADMINISTRATION'S CONSUMER PRIVACY BILL OF RIGHTS AND THE FTC'S PRIVACY REGIME HAVE SUCCESSFULLY PROTECTED CONSUMERS AND FACILITATED INNOVATION FOR DECADES; THE COMMISSION SHOULD RELY ON THOSE PRINCIPLES AS IT MOVES FORWARD IN THIS PROCEEDING.

The FTC has been the nation's chief privacy enforcement authority on the Internet – for both ISPs and online content and service providers – since the beginning of the commercial Internet.[18] In 2012, the Administration, recognizing that "[a]s a world leader in Internet Innovation, the United States has both the responsibility and incentive to help establish forward-looking privacy policy models that foster innovation and preserve basic privacy rights,"[19] developed a Consumer Privacy Bill of Rights that would "serve as a template for privacy protections that increase consumer trust on the Internet and promote innovation."[20] Both the FTC's privacy regime and the Administration's Consumer Privacy Bill of Rights are built on a core set of principles, such as transparency/notice, choice/respect for context, and security, as well as an understanding that flexibility in the implementation of these principles "will help

[18] *See 2012 White House Consumer Privacy Bill of Rights Report* at 29 ("The FTC is the Federal Government's leading consumer privacy enforcement authority."); *Protection of Children's Privacy on the World Wide Web: Hearing Before the Subcomm. on Communications of the Senate Comm. on Commerce, Science & Transportation*, 105th Cong. (Sept. 23, 1998) (prepared statement of Robert Pitofsky, Chairman, FTC), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-protection-childrens-privacy-world-wide-web/priva998.pdf ("The [FTC] has been involved in addressing online privacy issues . . . for almost as long as there has been an online marketplace. Through a series of workshops and hearings, it sought to understand this new marketplace and its information practices, to assess the impact of these practices on consumers, and to encourage and facilitate effective self-regulation.").

[19] *2012 White House Consumer Privacy Bill of Rights Report* at 7.

[20] *Id.* at 2

promote innovation" and "encourage effective privacy protections by allowing companies . . . to address the privacy issues that are likely to be most important to their customers and users, rather than requiring companies to adhere to a single, rigid set of requirements."[21]

The principles at the heart of both the FTC's regime and the Administration's Consumer Privacy Bill of Rights have established the guidelines by which online companies such as Google, Facebook, and Amazon have developed their successful marketing and advertising practices. They have also shaped ISPs' business practices, including their cybersecurity policies, their customer privacy notices, and the circumstances and manner in which they seek customer consent to use personal information. They are the context in which ISPs have planned the introduction of innovative services that, among other things, promise to enhance energy efficiency and enable the Internet of Things. And these privacy policies have worked to protect the interest of consumers.

The NPRM's proposals would upend the settled expectations of both providers and consumers by imposing a privacy regime that is completely divorced from these principles without any demonstration that the time-tested regime was insufficient, inadequate, or in any way harmful to consumers. The Commission's decision in the 2015 Open Internet Order to reclassify broadband Internet access services as Title II telecommunications services may have created a "gap" in consumer privacy protection, but it changed nothing about the wisdom behind the FTC's and Administration's approach to online privacy.[22] Rather than trying to reinvent the

[21] *Id.; see also 2015 Consumer Privacy Bill of Rights Discussion Draft* (proposing specific legislative language to give effect to these principles).

[22] *See Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd. 5601, ¶ 308 (2015) ("*2015 Open Internet Order*").

wheel, the FCC should look to those principles – which are the foundation of the Consensus Privacy Framework – to develop the kinds of rules it needs to fill the "gap" it created.

A. The Administration and FTC Approach to Privacy Has Successfully Protected Consumers' Privacy and Facilitated Robust Innovation and Investment.

Under both the FTC's approach to online privacy and the Administration's Consumer Privacy Bill of Rights, consumer information should be protected based on the sensitivity of the information and how the information is used, not on the type of business that collects and uses the data.[23] Three of the key principles that form the foundation of the FTC's work regarding online privacy and the Administration's Consumer Privacy Bill of Rights are transparency/notice, choice/respect for context, and security.[24]

1. The core principles of the FTC and Administration approach to privacy.

Transparency/Notice. According to the FTC, the transparency principle consists of three components. First, companies must provide consumers with understandable privacy notices.[25] Second, consumers should have access to their own data, and the ability to correct mistakes in that data.[26] Third, companies should make an effort to educate consumers about their data

[23] The FTC provided a comprehensive description and explanation of these principles in its 2012 Privacy Report. *See generally 2012 FTC Privacy Report*. In the Consumer Privacy Bill of Rights, the Administration took the position that "[b]ecause existing Federal laws treat similar technologies within the communications sector differently, the Administration supports simplifying and clarifying the legal landscape and making the FTC responsible for enforcing the Consumer Privacy Bill of Rights against communications providers." *2012 White House Consumer Privacy Bill of Rights Report* at 39.

[24] In the 2012 FTC Privacy Report, the FTC lists data security as a component of privacy by design, one of the tenants of its approach to protecting consumer privacy. *2012 FTC Privacy Report* at vii.

[25] *Id.* at 67.

[26] *Id.* And the greater the sensitivity of the data and its uses, the more a consumer should have the right to access and correct that data. *Id.* at 67-68. Note that the FTC concluded that such access and correction rights are often unnecessary for data used solely for marketing purposes. *Id.* at 65-67.

privacy practices.[27] Similarly, the Consumer Privacy Bill of Rights explained that "[c]onsumers have a right to easily understandable and accessible information about privacy and security practices."[28]

Choice/Respect for Context. The choice principle is designed to ensure that consumers have meaningful choices with respect to the collection and use of personal information. Both the FTC and the Administration have emphasized that respect for context is a key component of understanding how to best implement this principle on the Internet. For example, the FTC has explained that companies may collect and use consumer personal information that is "consistent with the context of the transaction, or the company's relationship with the consumer" without obtaining the consumer's prior consent.[29] Under both the FTC's regime and the Consumer Privacy Bill of Rights, "first-party marketing" (i.e., marketing by an organization that has a relationship with a given consumer) is considered a use of personal information that is consistent with the context of the consumer's relationship with the organization, and, as such, should generally be permissible based on *implied consent*.[30] Likewise, the FTC has explained that sharing of consumer data with, and marketing by, affiliates of the organization typically can occur based on *implied consent* as long as the affiliate relationship is clear to consumers (e.g.,

---

[27] *Id.* at 72.

[28] *2012 White House Consumer Privacy Bill of Rights Report* at 14; *see also 2015 Consumer Privacy Bill of Rights Discussion Draft*, § 101 (proposing specific legislative language to give effect to the Transparency principle).

[29] *2012 FTC Privacy Report* at 48; *2012 White House Consumer Privacy Bill of Rights Report* at 17.

[30] *2012 FTC Privacy Report* at 48 ("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, or are required or specifically authorized by law."); *2012 White House Consumer Privacy Bill of Rights Report* at 17 ("[C]ompanies may infer consent to use personal data to conduct marketing in the context of most first-party relationships, given the familiarity of this activity in digital and in-person commerce, the visibility of this kind of marketing, the presence of an easily identifiable party to contact to provide feedback, and consumers' opportunity to end their relationship with a company if they are dissatisfied with it."); *2015 Consumer Privacy Bill of Rights Discussion Draft*, § 103(a) (the requirements of section 103 would not apply "[i]f a covered entity processes personal data in a manner that is reasonable in light of context").

through the use of common branding in the affiliates' or their products' names).[31] For example, "[t]he purchase of an automobile from a dealership illustrates how this standard could apply. In connection with the sale of the car, the dealership collects personal information about the consumer and his purchase. Three months later, the dealership uses the consumer's address to send him a coupon for a free oil change. . . . [T]he data collection and subsequent use is consistent with the context of the transaction and the consumer's relationship with the car dealership."[32]

In contrast, under the FTC framework, companies must provide customers with an *opt-out* choice before engaging in marketing by an affiliate that the consumer would not reasonably recognize as being part of the same company (e.g., different names).[33] In addition, companies typically must obtain customers' *opt-in* consent before collecting or using highly sensitive personal information (e.g., health, financial, and children's information, Social Security Numbers, or precise geolocation data) to conduct marketing, or before using consumer data in a "materially different manner than claimed when the data was collected."[34]

Security. Companies must protect the data they collect from unauthorized access. For its part, the FTC does not specifically prescribe what kinds of security measures must be taken, merely that the companies must take measures that are consistent with the nature and scope of the activities in which the company engages, the sensitivity of the data, and the size and

[31] *2012 FTC Privacy Report* at 42.

[32] *Id.* at 39.

[33] *Id*. at 42; *see also 2012 White House Consumer Privacy Bill of Rights Report* at 15 ("If companies will use or disclose personal data for [purposes other than those that are consistent with their relationship with the customer and the context of the original disclosure], they should provide heightened Transparency and Individual Choice by disclosing these other purposes in a manner that is prominent and easily actionable by consumers at the time of data collection.").

[34] *2012 FTC Privacy Report* at 47, 60.

complexity of the relevant data operations of the company.[35] The FTC also requires that companies seek "to build data security into products and services from the design stage."[36] Likewise, the Consumer Privacy Bill of Rights explained that "[c]ompanies should assess the privacy and security risks associated with their personal data practices and maintain reasonable safeguards to control risks such as loss; unauthorized access, use, destruction, or modification; and improper disclosure."[37]

2. These principles have been very successful.

The Administration and FTC approach to consumer privacy has established the preconditions for significant investment and innovation in the Internet ecosystem. Under this regime, ISPs have invested $1.4 trillion of private capital to deploy broadband networks that reach nearly every corner of the United States since 1996.[38] In 2014 alone, ISPs invested $78 billion.[39] This approach has engendered sufficient trust with consumers that broadband adoption has doubled over the last ten years, and now over 80% of Americans are online.[40] And the

---

[35] *See Start with Security: A Guide for Business; Lessons Learned from FTC Cases*, Federal Trade Commission, (July 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[36] *2012 FTC Privacy Report* at 26.

[37] *2012 White House Consumer Privacy Bill of Rights Report* at 19 ("The Security principle . . . gives companies the discretion to choose technologies and procedures that best fit the scale and scope of the personal data that they maintain, subject to their obligations under any applicable data security statutes, including their duties to notify consumers and law enforcement agencies if the security of data about them is breached, and their commitments to adopt reasonable security practices."); *see also 2015 Consumer Privacy Bill of Rights Discussion Draft*, § 105 (proposing legislative language to implement the Security principle).

[38] US Telecom: The Broadband Association, Broadband Investment, https://www.ustelecom.org/broadband-industry/broadband-industry-stats/investment (last visited May 22, 2016). For its part, since 1996, the cable industry has invested $245 billion in broadband networks. Francesca Duffy, NCTA Blog, Platform (Jan. 20, 2016), https://www.ncta.com/platform/industry-news/the-building-blocks-of-a-digital-america/.

[39] US Telecom: The Broadband Association, Broadband Investment, https://www.ustelecom.org/broadband-industry/broadband-industry-stats/investment (last visited May 22, 2016).

[40] Andrew Perrin &Maeve Duggan, *Americans' Internet Access: 2000-2015*, Pew Research Center (June 26, 2015), http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015/. As described more below, the recent publication by NTIA of information showing that consumers are worried about disclosing their data online is a perfect example of why this issue must be approached comprehensively, consistent with the FTC and

ecosystem around broadband Internet access has grown tremendously: the number of devices connected to the Internet is expected to grow to an estimated 50 billion by 2020,[41] and 65% of U.S. broadband households now subscribe to an over-the-top video service (including 52% of U.S. broadband households that subscribe to Netflix).[42] The App Economy alone has provided 1.66 million jobs in the United States by year end 2015, up from 750,000 in 2013, demonstrating the incredible proliferation and popularity of apps on mobile devices which did not even exist 10 years ago.[43]

The FTC's privacy regime is widely regarded as highly effective at protecting privacy while fostering investment and innovation. Numerous commentators have reached exactly this conclusion.[44] That regime has been so successful that the Administration made it the centerpiece of the recently-announced EU-U.S. Privacy Shield program.[45] It is, therefore, now central to the manner in which companies operate in both the U.S. and Europe.

Administration approach, and not piecemeal, as the FCC's proposal would do. *See* Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NTIA Blog (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

[41] Dave Evans, *The Internet of Things: How the Next Evolution of the Internet is Changing Everything, Cisco Internet Business Solutions Group*, Cisco White Paper, at 3 (Apr. 2011), http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[42] Press Release, Parks Associates, Parks Associates Announces Update to OTT Subscriber Churn Rates for Netflix, Hulu, and Amazon Users, (Apr. 14, 2016), http://www.parksassociates.com/blog/article/pr-0414016.

[43] Michael Mandel, *App Economy jobs in the United States*, Progressive Policy Institute Blog (Jan. 6, 2016), http://www.progressivepolicy.org/slider/app-economy-jobs-part-1/.

[44] *See, e.g.*, Doug Brake, Daniel Castro, & Alan McQuinn, *Broadband Privacy: The Folly of Sector-Specific Regulation*, Information Technology & Innovation Foundation, at 5 (Mar. 2016), http://www2.itif.org/2016-broadband-privacy-folly.pdf; Letter from American Advertising Federation et al. to Senators Jeff Flake and Al Franken (May 10, 2016), http://thedma.org/wp-content/uploads/Industry-Hill-Letter-re-FCC-Privacy-NPRM.pdf; Jon Leibowitz &Jonathan Nuechterlein, *The New Privacy Cop Patrolling the Internet*, Fortune (May 10, 2016), http://fortune.com/2016/05/10/fcc-internet-privacy/.

[45] Statement of FTC Chairwoman Edith Ramirez on EU-U.S. Privacy Shield Framework (Feb. 29, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/statement-ftc-chairwoman-edith-ramirez-eu-us-privacy-shield-0 ("As I affirmed in my letter to EU Commissioner Věra Jourová, the FTC will make enforcement of the new

B. The "Consensus Privacy Framework," Developed by a Broad Cross-Section of Industry Stakeholders, Effectively Balances The Goals of Privacy, Competition, and Innovation.

Despite the innumerable problems with the Commission's proposals as set forth in the NPRM, assuming the Commission has any jurisdiction to adopt privacy rules for ISPs,[46] there is a path forward that would allow the Commission to protect consumers and the data they provide to ISPs, facilitate innovation, investment, and competition, and do so within the scope of Section 222. In particular, the Consensus Privacy Framework accomplishes all these goals by building on the Administration's and FTC's successful privacy framework, and the FCC, to the extent it has authority to adopt such rules, could adopt the Framework as rules under Section 222. Alternatively, the FCC could defer this proceeding and use a multistakeholder process that the FCC convenes, working closely with both the FTC and NTIA to identify issues and solutions in the context of the principles that have been an important part of the Internet's success thus far.

1. The Consensus Privacy Framework is built on the principles espoused by the FTC and the Administration.

Consistent with the goal expressed by Chairman Wheeler last year to establish "a common set of concepts that govern privacy" online,[47] any privacy rules for ISPs should heavily borrow from the principles that underlie the FTC's and Administration's successful approach to consumer privacy on the Internet. The Consensus Privacy Framework (attached as Appendix B) is a roadmap for implementing the privacy principles in a manner that "is consistent with the

framework a high priority, and we will work closely with our European counterparts to provide robust privacy and data security protections for consumers in the United States and Europe.").

[46] *See* discussion, *infra*, at Sections V.A.1-2 regarding the Commission's lack of authority to adopt broadband privacy rules based on the plain language and intent of Section 222.

[47] *Continued Oversight of the FCC: Hearing Before the Subcomm. on Communications & Technology of the House Energy and Commerce Comm.*, 114th Cong., Transcript, at 107-08 (2015) (Statement of Tom Wheeler, Chairman, FCC).

FCC's privacy recommendations in the 2010 National Broadband Plan, the FTC's and White House's 2012 Privacy Reports, and the White House's 2015 Consumer Privacy Bill of Rights, as well as with Chairman Wheeler's recent testimony before Congress acknowledging the importance of coordination with the FTC and harmonization with its privacy framework."[48]

The key aspects of the Consensus Privacy Framework are as follows:

- *Transparency/Notice*. Each ISP should provide notice to its customers that describes the CPNI that it collects, how it will use that CPNI, and whether and for what purposes it may share that CPNI with third parties.

- *Consumer Choice/Respect for Context*. Each ISP may use or disclose CPNI consistent with the context in which the customer provides the information.[49] Further, ISPs should give consumers easy-to-understand choices for non-contextual uses and disclosures of their CPNI.

- *Data Security*. Each ISP should establish, implement, and maintain a CPNI data security program that includes reasonable physical, technical, and administrative security safeguards to protect CPNI from unauthorized access, use, and disclosure, in light of the nature and scope of the activities the company engages in, the sensitivity of the data, and the size and complexity of the relevant data operations of the company.

- *Data Breach Notifications*. Each ISP should notify its customers whose CPNI has been breached when such breach is likely to cause substantial harm to customers. Providers should have flexibility to determine how and when to provide such notice.

In addition, the Commission could require ISPs to obtain customer opt-in consent before using or disclosing defined classes of sensitive information. The Commission could also permit ISPs to use and disclose CPNI that has been stripped of information that could be used to identify individual customers ("de-identified information") without obtaining prior customer approval. Following this roadmap "will benefit consumers by safeguarding privacy interests as it has for

---

[48] *See* App. B.

[49] As discussed above, both the FTC's framework and the Consumer Privacy Bills of Rights infer consent for the collection and use of consumer personal information that is consistent with the context of the transaction or the company's relationship with the consumer. *See 2012 FTC Report* at 48; *2012 White House Consumer Privacy Bill of Rights Report* at 17.

years and will ensure that the same privacy and security framework applies to all entities in the Internet ecosystem," which will foster innovation and competition.[50]

If the Commission has authority under Section 222 to adopt privacy rules for ISPs, then it could adopt the Consensus Privacy Framework as a set of high-level privacy rules under Section 222. For example, under Section 222(c)(1), a telecommunications carrier must obtain the "approval of the customer" in order to use, disclose, or permit access to CPNI.[51] The Commission could conclude that, in order to imply customer approval to use, disclose, or permit access to CPNI, an ISP must provide fair and accurate notice that describes the CPNI it collects, how it will use that CPNI, and whether and for what purposes it may share the CPNI with third parties, as set forth in the Transparency/Notice principle. Similarly, the Commission could conclude that a data breach constitutes the disclosure or provision of access to CPNI without the customer's consent in violation of Section 222(c)(1).[52] The Commission could rely on that same provision to require that ISPs adopt security safeguards in order to prevent breaches.[53] And the flexibility under Section 222(c)(1) that the Commission has previously recognized would allow ISPs to continue to rely on implied consent for first-party marketing, as implied consent has been permitted in such situations for decades.

---

[50] *See* App. B.

[51] *See* 47 U.S.C. § 222(c)(1).

[52] *See id.*

[53] The Commission has already concluded it has the authority to require telecom carriers to take steps under Section 222 to prevent data breaches. *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd. 6927, ¶ 27 (2007).

2. Multistakeholder processes may be a useful alternative to rules.

In the alternative, Comcast believes pursuing a multistakeholder process could be workable here, *but only if done before and in lieu of the Commission adopting any rules, not as a sidekick or supplemental form of regulation*. Leveraging multistakeholder processes would be consistent with the Administration's policy regarding Internet governance and questions of consumer privacy on the Internet, and it is a model that has been deployed to great effect.[54] These kinds of successes strongly suggest that the Commission could leverage this model to accomplish its goals in this proceeding without risking the important national policy goals of encouraging innovation, investment, and competition.

Such a process could be useful "to address the privacy practices of broadband providers more generally, or in other specific areas"[55] so that the Commission would fully understand current marketplace practices, as well as the potential costs and benefits of imposing certain possible regulations, *before* regulations are adopted. This process, which should involve and draw on the experience that both the FTC and NTIA have had with the multistakeholder model, would provide a reasonable and effective path for the Commission to pursue as an alternative to adopting rules.

* * *

In short, the Administration and the FTC for many years have espoused a technology-neutral policy towards consumer privacy on the Internet that has rested on the flexible implementation of principles such as transparency/notice, choice/respect for context, and data

---

[54] *See* NTIA, Privacy Multistakeholder Process: Facial Recognition Technology, https://www.ntia.doc.gov/other-publication/2016/privacy-multistakeholder-process-facial-recognition-technology (initiated December 3, 2013); NTIA Multistakeholder Process: Unmanned Aircraft Systems, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-unmanned-aircraft-systems (initiated on March 5, 2015).

[55] *NPRM* ¶ 293.

security. These policies have been successful in protecting consumers and promoting unprecedented innovation and investment; rather than diverge from these policies as the NPRM's proposals would do, the FCC should adhere to them. The Consensus Privacy Framework sets out a roadmap for how these policies could be translated specifically for ISPs.

III. THERE IS NO JUSTIFICATION FOR ABANDONING THE SENSIBLE FTC AND ADMINISTRATION PRIVACY FRAMEWORK AND APPLYING HIGHLY RESTRICTIVE RULES SOLELY TO ISPS.

In light of the success of the FTC's and Administration's privacy regime, the fact that it was developed over the course of years of study and application, and the high cost to consumer welfare associated with privacy rules that fail to strike an appropriate balance between promoting privacy and encouraging investment, the prudent approach for the FCC would be to simply incorporate those principles as described in the prior section. Chairman Wheeler has essentially stated that this is the right approach. As he observed, "What the FTC has done in that regard is to build a terrific model and so I think one of our challenges is to make sure we're consistent with the kind of thoughtful, rational approach that the FTC has taken."[56]

But that is not what the Commission has proposed in the NPRM – it is not even close. Instead, the FCC proposes to completely abandon the FTC's and Administration's approach in favor of what would be the most restrictive and onerous privacy regime ever adopted in this country – and to apply that approach only to ISPs. The proposed regime is essentially an even more onerous version of the legacy CPNI rules that the Commission designed primarily for telephone service providers. Under the FCC's proposal, ISPs would be required to obtain opt-in customer consent for many of the same exact types of collection and use for which *no consent* –

[56] Margaret Harding McGill, *FCC, FTC Chiefs Zero In on Data Security, Privacy*, Law360 (Jan. 6, 2016) (reporting Chairman Wheeler's remarks during a conversation with Gary Shapiro, president and CEO of the Consumer Technology Association at the Consumer Technology Association show).

or at most opt-out consent – is required under the FTC regime or the Administration's Consumer Privacy Bill of Rights.

The use of opt-in consent is especially troubling because well-established data show that opt-in consent mechanisms typically result in very low click rates.[57] By proposing to flip the existing privacy framework on its head in this key aspect alone and solely for ISPs would thus upend established marketing, advertising, and other business initiatives developed and implemented by ISPs in full compliance with the FTC framework.

A. Claims that Onerous Privacy Rules Are Required Solely for ISPs Based on Their Putative Unique Ability to Collect and Use Comprehensive Consumer Data Are Inconsistent with Marketplace Facts.

The NPRM suggests that imposing more onerous privacy rules solely on ISPs may be justified because ISPs have a unique ability to collect comprehensive online data from their customers.[58] But these unsubstantiated assertions simply not true. In reality, ISPs have limited – and diminishing – access to consumer data, whereas companies that would not be covered by the Commission's rules have access to the same information that would be covered by the ISP-only rules. In fact, the FTC expressly studied this issue back in 2012 and found in its 2012 Privacy Report that "[a]ny privacy framework should be technology neutral. ISPs are just one type of large platform provider [along with operating systems, browsers, and social media services] that may have access to all or nearly all of a consumer's online activity."[59] The NPRM completely

---

[57] *See* Mindi Chahal, *Consumers less likely to 'opt in' to marketing than to 'opt out,'* Marketing Week (May 7, 2014), https://www.marketingweek.com/2014/05/07/consumers-less-likely-to-opt-in-to-marketing-than-to-opt-out/.

[58] *NPRM* ¶¶ 4, 265.

[59] *2012 FTC Privacy Report* at 56. The FTC confirmed this conclusion after further analyzing the issue in a workshop on large platform providers in December 2012, after which staff reiterated that ISPs' data collection and use practices are not unique and that government should avoid picking winners and losers, and instead should maintain a technology-neutral online privacy regime. Maneesha Mithal, FTC, Remarks at The Big Picture: Comprehensive Online Data Collection FTC Workshop, Transcript, at 272-73 (Dec. 6, 2012),

ignores these key FTC findings and instead pretends as if the FTC had previously found that ISPs were the *only* large platform provider studied and that ISPs presented unique privacy concerns that must be uniquely addressed with more onerous restrictions.[60]

The reality is that any one ISP is the conduit for only a fraction of a typical user's online activity. This is because consumers increasingly use a number of different devices across multiple ISPs for Internet access. As Professor Swire has explained, today the average Internet user has over six connected devices, many of which are mobile and connect from diverse and changing locations that are served by multiple ISPs.[61] Consumers today connect to the Internet from virtually any and every location due to the availability of mobile connectivity over wireless and Wi-Fi networks. In 2014, Ericsson found that 97% of U.S. households had a mobile phone and 64% of consumers reported that "they use the Internet everywhere – indoors, outdoors and in vehicles."[62] And as Maneesha Mithal, Associate Director of the Division of Privacy and Identity Protection, FTC, observed in her closing remarks at the FTC's 2012 large platform provider workshop, "consumers are accessing the Internet through all sorts of different channels at work, at home, through their mobile devices."[63]

---

https://www.ftc.gov/sites/default/files/documents/public_events/The%20Big%20Picture%3A%20Comprehensive%20Online%20Data%20Collection/bigpicture_transcript_21206ftc.pdf.

[60] *See, e.g.*, *NPRM* ¶ 4 (selectively citing and quoting the FTC's 2012 Privacy Report solely with respect to ISPs and ignoring the FTC's conclusions that operating systems, browsers, and social media platforms are large platform providers, and also ignoring key FTC conclusions that none of these entities warrant special regulations and that instead a technology-neutral approach is best for online privacy regulation).

[61] *Swire Paper* at 7; Ericsson, North America Ericsson Mobility Report Appendix, at 2 (June 2015), http://www.ericsson.com/res/docs/2015/ericsson-mobility-report-june-2015-rnam-appendices.pdf (reporting that in 2014 50% of U.S. households had five or more Internet connected devices and 90% of U.S. households had at least three Internet connected devices).

[62] Ericsson, North America Ericsson Mobility Report Appendix, at 3 (June 2015), http://www.ericsson.com/res/docs/2015/ericsson-mobility-report-june-2015-rnam-appendices.pdf.

[63] Maneesha Mithal, FTC, Remarks at The Big Picture: Comprehensive Online Data Collection FTC Workshop, Transcript, at 272-73 (Dec. 6, 2012),

ISPs' visibility into the Internet behavior of their customers is also limited because more and more of the traffic that they do carry is encrypted by a third party. Where traffic is encrypted using HTTPS, the ISP only sees the top-level domain used to deliver packets, but otherwise is prevented from seeing either the contents of packets received or transmitted by the customer, or the full website address (i.e., uniform resource locator, or "URL") of the websites that the customer visits.[64] For example, Sandvine, a prominent manufacturer of network equipment, has explained that when traffic is encrypted, Sandvine's equipment can see the website to which the user is connecting but "cannot tell . . . exactly what you're watching listening to, saying, reading or writing."[65]

The percentage of Internet traffic that is encrypted is relatively high and rising rapidly. Professor Swire reports that "the HTTPS portion of total traffic has risen from 13 percent to 49 percent just since April 2014."[66] Professor Swire also notes that all 10 of the top websites and 42 of the top 50 websites either use HTTPS by default, or shift to HTTPS when users log in to the site.[67] For example, Google accounts for 93% of organic search traffic worldwide and, in 2013, accounted for nearly 25% of Internet traffic in North America.[68] As of January 2016, Google

---

https://www.ftc.gov/sites/default/files/documents/public_events/The%20Big%20Picture%3A%20Comprehensive%20Online%20Data%20Collection/bigpicture_transcript_21206ftc.pdf.

[64] *Swire Paper* at 27. In contrast, web browsers have the technical ability to access both the full URLs of the websites a user visits and the specific content of those URLs, which provides significantly more information about what the customer is looking at on the website. *Id.*

[65] *See* Robert Hackett, *Most Internet traffic will be encrypted by year end. Here's why.*, Fortune (Apr. 30, 2015), http://fortune.com/2015/04/30/netflix-internet-traffic-encrypted/.

[66] *Swire Paper* at 3, 38 (reporting statistics derived from Center for Applied Internet Data Analysis data).

[67] *Id.* at 28.

[68] *See* eMarketer, *How Much Search Traffic Actually Comes from Googling?* (Jan. 13, 2015), http://www.emarketer.com/Article/How-Much-Search-Traffic-Actually-Comes-Googling/1011814; Dara Kerr, *Google sets Internet record with 25 percent of U.S. traffic*, CNET (July 22, 2013), http://www.cnet.com/news/google-sets-internet-record-with-25-percent-of-u-s-traffic/.

reports that over 75% of its Internet requests across its products and services use encryption, up from over 50% at the beginning of 2014.[69] Sandvine estimates that "by the end of 2016, global Internet traffic will be more than 70% encrypted, with some networks surpassing the 80% threshold."[70] As Professor Swire concluded, as the overall percentage of encrypted traffic increases, ISPs have severely diminishing visibility into consumers' Internet traffic.[71]

In contrast to ISPs' limited ability to access consumer's web traffic, many non-ISP content and service providers are able to collect significant amounts of information due to the numerous ways in which they interact with and track consumers across devices and Internet connections. These other types of entities have access to an enormous amount of consumer information.[72] For example, as the White House has observed, "[t]he 'data services' sector . . . encompasses a class of businesses that collect data across many sources, aggregate and analyze it, and then share that information, or information derived from it."[73] These brokers are able to create profiles of individual consumers that "can be exceptionally detailed, containing upwards of thousands of pieces of data."[74] These data brokers typically do not have direct relationships with consumers – as detailed above, there are any number of ways that non-ISPs are collecting

---

[69] Google Transparency Report, https://www.google.com/transparencyreport/https/ (last visited Apr. 27, 2016).

[70] Sandvine, *2016 Global Internet Phenomena Spotlight: Encrypted Internet Traffic*, at 4-6, 11 (Feb. 25, 2016), https://www.sandvine.com/downloads/general/global-internet-phenomena/2016/global-internet-phenomena-spotlight-encrypted-internet-traffic.pdf (reporting that 37.5% of web traffic on wired networks and 64.5% of mobile traffic is encrypted).

[71] *Swire Paper* at 3-4.

[72] *Swire Paper* at 4 ("At the same time that the above technological and marketplace developments are reducing the online visibility of ISPs, non-ISPs are increasingly gathering commercially valuable information about online user activity from multiple contexts.").

[73] Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, White House Report, at 43 (May 2014), https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf ("*2014 White House Big Data Report*").

[74] *Id.* at 44.

information about consumers directly and then providing it to the data brokers for compilation and analysis.[75]

Similarly, browsers have access to enormous volumes of customer information. As one commentator recently observed, "the best place to be in the Internet to track users is in the browser. . . . The browser knows if I read the pages I visit because it sees me scrolling and tracks my mouse clicks. It knows when I forward links to the pages I read to others. And it knows which paragraphs I re-read. The browser 'is just taking you to get that information' and it knows more about what you're doing than the network operator does."[76]

Importantly, non-ISPs have access to the *same information* to which ISPs have access, and, as Professor Swire found, *often much more*.[77] Because non-ISPs will not be subject to the rules proposed in the NPRM, they will be able to use and disclose the information to which ISPs have access without complying with the rules proposed by the Commission. A leading consumer privacy advocate, EPIC, has highlighted this fundamental flaw in the NPRM's premises:

> [The FCC's] narrow focus on ISPs misses a significant portion of invasive tracking practices that threaten the privacy of consumers' online communications. . . . ***[as] many of the largest email, search, and social media companies exceed the scope and data collection activities of ISPs***. . . . ***The current description of the problem presents ISPs as the most significant component of online communications that pose the greatest threat to consumer privacy. This description is inconsistent with the reality of the online communications ecosystem***, incorrectly frames the scope of communications privacy issues facing Americans today, and is counterproductive to consumer privacy.[78]

---

[75] *Id.*

[76] Richard Bennett, *Privacy and the Internet: What the FCC Doesn't Get*, HighTech Forum (May 17, 2016), http://hightechforum.org/privacy-internet-fcc-doesnt-get/.

[77] *Swire Paper* at 3-4.

[78] Claire Gartland et al., *FCC Communications Privacy Rulemaking*, EPIC Memorandum, 1 (Mar. 18, 2016), https://epic.org/privacy/consumer/EPIC-Draft-FCC-Privacy-Rules.pdf (emphasis added); *see also* Rick Boucher, *Consumer internet privacy: Leaving the back door unlocked*, (May 25, 2016), http://thehill.com/blogs/congress-blog/technology/280603-consumer-internet-privacy-leaving-the-backdoor-unlocked ("Singling out one segment of the internet ecosystem for special and more onerous treatment is flawed policy.").

Consistent with this analysis, another leading consumer privacy advocate, CDT, previously called for *technology-neutral* online privacy regulation in 2012 when the FTC was studying whether unique regulations should be imposed on ISPs:

> There are all kinds of technologies that can be used for essentially very similar purposes and not just on a sector-by-sector basis, but even what can a network operator use. What can an operating system vendor use? What can a device maker use to do data collection? ***I really think we should stay away from trying to evaluate these practices on the basis on which technology is being used***, in part, because I think DPI does have bad name now for various reasons. . . . ***So[I] think extreme caution necessary on trying to be technology-specific***.[79]

Additionally, non-ISPs that have affiliate relationships with many different types of Internet businesses are able to track users across multiple websites, apps, devices, services, and locations, and compile extensive and comprehensive consumer profiles across those platforms. Google is the most notable example of this. Google uses its platform to provide a host of novel and innovative services, which benefits consumers in numerous ways. But there can be little doubt that non-ISPs like Google, ad networks, data brokers, and the other entities analyzed in Professor Swire's report have access to consumer information that far exceeds a stand-alone ISP's access to information.

At the recent Senate hearing on privacy, Chairman Wheeler attempted to contrast what an ISP can collect from its customers with what a website can collect. The Chairman concluded that "Only one entity connects *all* of that information . . . and can turn around and monetize it."[80]

---

[79] Alissa Cooper, Chief Computer Scientist, Center for Democracy and Technology, FTC's The Big Picture Comprehensive Online Data Collection, Transcript, at 267-68 (Dec. 6. 2012), https://www.ftc.gov/sites/default/files/documents/public_events/The%20Big%20Picture:%20Comprehensive%20Online%20Data%20Collection/bigpicture_transcript_21206ftc.pdf (emphasis added).

[80] *Examining the Proposed FCC Privacy Rules: Hearing Before the Subcomm. on Privacy, Technology and the Law of the Senate Comm. on the Judiciary*, 115th Cong. (May 11, 2016) (statement of Tom Wheeler, Chairman, FCC), http://www.c-span.org/video/?409389-1/fcc-commissioners-testify-proposed-internet-privacy-rules (starting at 01:16:56); Stacey Gray, *Comprehensive Online Tracking Is Not Unique to ISPs*, Future of Privacy Forum (May 20, 2016), https://fpf.org/2016/05/20/14382/ (reporting statements by Chairman Wheeler at the May 11, 2016 Senate hearing on the FCC's privacy NPRM).

But as several Internet experts have subsequently pointed out, that is not how the Internet works, and in fact, there is a tremendous amount of additional data being collected and used by many non-ISPs behind the scenes. For instance, as the Future of Privacy Forum has explained in response to Chairman Wheeler's statement:

> ***[Chairman Wheeler's] framing of the issue reflects a fundamental misunderstanding of the current online advertising ecosystem*** …. ***After installing the Firefox browser and visiting only one website (WebMD.com) (See Fig. 1, below), I have connected with 24 third party sites. After visiting three additional sites – for a grand total of four websites – I have connected with 119 third party entities*** (see Fig. 2, below). . . . But even for those that are not directly connected to a particular site, third party entities who are linked are capable of buying and selling this data at third party data exchanges. ***These data exchanges, by linking and compiling data from hundreds of different online and offline sources, can "match up" consumer behavior across the Internet, creating comprehensive and detailed individual profiles***. The third party advertising networks and data partners visualized above use a variety of methods designed to create comprehensive profiles of a user's entire web browsing history. This includes persistent identifiers (cookies), IP addresses, device identifiers, direct authentication (such as email addresses), or probabilistic methods (such as browser fingerprinting). For a more extensive explanation of these tracking methods, see our 2015 report on Cross-Device Tracking. Furthermore, this information can be combined with ***offline*** data (appended data), such as a user's in-store purchase history, for an even more comprehensive consumer profile. Many of the leading online platforms also correlate data across websites. For example, many websites (including WebMD, seen above) carry social media plug-ins that allow those social media platforms to compile browsing histories of individuals across the Internet and link that browsing activity to the same user's social media behavior. . . . ***Despite industry efforts, for many advocates and consumers the comprehensive and pervasive nature of online tracking continues to be debated. But one thing is certain: it is not unique to ISPs.***[81]

Moreover, the Internet of Things is radically increasing the number of devices connected to the Internet and will likely also radically increase the amount and type of information

---

[81] Stacey Gray, *Comprehensive Online Tracking is Not Unique to ISPs*, Future of Privacy Forum (May 20, 2016), https://fpf.org/2016/05/20/14382/ (emphasis added); *see also* Scott Cleland, *Google's Omnipresent Tracking Much Harder to Leave than an ISP for Privacy*, Precursor Blog, (May 17, 2016) http://www.precursorblog.com/?q=content/google%E2%80%99s-omnipresent-tracking-much-harder-leave-isp-privacy ("What I do respectfully challenge [of what Chairman Wheeler said] is that first, Google essentially doesn't "*collect all of that information*" because they do (see [http://googlemonitor.com/wp-content/uploads/2016/05/Google-is-Biggest-Privacy-Risk-With-Least-FTC-FCC-Privacy-Accountability.pdf]), and second, that Google somehow is easy to escape, when it comes to collecting one's private information, because it is not, as I will prove below.").

collected by companies other than ISPs in the Internet ecosystem. For example, Amazon now offers a device called the "Amazon Echo," which uses voice recognition technology to perform tasks such as answering questions by searching the Internet, providing information on the weather, traffic, sports, and local news, checking account balances for bank and credit card accounts, controlling lights, switches, and thermostats, tracking your vehicle location, and ordering pizza or an Uber.[82] Devices like this that know substantial and intimate details about consumers' lives are becoming more and more prevalent.[83]

Of course, the FTC has already studied the privacy implications of the Internet of Things and published a helpful paper just last year on this topic, and the Administration has begun a proceeding to learn more.[84] Importantly, in its report, the FTC (1) again, did *not* single out ISPs as a basis for unique privacy concerns, but instead maintained the same technology-neutral approach it always has, and (2) confirmed that the notice and choice principles adopted in the FTC's 2012 Privacy Report "appl[y] equally to the Internet of Things," including application of

---

[82] *See* Amazon Echo, http://www.amazon.com/Amazon-SK705DI-Echo/dp/B00X4WHP5E; Heather Kelly, *Eight odd tricks to try with your Amazon Echo*, CNN Money (Mar. 11, 2016), http://money.cnn.com/2016/03/11/technology/amazon-echo-tricks/.

[83] *See* Farhad Manjoo, *The Echo from Amazon Brims with Groundbreaking Promise*, N.Y. Times (Mar. 9, 2016), http://www.nytimes.com/2016/03/10/technology/the-echo-from-amazon-brims-with-groundbreaking-promise.html?_r=0 ("Amazon would be wise to step on the gas because while the Echo has no direct competitors, a few may be emerging. Among them is SoundHound, a start-up that has been working on voice-recognition for more than a decade, which is now offering hardware makers access to its service. Within the next year, according to the company, lots of gadgets will be using SoundHound's software to talk to users."); Hayley Tsukayama, *Why Google's Chirp could be better than Amazon's Alexa*, Wash. Post (May 12, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/05/12/why-googles-chirp-could-be-better-than-amazons-alexa/; Dieter Bohn, *Google Home: a speaker to finally take on the Amazon Echo*, The Verge (May 18, 2016), http://www.theverge.com/2016/5/18/11688376/google-home-speaker-announced-virtual-assistant-io-2016 (describing Google's new device "Google Home" and the various data that will be accessible to this device and the other devices it will interact with).

[84] *See* Press Release, Federal Trade Commission, FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks (Jan. 27, 2015), https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices; NTIA, *The Benefits, Challenges, and Potential Rules for the Government in Fostering the Advancement of the Internet of Things*, Request for Comment 91 Fed. Reg. 19956 (Apr. 6, 2016).

opt-in consent to sensitive data and implied consent or opt-out consent for other data, uses, and disclosures.[85] So there is no basis for the FCC or others to claim that any *potential future* data collection that may arise in connection with the Internet of Things justifies different privacy restrictions imposed on ISPs.

B. There Is No Evidence that Consumers Support the Imposition of Different – and More Onerous – Privacy Rules Solely on ISPs.

The objective of protecting consumers' privacy can only be defined by reference to the actual expectations and preferences of consumers themselves. In the NPRM, the Commission seems to assume that consumers support tighter privacy regulations for ISPs. But the Commission does not cite any basis for this conclusion, which is not surprising, because there is no basis for it. *In fact, extensive survey data from reputable independent organizations show that consumers tend to trust their ISPs as much if not more than many other entities in the Internet ecosystem*.[86]

For example, as the chart in Appendix A illustrates, consumers consistently trust ISPs with their private information *more* than other companies in the Internet ecosystem with that information. Some examples of surveys that reflect this fact include the following:

- A recent 2016 report by the Information Technology & Innovation Foundation indicated that, after themselves, people expressed more trust in ISPs to protect their privacy than any other entity or regime, including government, search engines, and browsers.[87]

---

[85] *See* FTC, *Internet of Things: Privacy & Security in a Connected World*, FTC Staff Report, at 39-46. (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf ("*2015 FTC IoT Report*").

[86] *See* App. A.

[87] *See* Doug Brake, et al., *Broadband Privacy: The Folly of Sector-Specific Regulation*, Information Technology and Innovation Foundation, 4-5 (Mar. 2016), http://www2.itif.org/2016-broadband-privacy-folly.pdf (citing TRUSTe & Harris Interactive, *2011 Consumer Research Results Privacy and Online Behavioral Advertising*, (July 25, 2011), https://www.eff.org/files/truste-2011-consumer-behavioral-advertising-survey-results.pdf).

- In 2014, GfK conducted a survey wherein 54% of respondents said they trusted ISPs with personal data completely or mostly, well above providers of online services (47%) and online social networks (39%).[88]

- A 2015 Pew Research Center survey found that edge providers "are among the least trusted entities when it comes to keeping information private and secure" with consumers rating cable and telephone companies as more trustworthy than most edge providers.[89]

- A 2015 global digital consumer survey conducted by Accenture found that digital consumers consider "telecom operators" and "banks" as being the two categories of companies most trusted to handle their personal data, explaining that these companies "have had access to personal information for quite some time and have gradually built a level of trust."[90]

- In a 2015 study by the National Cyber Security Alliance, ISPs ranked fifth on the list of the 16 institutions that consumers rated for trustworthiness to responsibly use personal information provided to them, and third out of 16 for institutions consumers rated for trustworthiness to responsibly use personal information collected without consumers' knowledge.[91]

- A 2015 study by Columbia Business School found that 49% of U.S. respondents were "very comfortable" or "somewhat comfortable" with how the telecommunications industry handles their personal data, placing the telecommunications industry in second place behind financial services. In contrast, only 35% and 33% of customers were very comfortable or somewhat comfortable with how web services companies and e-commerce companies, respectively, handling their data.[92]

- In May 2015, the Harvard Business Review published the results of a survey in which 73% of respondents said that telecommunications carriers were either "completely

---

[88] GfK, *Survey on Data Privacy and Trust*, at 22 (2014); *see also*, Press Release, GfK, New GfK US Survey Reveals Growing Concerns over Data Privacy, Desire for Corporate and Government Action, (Apr. 4, 2014), http://www.gfk.com/insights/press-release/new-gfk-us-survey-reveals-growing-concerns-over-data-privacy-desire-for-corporate-and-government-action-1/.

[89] Mary Madden & Lee Rainie, *American Attitudes about Privacy, Security and Surveillance*, Pew Research Center, at 7 (May 20, 2015), http://www.pewinternet.org/files/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf.

[90] Accenture, *Digital Trust in the IoT Era*, at 7 (2015), https://www.accenture.com/t20160318T035041__w__/us-en/_acnmedia/Accenture/Conversion-Assets/LandingPage/Documents/3/Accenture-3-LT-3-Digital-Trust-IoT-Era.pdf (reporting that whereas 33% of respondents said they trusted telecom operators and banks, only 22% said they trusted search engines, 17% said they trusted social media, and 11% said they trusted online retail companies).

[91] National Cyber Security Alliance, *Perceptions of Privacy Online and in the Digitally Connected World* at 4-5 (Jan. 28, 2015), https://iapp.org/media/pdf/resource_center/DPD_Research_Summary_Jan-2015.pdf.

[92] Matthew Quint & David Rogers, *What Is the Future of Data Sharing: Consumer Mindsets and the Power of Brands*, Columbia Business School, at 14 (Oct. 2015), http://www8.gsb.columbia.edu/globalbrands/research/future-of-data-sharing.

trustworthy" or "trustworthy" with respect to ensuring that personal data was not misused.[93]

The results of each of these surveys demonstrate that consumers do not perceive their ISPs as a particular threat to their personal privacy.

Moreover, a recent national survey of Internet users conducted by Public Opinion Strategies & Peter D. Hart included the following key findings that are squarely inconsistent with key premises of the FCC's proposed rules:

- ***By an overwhelming margin, Internet users strongly agree that all Internet companies should operate under the same set of privacy rules and regulations***. By an overwhelming 90%-8% margin, Internet users indicated their view that "all Internet companies should operate under the same set of rules and regulations so that standards are fair and equal across the board," including 74% of Internet users who say they "strongly" agree with that statement.[94]

- ***By an 83%-12% margin, Internet users say their online privacy should be protected based on the sensitivity of their online data, rather than by the type of Internet company that uses their data.***[95]

These findings undermine the Commission's entire proposal for ISP-specific privacy regulations. They clearly show that there is no basis for concluding that consumers expect or support tighter privacy rules for ISPs; rather, these findings fully support the conclusion that the NPRM's proposed approach must be abandoned in favor of the Consensus Privacy Framework.

---

[93] Timothy Morey, Theodore Forbath, & Allison Schoop, *Consumer Data: Designing for Transparency and Trust*, Harvard Business Review (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust (surveying 900 people in the United States, the United Kingdom, Germany, China, and India).

[94] Neil Newhouse, Robert Blizzard, & Peter D. Hart, *Key Findings from Recent National Survey of Internet Users*, Progressive Policy Institute Memorandum, at 2 (May 26, 2016), http://www.progressivepolicy.org/wp-content/uploads/2016/05/Internet-User-National-Survey-May-23-25-Key-Findings-Memo.pdf (emphasis added).

[95] *Id.* at 3.

C. ISPs Have a Positive Track Record in Protecting Consumer Privacy and Have Powerful Marketplace-Based Incentives to Maintain That Record.

ISPs have a strong track record of protecting their customers' personal information and well-recognized market-driven incentives to continue to do so. This further contradicts the logic and key assumptions underlying the Commission's proposal. In this respect, the NPRM correctly observes that "[t]he importance of privacy protection is certainly not new to the nation's largest broadband providers."[96] ISPs have made the security of their customers' information a priority, and as the Commission moves forward in this proceeding, it should look back at the facts regarding how ISPs have behaved with respect to protecting customer data. Actual experience under the FTC regime shows that ISPs have strong incentives to protect consumers' privacy and act on those incentives by implementing robust privacy and security practices and by acting responsibly in their uses of customer information.

1. ISPs have a strong track record of protecting consumer privacy.

The NPRM recognizes that the FTC has been willing and able to use its authority under Section 5 of the FTC Act to take action against behavior that harms or deceives consumers.[97] In all the time during which ISPs were subject to FTC oversight, however, there were very few ISP-related privacy or data security issues. In one case, the FTC investigated Verizon for unfair and deceptive practices, but closed the investigation without finding a violation had occurred.[98] In the other, the FTC settled a claim with Level 3 for misrepresenting compliance with the U.S.-E.U. Safe Harbor Framework for transferring personal data outside of Europe.[99]

---

[96] *NPRM* ¶ 10.

[97] *Id.* ¶ 8.

[98] Letter from Maneesha Mithal, Associate Director Division of Privacy and Identity Protection, FTC, to Dana Rosenfeld, Counsel to Verizon (Nov. 12, 2014).

[99] *See Level 3 Communications, LLC*, Decision and Order, FTC Docket No. C-4470 (June 19, 2014).

In contrast, the FTC has pursued at least 11 enforcement actions to curb unfair or deceptive practices by non-ISPs in the last five years. In 10 of these actions, the companies settled with the FTC or were required to comply with permanent injunctions and/or to pay civil penalties.[100] These matters concerned a wide range of conduct.[101] Likewise, the FTC has launched investigations into the privacy and data security practices of device manufacturers which have resulted in two consent decrees.[102]

2. ISPs have unique and powerful incentives to protect consumer privacy, and neither the NPRM's asserted lack of competitive alternatives nor allegedly high switching costs justifies unique ISP regulations.

In its 2002 CPNI rulemaking, the Commission recognized that providers with a pay subscription business, such as ISPs, have little incentive to risk those revenue streams by engaging in inappropriate privacy practices:

> Because of commercial constraints required to ensure customer accountability, therefore, the carrier with whom the customer has the existing business relationship has a strong incentive not to misuse its customers' CPNI or it will risk losing its customers' business.[103]

---

[100] *See Snapchat, Inc.*, Decision and Order, FTC Docket No. C-4501 (Dec. 23, 2014); *United States v. Yelp Inc.*, No. 14-4163, Stipulated Order for Permanent Injunction and Civil Penalty Judgment (N.D. Cal. Sept. 16, 2014); *Fandango, LLC*, Decision and Order, FTC Docket No. C-4481 (Aug. 13, 2014); *United States v. Path, Inc.*, No. 13-448, Consent Decree and Order for Civil Penalties, Permanent Injunction and Other Relief (N.D. Cal. Feb. 8, 2013); *United States v. Google*, No. 12-4177, Order Approving Stipulated Order for Permanent Injunction and Civil Penalty Judgment (N.D. Cal. Nov. 16, 2012); *Myspace LLC.*, Decision and Order, FTC Docket No. C-4369 (Aug. 30, 2012); *Facebook, Inc.*, Decision and Order, FTC Docket No. C-4365 (July 27, 2012); *Upromise, Inc.*, Decision and Order, FTC Docket No. C-4351 (Mar. 27, 2012); *Google Inc.*, Decision and Order, FTC Docket No. C-4336 (Oct. 13, 2011); *Twitter, Inc.*, Decision and Order, FTC Docket No. C-4316 (Mar. 2, 2011).

[101] *See, e.g.*, *Facebook, Inc.*, Decision and Order, FTC Docket No. C-4365 (July 27, 2012) (settling charges for deceptive privacy practices related to the treatment of personal information shared on the site); *Fandango, LLC*, Decision and Order, FTC Docket No. C-4481 (Aug. 13, 2014) (settling charges against Fandango for improperly securing customers' credit card information); *Twitter, Inc.*, Decision and Order, FTC Docket No. C-4316 (Mar. 2, 2011) (settling charges against Twitter over insufficient security practices).

[102] *See TRENDnet, Inc.*, Decision and Order, FTC Docket No. C-4426 (Jan. 26, 2014); *HTC America, Inc.*, Decision and Order, FTC Docket No. C-4406 (June 25, 2013).

[103] *Implementation of Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended, 2000 Biennial Regulatory Review – Review*

Not surprisingly, the FTC has agreed with this principle, as its privacy framework calls for more flexibility and reliance on implied consent when the user has a relationship with the ISP or other provider and when the context of the data collection and use is consistent with that relationship (e.g., an ISP customer likely expects that the ISP will market him or her other services like video, voice, home security, music, energy management, and other services, so privacy restrictions should be reduced).[104]

This principle remains true today. Comcast has found that ensuring a customer's comfort with privacy practices of her ISP is crucial to ensuring that the customer signs up for and stays with Comcast's Internet service. It is simply bad business to use, share, or fail to secure customers' private information in a manner that is inconsistent with consumer expectations.

The NPRM suggests that perhaps ISPs' inherent incentive to protect consumers' privacy is diminished because ISPs do not face sufficient competition, or because consumers have trouble switching to a different ISP.[105] This misses the point and, in any event, is untrue. ISPs' collection and use of data is subject to the same company-wide privacy policy.[106] This means it is the same across all customers, and, as such, would be the same in markets with multiple competitors as in the few markets with only a single provider. In other words, an ISP's privacy practices would be set at the highest, not the lowest, common denominator, so the perceived lack

---

of Policies and Rules Concerning Unauthorized Changes of Consumers' Long Distance Carriers, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd. 14860, ¶ 37 (2002) ("*2002 CPNI Order*").

[104] *2012 See FTC Privacy Report* at 38-39.

[105] *NPRM* ¶ 4.

[106] *See, e.g.*, Comcast, Privacy Notice for Cable Video, High-Speed Internet, Phone, and Home Security Services, http://www.xfinity.com/Corporate/Customers/Policies/CustomerPrivacy.html (last visited May 22, 2016).

of competition in any one particular area should have no bearing on the ISP's privacy practices – or form the basis for harsher ISP regulations.

Moreover, even if the Commission persists in its belief that competition among ISPs is relevant to privacy concerns, it must still account for the fact that ISPs have always been good stewards of their customers' data under the FTC regime – *regardless* of what one may think of the state of competition at any given point in time.[107] No evidence has been presented to suggest that anything has changed in the marketplace to justify the imposition of such onerous regulations. Consumers are protected today just as much as they were prior to Title II reclassification. And in any event, as noted, ISPs are not the only "large platform providers," and competitive alternatives for ISPs are just as numerous as those for other such platforms.

While the NPRM suggests that consumers who do not like the privacy policies of an email provider, social media site, or other edge provider are free to switch to another service, the reality is far more complicated. Many of these online services are characterized by network effects. This means that the value of the service to a consumer is significantly derived from the number of consumers who use the service.[108] For example, Facebook is far more valuable than other social networks because more people use it. This means that it is difficult for a consumer to justify switching to a competitive alternative that has fewer users and is, therefore, less valuable. As one analyst observed, "a person with a year or so of e-mail housed in Gmail is

---

[107] According to the Commission's data, as of December 2014, 89% of American homes lived in census blocks where they have choice of two or more wired ISPs delivering download speeds of at least 10 Mbps, *Internet Access Services: Status as of December 31, 2014*, Industry Analysis and Technology Division, Wireline Competition Bureau, FCC, at 10 (Mar. 2016), which is the Commission's definition of broadband in the universal service context, *Connect America Fund, ETC Annual Reports and Certifications, Petition of USTelecom for Forbearance Pursuant to 47 U.S.C. § 160(c) from Obsolete ILEC Regulatory Obligations that Inhibit Deployment of Next-Generation Networks*, Report and Order, 29 FCC Rcd. 15644, ¶ 15 (2014).

[108] *See* David Easley and Jon Kleinberg, *Networks, Crowds, and Markets: Reasoning about a Highly Connected World*, at 509, 527-28 (2010).

highly unlikely to switch as a practical matter."[109] And economists and analysts have recognized that "[t]he 'experience effects,' . . . of users and advertisers familiar with Google's services make them less likely to switch."[110]

Beyond network effects, these services are also subject to meaningful switching costs. Users that have spent the time to learn how a service works, establish contacts, and build up data on the platform face numerous administrative costs in switching to another service. Analysts have recognized that switching costs, e.g., lack of data portability, can lock users into a service, and that these concerns are present in the context of online platforms such as social networks.[111] They have similarly recognized that these platforms have incentives to develop products that are incompatible with rival services to deter users from switching services.[112] But even when the data is portable and products are compatible, the administrative burden of switching from one provider to another may be so high that the user simply will choose not to switch. Others who have analyzed the costs of switching between Android and iPhone mobile operating systems have likewise concluded, "Given the headaches of switching, most people avoid it."[113]

---

[109] *See* Steve Lohr, *Google, the new master of network effects*, N.Y. Times (July 7, 2008), http://www.nytimes.com/2008/07/07/technology/07iht-07google.14282611.html?_r=0.

[110] *Id.*

[111] *See, e.g.*, Christopher Yoo, *When Antitrust Met Facebook*, 19 George Mason L. Rev. 1147, 1154-55 (2012) ("Another potential source of monopoly power is the absence of data portability. The most frequently cited concern is that the inability to move data from one social networking site to another can create a form of lock-in.").

[112] *See id.* at 1156.

[113] Vindu Goel, *How to Switch to iPhone From Android: Patience and Persistence*, N.Y. Times (Apr. 6, 2016), http://www.nytimes.com/2016/04/07/technology/personaltech/how-to-switch-to-iphone-from-android-patience-and-persistence.html?smprod=nytcore-iphone&smid=nytcore-iphone-share&_r=0 ("A lot of contacts and photos never made it through. It was as if a moving company had lost half my stuff during a cross-country haul. . . . Michael R. Levin, partner and co-founder of Consumer Intelligence Research Partners, which surveys smartphone users in the United States, said only about one out of five people activating a new iPhone or Android was switching from the other platform. 'In the past two years, the loyalty and switching rates have gotten very, very set,' he said."); *see also* Damon Darlin, *Amazon's Fire and the Real Cost of Switching Phones*, N.Y. Times (June 18, 2014), http://www.nytimes.com/2014/06/19/upshot/amazons-fire-the-real-cost-of-switching-phones.html?smprod=nytcore-iphone&smid=nytcore-iphone-share&_r=0 ("The friction isn't in slipping a Benjamin from your wallet but the agony — or the belief there will be agony — of learning how to use it, of finding new apps, of loading those apps, of

By contrast, in 2010, the FCC conducted a survey finding that one out of six customers switch wireline providers every year and that over the prior three years, 36% of Internet users had indicated that they had switched their provider, with 13% of users switching providers more than once, and almost one-third of those who had not switched providers having considered doing so.[114]

In short, whether viewed through the lens of ISPs' incentives to protect consumer privacy, the availability of competitive alternatives, and/or the incentives and costs of customers to switch services, ISPs fare very well when compared to non-ISPs. So any suggested bases for unique and onerous ISP privacy regulations are as unfounded as they are illusory.

IV. THE COMMISSION'S PROPOSALS WILL HARM CONSUMERS IN NUMEROUS WAYS.

In addition to being wholly unsupported by the facts, the Commission's proposed rules would affirmatively harm consumers and undermine other important policy objectives.

A. The Proposed Rules Would Cause Significant Consumer Confusion.

Two of the key tenets of the FTC's regime and Administration's Consumer Privacy Bill of Rights are transparency and choice, including making privacy practices as simple and clear as possible so that consumers can make informed decisions.[115] But the FCC's proposal would run directly counter to these principles by making it *harder* for consumers to understand the privacy rules that apply to their online information.

---

never again using a favorite app, of moving your contact list over, of losing all the text messages you sent, or of worrying that the movies and music you had on one system won't work on the other. How do you value that? It's easier to sit where you are.").

[114] FCC, *Broadband Decisions: What Drives Consumers to Switch—Or Stick With—Their Broadband Internet Provider*, at 2-3 (FCC Working Paper, Dec. 2010).

[115] *2012 FTC Privacy Report* at 60-64.

Consumers may reasonably believe that the FCC's new rules apply to all companies in the Internet ecosystem. "Consumers are unlikely to understand if asked to consent to ISP uses of information that the consumer choices apply only to the ISP and would have no bearing on use of consumer data elsewhere in the Internet ecosystem."[116] Where a set of rules applies to companies in the same ecosystem differently, the government's efforts to regulate one set of companies but not another, are bound to sow confusion, *especially when the same data is at issue*.

Here, because the FCC's proposed rules are very different from the existing privacy framework, they are sure to confound even the most dedicated and privacy-conscious of consumers. Consumers are likely to assume that their data is subject to the same protections as they move around the Internet and between apps, services, and online devices. This, of course, would not be the case because most of their data exposure comes from interaction with *non*-ISPs.

For example, a consumer who declines to provide her ISP with consent to use her information to provide targeted advertising may believe that, in so doing, she has prevented other companies in the Internet ecosystem from sending her targeted advertisements based on her web-browsing history. She would therefore be confused if she later receives targeted ads from various non-ISPs that have access to her web-browsing history (which is common on the Internet given the use of website cookies and other tracking technologies). The consumer might also blame her ISP for failing to honor her refusal to consent to the use of her web-browsing history for advertising, even though the ISP did in fact honor her decision.

[116] Jim Halpert, *Why Privacy Pros Should Care About the FCC's Broadband Privacy Rules*, Privacy Perspectives, iapp (Apr. 5, 2016), https://iapp.org/news/a/why-privacy-professionals-should-care-about-the-fccs-broadband-privacy-rulemaking/.

This confusion is likely to be exacerbated by the fact that the Commission's approach would require notice and consent at multiple points, including potentially a "just-in-time" approach that would almost certainly result in warning fatigue and leave customers confused and frustrated.[117] Analysts have determined that warning fatigue can occur "after just one or two exposures to a new [warning],"[118] and the Commission's proposed regime would likely result in customers receiving many more than two notices. Warning fatigue causes customers to pay less attention to warnings, which in turn reduces the extent to which their responses to the warnings reflect the customers' actual preferences. For example, frequent consent solicitations could cause many customers to reflexively deny consent even if they would grant consent under other circumstances. Such false negatives would likely lead customers to be very confused when they realize they are not being informed about the benefits of discounts, promotions, and services that their neighbors are and to which they might in fact wish to subscribe.

B. The Proposed Rules Would Deprive Consumers of Discounted Bundles and Other Benefits That They Routinely Enjoy Today, and Will Reduce Broadband Investment.

The Commission has long recognized that the ability to offer promotional bundles benefits both consumers, through better prices for Internet and other services, and the public interest, by facilitating additional investment in next-generation broadband networks. Ensuring that the benefits of competition flow to consumers through better products and better prices and expanding the deployment of modern broadband networks are two of the Commission's highest policy priorities. Unfortunately, the Commission's proposal in the NPRM would prevent many ISP customers from ever even learning about – and therefore enjoying – the benefits of

[117] *NPRM* ¶¶ 141-42.

[118] Cristian Bravo-Lillo, et al., *Harder to Ignore?*, Tenth Symposium on Usable Privacy and Security, USENIX Assoc., at 105 (2014), https://www.usenix.org/system/files/soups14-paper-bravo-lillo.pdf.

discounted bundles, as well as many other promotional and lower-priced offerings and innovative new services *that they routinely hear about and subscribe to today*. The result will be a tremendous loss of benefits and value to consumers, reduced broadband investment, and decreased ISP incentives to launch new, innovative services – and all with no corresponding enhancement to consumers' privacy protection.

The Commission has concluded that "bundled services will benefit consumers by driving down prices and improving the quality of service offerings."[119] More recently, the Commission recognized in the AT&T/DIRECTV Order that more than 97% of AT&T's 5.7 million video customers subscribe to bundled services, and nearly 80% of video customers purchase a broadband-video bundle or another bundle.[120] And one of the primary benefits the Commission identified of that transaction was with respect to the benefits of bundles: "We find that the combined AT&T-DIRECTV will increase competition for bundles of video and broadband, which, in turn, will stimulate lower prices, not only for the Applicants' bundles, but also for competitors' bundled products – benefiting consumers and serving the public interest."[121]

The Commission has also explained that the ability to offer additional services over the same network improves the business case for making the kinds of investments necessary to support the deployment of next generation broadband networks.[122] In its 2006 Franchising Order, the Commission concluded that "a provider's ability to offer video service and to deploy broadband networks are linked intrinsically, and the federal goals of enhanced cable competition

---

[119] *Implementation of Section 62l(a)(1) of the Cable Communications Policy Act of 1984 as amended by the Cable Television Consumer Protection and Competition Act of 1992*, 22 FCC Rcd. 5101, ¶ 2 (2006) ("*Franchising Order*").

[120] *Applications of AT&T Inc. and DIRECTV*, 30 FCC Rcd. 9131, ¶ 157 (2015).

[121] *Id.* ¶ 4.

[122] *Franchising Order* ¶ 51.

and rapid broadband deployment are interrelated."[123] And in its recent decision to preempt certain state laws regarding the provision of broadband by municipalities, the Commission concluded that "providers may not always have a business case for building a network unless they can optimize revenue by bundling multiple services. This bundling therefore promotes broadband deployment."[124]

Today, the benefits of bundles go beyond the traditional "triple-play" bundle that has been at the center of the Commission's analysis. Comcast and other ISPs are partnering with companies from diverse areas of the economy to offer innovative services to consumers in new areas like home security, energy management, music, and many other areas.[125] For example, in a few trial markets Comcast has partnered with Sunrun to offer solar-based home energy solutions.[126] Data from these trials show that these solar-based solutions have saved Comcast customers approximately 20-30% on their electricity costs – over $21 million in savings.[127] Comcast also has partnered with competitive energy providers and energy management companies to develop a suite of solutions to help consumers manage their home energy consumption.

---

[123] *Id.* ¶ 62.

[124] *City of Wilson, North Carolina, Petition for Preemption of North Carolina General Statute Sections 160A-340* et seq., *The Electric Power Board of Chattanooga, Tennessee Petition for Preemption of a Portion of Tennessee Code Annotated Section 7-52-601*, Memorandum Opinion and Order, 30 FCC Rcd. 2408, ¶ 79 (2015) ("[T]he inability to offer video services as part of a triple play package places the economic feasibility of investing in broadband infrastructure at risk and may preclude municipal electric providers from competing effectively for business from consumers preferring 'bundled packages' combining broadband, video programming, and telecommunications services.").

[125] *See, e.g.*, Press Release, SunPower Corp., AT&T Plans Renewable Energy System for San Ramon Campus (Oct. 1, 2008), http://newsroom.sunpower.com/press-releases?item=122728.

[126] Xfinity, *Solar savings are big. We're making them bigger*, http://www.sunrun-comcast.com/ (last visited May 27, 2016).

[127] These efforts have yielded significant results not just for those customers who subscribe to these services, but for the public as a whole – over 101 tons of carbon dioxide has been mitigated as a result of these projects.

But for consumers to be in a position to take advantage of the benefits inherent in these and other offers, they need to be informed about them. Under the FTC regime that was in place for ISPs until last February, that assumption was a reasonable one because it was acceptable for an ISP to make offers and inform subscribers about other services the provider offers and the benefits of bundling such services.[128] That is also true of services offered by the ISP's affiliates.[129] As the FTC concluded in its 2012 Privacy Report, most forms of first-party marketing – by companies or their affiliates – do not raise the kinds of concerns that would necessitate *any* form of consumer consent, since such first-party marketing is within the context of the ISP-customer relationship and thus within the expectation of the consumer.[130]

Unfortunately, the Commission's proposed rules introduce additional hurdles that, if adopted, would make it much harder for providers to keep their customers informed about the benefits of bundles, and potentially forestall the viability of other innovative services that could benefit both consumers and the public-at-large. Under the Commission's proposal, ISPs' use of customer data to market "communications-related services" offered by the ISP would be subject, for the first time ever, to opt-out consent.[131] Even more problematic, using this data to market any non-communications-related services offered by the ISP or its affiliates would be subject to opt-in consent under the FCC's proposal.[132]

---

[128] *See, e.g., 2012 FTC Privacy Report* at 39; *2012 White House Consumer Privacy Bill of Rights Report* at 17.

[129] *Id.* at 42.

[130] *Id.* at 38-42. The FTC noted that in cases where a customer might not reasonably understand that an entity was an affiliate of the company, such as where the entities have different names, then opt-out consent should be used for such affiliate marketing. *See id.* at 42.

[131] To be sure, the proposal in the NPRM uses the same terms as the legacy voice CPNI rules, but the proposed interpretations offered in the NPRM suggest that the Commission intends for this new proposal to include significantly *fewer* uses of customer data that are subject to implied consent, which necessarily means that more uses would be subject to both opt-out and, in most cases, opt-in consent.

[132] *NPRM* ¶ 127.

It is well understood that an opt-in consent mechanism results in far fewer individuals conveying their consent than is the case under an opt-out consent mechanism. In fact, a series of studies has shown that people faced with an opt-in choice almost never opt-in even where there are substantial benefits at stake, while others, faced with an opt-out choice, preserve their consent in much higher numbers. For example, studies on enrollment in employer-offered savings plans have found that changing the default participation status from an opt-in to an opt-out model for newly hired employees dramatically increased early participation. Although most employees eventually participated in the companies' savings plans, one study found that initial enrollments jumped from 49% to 86% when the company switched from an opt-out to an opt-in default participation in the plan.[133] In the case of organ donation, where these effects have been studied extensively, studies agree that opt-out regimes lead to much higher rates of donation. A relatively recent study found that the difference in organ donation rates "typically exceed[] 90% in opt-out countries and fail[] to reach even 15% in opt-in countries."[134]

In the marketing context, a rough rule of thumb is that opt-out consent mechanisms may yield approximately 82% or much higher of individuals preserving their consent, whereas an opt-in consent model may yield only approximately 18% or much lower of individuals consenting.[135]

---

[133] *See* Brigitte Madrian & Dennis Shea, *The Power of Suggestion: Inertia in 401(k) Participation and Savings Behavior*, 116 Quarterly Journal of Economics 1149, 1159-61 (Nov. 2001).

[134] Shai Davidai, Thomas Gilvich, & Lee D. Ross, *The Meaning of Default Options for Potential Organ Donors*, 109 PNAS 15201, 15201 (Jul. 30, 2012); *see also* R. W. Gimbel, et al., *Presumed Consent and Other Predictors of Cadaveric Organ Donation in Europe*, 13 Progress in Transplant. 17 (2003) (finding that, in a broad set of European countries during 1999, when donation became the default, donations rose by 56.5%).

[135] *See, e.g.*, Mindi Chahal, *Consumers less likely to 'opt in' to marketing than to 'opt out,'* Marketing Week (May 7, 2014), https://www.marketingweek.com/2014/05/07/consumers-less-likely-to-opt-in-to-marketing-than-to-opt-out/.

The FCC itself previously has recognized the significant variance between participation rates for a given data usage activity based upon whether an opt-in or opt-out choice is offered.[136]

This dramatic difference in consent rates for the two models would have dramatic effects on the ecosystem were the FCC to switch from the current FTC approach to a default opt-in model for certain ISP first-party marketing going forward. Notably, by subjecting all but a small portion of ISPs' consumer data usage and disclosure activities to an opt-in requirement, the Commission would be stepping into the consumers' shoes and ensuring that ISPs will *not* be able to effectively inform consumers about products and services from which they could benefit.

For example, the primary avenue for marketing the above-mentioned home energy solutions is simply identifying Comcast customers and sending them bill inserts and other materials with information about the solutions. But under the Commission's proposal, ISP customer address information for the first time ever could be subject to the Commission's Section 222 rules and, as a result, a significant number of customers may not be informed about the bundled discounts and other benefits available to them. Such unknowing denials will harm consumers.

While an opt-in consent approach may make sense when, for example, sensitive customer data is at issue or when an ISP wishes to make material changes to the privacy promises it previously made to consumers – two areas where the FTC framework calls for opt-in consent – it does not make any sense, and would harm consumers, to overextend an opt-in requirement to areas like an ISP's or its affiliates' use of ISP customer data to market additional products and services to ISP customers. It would especially harm them in this marketplace. All ISP

[136] *2002 CPNI Order* ¶ 62 ("Testimony submitted to the Federal Trade Commission (FTC) shows that opt-out results in disclosure rates of 95 percent, but when the default is opt-in, 85 percent of consumers would choose not to provide their data").

customers have for many years received marketing for lower-priced bundle offerings, promotional discounts for new services, and other offers of value from their ISPs or their affiliates. These customers have substantially benefited from such lower prices and new services. Yet, under the Commission's proposal, most of these customers would never even receive such offers going forward because they would have failed to opt in to the ISPs' use of their data for such purposes in the first place.

How can it make sense to deny the ISP customers in the above examples the benefits of learning of new company offerings and potential attendant price discounts for the existing services the customer receives when the FTC and the Administration in its Consumer Privacy Bill of Rights have concluded for years that such marketing is within the clear expectation of ISP customers? How can it make sense when the federal CAN-SPAM law allows *any* company to send a marketing email to *any* U.S. consumer about *any* product or service, even though that company has *no relationship* with the consumer, subject only to the ability of the consumer to *opt-out* of any such future marketing from the company? The short answer is it does not make any sense.

Accordingly, the Commission should adopt the Consensus Privacy Framework, which would follow the FTC and Administration approach and allow ISPs to market any product or service that the company or its affiliates offer based on implied consent (or opt-out consent where consumers would not reasonably understand an affiliate is part of the company). This approach would avoid the significant consumer harms noted above, and at no cost to consumer privacy. Indeed, all ISP customers have been under this regime for many years, so unless the FCC concludes that the FTC model has been ineffective with respect to regulating ISPs (which

would be inconsistent with the NPRM's broad praise for the FTC model[137]), then there should be no reduction in consumer privacy protection by removing the opt-in consent requirement for first-party marketing.

On the other hand, applying an opt-in consent model to ISPs' first-party marketing would not only harm consumers as described above, it would have other significant negative effects. It would discourage ISPs from investing time and resources in developing new products and services out of a concern that they will not be able to effectively market and monetize them. It would also reduce revenues the ISP receives from discounted bundled offerings, thereby reducing its ability to invest in broadband deployment, upgrades, and innovations, as the FCC previously recognized in the cases cited above.

Finally, it's worth highlighting that even the FCC's own prior statements support a more flexible approach to consent for first-party marketing. In adopting the CPNI rules in 2002, the FCC "reaffirm[ed] our 'total services approach,' which permits the carrier to use CPNI to market new product offerings within the carrier-customer service relationship, on the basis of the customer's implied consent."[138] And in the context of creating the "communications-related services" category, the Commission stated that "we find *the potential harm to privacy to be much less significant* in instances where the entity that uses and shares the CPNI is subject to section

---

[137] *NPRM* ¶¶ 8-9. This FCC conclusion would also be fundamentally inconsistent with the clear statements by FTC Chairwoman Ramirez and FTC Commissioner Ohlhausen at a recent Senate hearing on the FCC's NPRM, in which they both strongly indicated that the FTC's privacy framework has been an effective means of regulating ISPs and other online providers and of protecting consumers' online privacy for decades. *See Examining the Proposed FCC Privacy Rules: Hearing Before the Subcomm. on Privacy, Technology and the Law of the Senate Comm. on the Judiciary*, 115th Cong. (May 11, 2016) (statements of Edith Ramirez, Chairman, FTC and Maureen Ohlhausen, Commissioner, FTC), http://www.c-span.org/video/?409389-1/fcc-commissioners-testify-proposed-internet-privacy-rules (starting at 01:02:40 and 01:10:12).

[138] *2002 CPNI Order* at App. C ¶ 5.

222 and our implementing rules."[139] These statements and the FTC's longstanding view that first-party marketing should be permitted for all of a company's and its affiliates' products and services under an implied consent, or at most an opt-out consent, model, highlights the significant loss in value and benefits that ISP customers will experience if the FCC were to apply an opt-in consent requirement to these activities going forward.

And it is no answer for the Commission to claim that if ISP customers really want those benefits, then they will opt in. The statistics on opt-in consent rates cited above show that this is not the case, and that many individuals will simply not pay attention to the choice or skip past it to get to the service. Rather than convey the consumers' real choice, the opt-in consent requirement so broadly imposed by the FCC's proposal will simply harm many ISP customers who really would prefer to continue to receive the bundled discounts, lower price offers, innovative new services, and other benefits *that they have been receiving for many years under the FTC's privacy framework.*

C. The Proposed Rules Would Block ISPs from Bringing New Competition to the Highly Concentrated Online Advertising Market, Thereby Depriving Consumers and Businesses of Lower Prices and Innovative Service Offerings.

In addition to the harms that the Commission's proposal poses for ISPs' customers, the proposal also poses serious harms for the online advertising market and other markets where firms utilize consumer data as an input. Although the Commission barely addresses this issue in the NPRM, it could have far-reaching consequences for the prices consumers pay for products and services.

[139] *Id.* ¶ 38 (emphases added).

"Since the earliest days of the commercial web, online advertising has been a vital driver of the growth of the Internet."[140] The use of and disclosure of customer information are central to this business. In fact, consumer information has essentially become the currency of the Twenty-First Century online advertising market. To the extent that privacy rules restrict a firm's ability to use and disclose consumer information, such rules are likely to reduce the firm's ability to participate in the market for online advertising. As one commentator has observed, "privacy rules that limit how information can be used and shared across firms will artificially push towards greater consolidation, something that usually works against maintaining robust competition."[141]

Assessing the prospects for entry into the online advertising marketplace is important because that market is highly concentrated. The top ten companies selling advertising in the U.S. online advertising market account for over 70% of total online advertising revenues, which is consistent with the trend over the past ten years during which the concentration of top-10 revenues has fluctuated between 69% and 74%.[142]

Facebook and Google have a particularly strong incumbent position in this market. For example, in 2014, Facebook's digital display ad revenues accounted for just under one-quarter of the US total market and Google's digital display ad revenues accounted for about one-fifth of total market revenues.[143] According to a recent MoffettNathanson Report, today Google and

---

[140] *2014 White House Big Data Report* at 40.

[141] Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud*, 103 Northwestern Univ. L. Rev. 1, 11-12 (2008).

[142] IAB, *Internet Advertising Revenue Report*, at 11 (Oct. 2015), http://www.iab.com/wp-content/uploads/2015/10/IAB_Internet_Advertising_Revenue_Report_HY_2015.pdf.

[143] eMarketer, *Facebook and Twitter Will Take 33% Share of US Digital Display Market by 2017* (Mar. 26, 2015), http://www.emarketer.com/Article/Facebook-Twitter-Will-Take-33-Share-of-US-Digital-Display-Market-by-2017/1012274.

Facebook together control almost 55% of the digital ad market.[144] Facebook alone controls a 65% share of advertising on social media.[145] And Google's dominance in the search market gives it a significant advantage in terms of search-related advertising.[146]

These two companies are extending that dominance into the fastest growing area of online advertising – mobile. In 2014, Google earned an estimated 37% share of the total net U.S. mobile ad revenues, followed by Facebook with a nearly 19% share of U.S. mobile ad revenues.[147] The next closest mobile ad seller was Twitter with a nearly 4% share of ad revenues.[148] Today, Google and Facebook have a combined 67% share of the mobile ad revenue industry, which now accounts for more than 80% of all digital ad growth.[149]

The high level of concentration in this market almost certainly results in prices for advertising that are set above competitive levels. This is in part because the barriers to entry appear to be significant. In order to compete, firms must have access to, among other things, a sufficiently large audience and the technical expertise to navigate the complex web of firms in the advertising ecosystem.

ISPs are among the few companies that have the ability to overcome these barriers to entry. For example, today the dominant online advertisers use a combination of cookies, IP

---

[144] MoffettNathanson, *The Digital Duopoly*, at 1 (May 3, 2016).

[145] *Id.*

[146] As of January 2016, Google led the U.S. search market with a nearly 64% share of explicit core searches. comScore, comScore Releases April 2015 U.S. Desktop Search Engine Rankings (May 15, 2015), https://www.comscore.com/Insights/Rankings/comScore-Releases-January-2016-US-Desktop-Search-Engine-Rankings.

[147] Jack Marshall, *Facebook to Boost Mobile-Ad Market Share, as eMarketer Reverses Forecast*, W.S.J. (Sept. 8, 2015), http://blogs.wsj.com/cmo/2015/09/08/facebook-projected-to-narrow-mobile-ad-gap-with-google-as-emarketer-reverses-forecast/.

[148] *Id.*

[149] MoffettNathanson, *The Digital Duopoly*, at 1 (May 3, 2016).

address, and other technologies to deliver geo-targeted advertisements to consumers. ISPs could compete with these incumbents by offering advertisers the ability to reach consumers with targeted advertisements using much of the same data that online advertisers already use.

Unfortunately, the FCC's proposed rules would prevent this new competition from developing. Application of the sweeping opt-in consent requirement would mean that ISPs are able to make use of far less data that is essential to participate in the online advertising market than all non-ISPs with which it would be competing. For example, if an ISP can only use the IP address of 10-15 of every 100 of its customers who opt-in to develop online ad campaigns, it will not be able to compete with others in the Internet ecosystem that are able to make use of IP addresses for 85-90 or more consumers for every 100 under the opt-out model that applies to them.

The profoundly negative impact on competition would affect political ads as well. Under the FTC's regime, a political candidate could provide a list of zip codes where she wants to have an advertisement delivered online, and the ad network, data broker, or other entity is able to match the IP addresses of users in those zip codes, so that the political ad is delivered to the websites specified by the candidate when users with those IP addresses visit those sites. But under the FCC's proposal, by contrast, an opt-in consent requirement for using this kind of data for this purpose might mean that ISPs would be effectively prohibited from participating in this typical online advertising activity, which delivers ads to groups of users associated with a fairly large geographic area, because it could deliver only 10-15 online targeted ads for every 100 users as compared to 85-90 or more by the edge provider, data broker, or other non-ISP with access to the same data under a more flexible and reasonable opt-out model. As a result, the candidates

would continue to pay more for such website ads because they would be forced to work with the dominant providers in the online advertising sale and delivery markets.

Increased competition in the online advertising market is likely to result in widespread benefits to consumer welfare. Online advertising is an increasingly indispensable means of promoting the sale of consumer products and services.[150] Thus, the costs of online advertising are quickly becoming an unavoidable input to a large number of products and services across the economy.[151] Competition would likely drive down the prices that firms pay for online advertising. Firms in competitive markets have the incentive to pass such lower costs through to customers in the form of lower downstream prices.[152]

Chairman Wheeler has repeatedly claimed that the FCC's core objective is to promote "Competition, Competition, Competition." Here is a perfect opportunity for the Commission to further this goal by adopting sensible broadband privacy rules modeled after the FTC and Administration's approach that would allow ISPs, which are capable new *insurgents* to this highly concentrated market – a market about which a leading industry analyst recently remarked, "We can't think of any other media marketplace with this level of dominance"[153] – to unleash new competition, with significant benefits for consumers, advertisers, and businesses in terms of lower prices and the creation of additional innovative services offerings. Comcast strongly urges

[150] *2014 White House Big Data Report* at 40-41.

[151] Council of Economic Advisors Issue Brief, *Benefits of Competition and Indicators of Market Power*, at 3 (Apr. 2016), https://www.whitehouse.gov/sites/default/files/page/files/20160414_cea_competition_issue_brief.pdf ("Market share may increase as a firm realizes economies of scale, or efficiencies created by larger operations, resulting in lower costs that are passed on to consumers in the form of lower prices.").

[152] *Id.* at 13.

[153] MoffettNathanson, *The Digital Duopoly*, at 3 (May 3, 2016).

the Commission to pursue this path to additional competition rather than unprecedented, unjustified, and unfair targeted ISP regulation.

D. Consumers Would Also Be Harmed if the Commission Prevents ISPs From Offering Innovative Services, Price Discounts, or Other Benefits in Exchange for Customer Consent to Use and Disclose Data for Marketing or Advertising Purposes.

The NPRM seeks comment on whether the Commission should, as part of its adoption of rules in this proceeding, prohibit certain practices outright.[154] The NPRM specifically cites "privacy sharing inducement plans" – i.e., those offers whereby the customer enjoys a lower price for the service in exchange consent to use and share her confidential information – and uses AT&T's pricing for GigaPower fiber-to-the-premises (FTTP) services as an example of such an offer.[155] This prohibition is ill-conceived, both as a matter of law and as a matter of policy, and should not be adopted.

The Commission has no authority to prohibit or limit these types of programs. If the customer is providing her consent to take the lower price in exchange for allowing the ISP greater flexibility to use and share her data, then the statutory requirements are satisfied. The statute does not authorize the FCC to determine whether the customer is actually making a good choice. As Chairman Wheeler said in an interview, in an apparent concession of the

---

[154] *NPRM* ¶ 259.

[155] *Id.* GigaPower customers may participate in an "Internet Preferences" program (also called GigaPower Premiere) by selecting a GigaPower service offering that includes Internet Preferences. As part of this program, the customer pays a reduced monthly service charge and fees in exchange for allowing AT&T to track and collect the customers' "individual Web browsing information, like the search terms . . . enter[ed] and the web pages . . . visit[ed]." *See U-Verse with AT&T GigaPower Internet Preferences, Detailed Information and Frequently Asked Questions*, AT&T, http://www.att.com/esupport/article.html#!/u-verse-high-speed-internet/KM1011211 (last visited May 27, 2016) ("GigaPower Internet Preferences FAQs").

Commission's limited authority to constrain such practices, "[a]t this point in the debate, we have to deal with what we can deal with today."[156]

Such a prohibition would also be bad policy. As the NPRM acknowledges, financial inducements for customer consent to use or share confidential information could result in significant benefits for consumers.[157]

Finally, the Commission cannot ignore the fact that this is the same bargained-for exchange that consumers operate under with any number of online providers – e.g., free service in exchange for greater use of the customer's data – and this exchange is perfectly acceptable and consistent with decades of legal precedent and policy goals related to consumer protection, privacy, and innovation.[158] There is nothing coercive or underhanded about this practice. In fact, an offering like AT&T's GigaPower program provides a more clear, straightforward choice for consumers, data than the more typical online relationship because the consumer is presented with information about it in advance and makes the decision – a choice that many online service providers offer only with respect to sensitive data. There is no basis for the Commission taking such a paternalistic view of consumers' ability to make informed choices.

Given the potential benefits of these types of inducements, the lack of statutory authority the Commission has to restrict them or to second-guess a consumers' consent choices, and the fact that such offerings are widely accepted throughout the rest of the Internet economy, it would be both illegal and poor public policy for the FCC to prohibit such arrangements.

---

[156] Julia Angwin, *5 Things You Should Know About the FCC's Proposed Privacy Rules*, ProPublica (Mar. 14, 2016), https://www.propublica.org/article/5-things-you-should-know-about-the-fccs-proposed-privacy-rules.

[157] *NPRM* ¶ 263.

[158] *See 2014 White House Big Data Report* at 40-41; *2012 FTC Privacy Report* at 52.

E. The Proposed Rules Will Make it Harder for ISPs to Deliver a Secure, Reliable Service.

The NPRM makes two proposals the likely effect of which will be to significantly hamstring ISPs as they endeavor to maintain the security, reliability, and integrity of the service they are delivering to their customers.

First, the Commission proposes to interpret Section 222(d)(2) to permit ISPs to "use or disclose CPNI whenever reasonably necessary to protect themselves or others from cyber security threats or vulnerabilities."[159] Given the constant threat of cyberattacks, this is a key application of ISPs' right to use and share customer information in order to "protect the rights or property of the carrier." But the NPRM's suggestion that this is the complete universe of information that is covered by the exception in Section 222(d)(2) is both an impermissible reading of the statute and a poor policy choice.

The terms of Section 222(d)(2) do not limit carriers' right to use customer information without prior consent to cybersecurity.[160] That provision gives ISPs the right to use or disclose customer information without customer consent as needed to protect carriers and users against *any* fraudulent, abusive, or unlawful use of, or subscription to, broadband services. Such fraudulent, abusive, or unlawful use includes the abuse and exploitation of children, including the distribution of child pornography, the distribution of spam messaging, the infringement of copyright or other proprietary rights, the perpetuation of or participation in illegal schemes or criminal activity, and the unauthorized resale of ISPs' services.

---

[159] *NPRM* ¶ 117. The FCC also proposes "to allow telecommunications carriers to use or disclose calling party phone numbers, including phone numbers being spoofed by callers, without additional customer consent when doing so will help protect customers from abusive fraudulent or unlawful robocalls." *Id.* ¶ 118.

[160] *Compare* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986), *with* 47 U.S.C. § 222(d)(2).

Protecting the rights of the ISP and the user against these threats is critical to the viability of the Internet, and it requires substantial use of customer information and periodic disclosure of customer information to trusted third parties. For example, Comcast has relationships with trusted vendors, researchers, and academics whereby Comcast shares with them under strict confidentiality agreements certain information – some of which may be considered CPNI under the Commission's proposal – to improve both the integrity and reliability of the service, and to aid in the development of new solutions or other upgrades to its network meant to better protect both the integrity of the network and the customer data flowing across it.

Second, the NPRM proposes specific cybersecurity requirements for ISPs, as well as a requirement that ISPs somehow oversee the data security operations of third parties with which ISPs have lawfully shared customer data.[161] This is a complete about-face from Administration policy[162] and Chairman Wheeler's previous public statements on the issue. Chairman Wheeler has consistently expressed support for allowing the private sector to define the specific measures needed to avoid, fend off, and remedy cyberattacks.[163] Until this NPRM, the Commission's

[161] *NPRM* ¶ 174.

[162] For example, the Department of Commerce's National Institute of Standards and Technology ("NIST") released a "voluntary how-to guide for organizations in the critical infrastructure community to enhance their cybersecurity." White House Press Release, Launch of the Cybersecurity Framework (Feb. 12, 2014), https://www.whitehouse.gov/the-press-office/2014/02/12/launch-cybersecurity-framework. "For organizations that don't know where to start, the Framework provides a road map. For organizations with more advanced cybersecurity, the Framework offers a way to better communicate with their CEOs and with suppliers about management of cyber risks." *Id.*

[163] As the Chairman has explained, "[i]f critically-positioned companies just comply ***reactively*** with a regime of prescribed mandatory requirements then our networks will always be a step behind. This is particularly true vis-à-vis aggressors. These threats move faster than a notice-and-comment rulemaking process." FCC Chairman Tom Wheeler, Remarks at the NSTAC Closed Session, at 1 (Nov. 19, 2014), https://apps.fcc.gov/edocs_public/attachmatch/DOC-330574A1.pdf (emphasis in original). He expressed a similar sentiment in his 2014 speech at AEI, stating, "proactive risk management, not reactive compliance with a cybersecurity to-do list," is "the only workable strategy for securing commercial networks" because "[t]he pace of innovation on the Internet is much, much faster than the pace of a notice-and-comment rulemaking." FCC Chairman Tom Wheeler, Remarks at the American Enterprise Institute, Washington, D.C., at 3-4 (June 12, 2014), https://apps.fcc.gov/edocs_public/attachmatch/DOC-327591A1.pdf.

approach to cybersecurity "relie[d] on industry and the market first while preserving other options if that approach is unsuccessful."[164] The Commission is changing its approach here, but without explaining why that approach was unsuccessful.

F. The Commission's Data Breach Proposals Will Harm Consumers.

In the NPRM, the Commission proposes a set of data breach regulations that significantly broaden the scope of reportable incidents, speed up the reporting of such incidents, and change the way incidents are reported to the Commission itself. These changes will harm consumers and provide little, if any, benefit.

First, the Commission proposes to define a "breach" as "any instance in which a person without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information."[165] Under the definition proposed in the NPRM, a breach would occur regardless of whether the unauthorized access or use occurs accidentally in the course of conducting legitimate business, and regardless of whether the unauthorized access or use harms a consumer. This strict liability standard departs substantially from state-level data breach notification requirements, which typically contain limiting factors such as harm triggers,

[164] FCC Chairman Tom Wheeler, Remarks at the American Enterprise Institute, Washington, D.C., at 1 (June 12, 2014), https://apps.fcc.gov/edocs_public/attachmatch/DOC-327591A1.pdf. The Commission's advisory committee on cybersecurity, CSRIC also supports the NIST framework and recommends that the Commission "promote the *voluntary* use of the NIST [framework] among all communications sector members." Cybersecurity Risk Management and Best Practices Working Group 4: Final Report, at 31 (Mar. 2015) (emphasis added), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[165] *NPRM* ¶ 75.

good faith exceptions, and exceptions for encrypted data.[166] Even the legacy CPNI definition of breach contains a requirement that the disclosure be intentional.[167]

In addition, the definition proposed in the NPRM would significantly expand the type of information subject to the breach requirements.[168] Under the proposed rule, *all* customer proprietary information is included. As explained, the definition of customer proprietary information proposed by the Commission is unlawfully broad,[169] and this approach thus goes far beyond any data breach notification law of which we are aware, all of which typically cover only sensitive personal information, such as name plus social security number, when defining security breaches that trigger a notification obligation. Under this rule, the accidental disclosure of completely innocuous information – including information like an IP address that is likely of no practical importance to a consumer, that cannot, by itself, be linked to the consumer, and that, in any event, *is already publicly available from databases that anyone can access* – would result in a breach notification.

These changes to the definition of "breach" would harm consumers. The broad definition proposed by the Commission would likely cause ISPs to issue breach notices to customers for incidents that have resulted in no harm and have no reasonable possibility of causing any harm.

---

[166] *See, e.g.*, Conn. Gen. Stat. § 36a-701b(b)(1) ("Such notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed."); Ind. Code § 24-4.9-2-2 (Breach does not include the "[u]nauthorized acquisition of a portable electronic device on which personal information is stored, if all personal information on the device is protected by encryption and the encryption key: (A) has not been compromised or disclosed; and (B) is not in the possession of or known to the person who, without authorization, acquired or has access to the portable electronic device."); N.J. Stat. Ann. § 56:8-163(a) ("Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible.").

[167] 47 C.F.R. § 64.2011(e).

[168] *See NPRM* ¶ 234.

[169] *See infra* Section V.A.2.

For example, this rule may require carriers to go through the entire breach notification process when an ISP's employee accidentally obtains access in excess of his authority to a customer's data, regardless of the data's nature or whether it is "linked or linkable to an individual," and even if the employee's unsanctioned access is for the briefest of moments only. If customers receive such meaningless breach notifications, they are more likely to disregard the notifications that are meaningful – not only from their ISP, but generally. At the same time, because there is no harm trigger, some customers may be unnecessarily frightened into believing that they are in more danger than is actually the case. This would result in the customer inefficiently expending resources to assure that no harm was actually posed.

Second, the Commission has proposed to require that ISPs notify affected customers of breaches "no later than 10 days after the discovery of the breach, subject to law enforcement needs."[170] A 10-day notification period is the lowest amount of time we have ever seen in a data breach law. The HIPAA breach notification law allows for 60 days,[171] and states that identify a specific period in their breach laws typically set it at 30 or 45 days.[172] Ten days would not give ISPs enough time to complete confirmation steps required to avoid inaccurate breach reporting to

[170] *NPRM* ¶ 234.

[171] 47 C.F.R. § 164.404(b) ("Except as provided in § 164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach").

[172] *See, e.g.,* Fla. Stat. § 501.171(4)(a) ("A covered entity shall give notice to each individual in this state whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of the breach. Notice to individuals shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than 30 days after the determination of a breach or reason to believe a breach occurred unless subject to a delay authorized under paragraph (b) or waiver under paragraph (c)."); Ohio Rev. Code § 1349.19(B)(2) ("The person shall make the disclosure described in division (B)(1) of this section in the most expedient time possible but not later than forty-five days following its discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement activities described in division (D) of this section and consistent with any measures necessary to determine the scope of the breach, including which residents' personal information was accessed and acquired, and to restore the reasonable integrity of the data system.").

customers. Instead the Commission should follow other well-established breach laws and allow at least 30 days after discovery of a breach to notify consumers.

G. The Commission's Proposal Undermines the EU-U.S. Privacy Shield Regime By Casting Serious Doubt on the Administration's Consumer Privacy Efforts.

The Commission's proposed rules have potentially far-reaching implications beyond the parties whom it purports to regulate directly – and even beyond the many entities from the advertising, diversity, and other communities that have already signaled their strong opposition to the Commission's proposal. Notably, the Commission's rejection of the Administration and FTC consumer privacy policies will become an important piece of evidence used by opponents to try and undermine the recently announced EU-U.S. Privacy Shield regime. Privacy Shield is too important to U.S. economic interests for the FCC to move forward with rules that provide opponents ammunition to help invalidate it.

Last October, the European Court of Justice sent shockwaves through the consumer privacy world when it invalidated the EU-U.S. Safe Harbor regime that had been at the heart of trans-Atlantic data flows for almost 15 years.[173] In the ensuing months, officials from both sides of the Atlantic have been working diligently to put into place a new regime to replace Safe Harbor. The result – the EU-U.S. Privacy Shield – is a carefully crafted agreement founded upon the Administration's position that the FTC's enforcement regime meets the EU's "adequacy" standard for data transfers to non-EU countries.[174] "[T]he [FTC] has a robust privacy and data security program for U.S. commercial practices that protects consumers

[173] *See* Case C-362/14, Maximillian Schrems v. Data Protection Commissioner (Oct. 6, 2015), http://curia.europa.eu/juris/liste.jsf?num=C-362/14.

[174] Press Release, Federal Trade Commission, Statement of FTC Chairwoman Edith Ramirez on EU-U.S. Privacy Shield Framework (Feb. 29, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/statement-ftc-chairwoman-edith-ramirez-eu-us-privacy-shield-0.

worldwide."[175] "The new Privacy Shield Framework, which ensures meaningful safeguards for EU citizens, will operate against this larger backdrop in which the protection of consumers' privacy and security continues to be an important priority."[176]

Critics of the EU-U.S. Privacy Shield Framework have already pointed to, among other things, perceived shortcomings in the FTC's ability to protect consumer privacy. For example, the Article 29 Working Party – a group of EU national data protection authorities that advise the European Commission on data privacy matters – commented that while it "welcomes that the FTC and the Department of Commerce are invested with investigatory powers in cases of complaints," it "would like to make sure that such an approach is sufficient to meet the CJEU's requirement of effective detection and supervision mechanisms of infringement."[177] It is widely anticipated that the EU-U.S. Privacy Shield will be subject to legal challenge, and the FTC's ability to protect consumers will be an important part of the legal analysis. As detailed above, however, the differences between the FCC's proposals and the longstanding consumer privacy framework of the Administration and the FTC are so stark that any neutral observer would consider the FCC proposals to constitute a rejection of the argument that the FTC can protect consumer privacy on the Internet.

For example, if the FTC privacy framework is truly so robust and effective, then how can the FCC now justify a proposed approach for ISP privacy regulation that *discards* that well-

[175] The EU-U.S. Privacy Shield Framework in Context: An Overview of the U.S. Privacy and Security Landscape at 1, https://www.ftc.gov/system/files/documents/public_statements/927423/attachment_a_to_ftc_privacy_shield_letter.pdf.

[176] *Id.* at 4.

[177] Opinion 01/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision, EU Article 29 Data Protection Working Party, at 30 (Apr. 13, 2016), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

established FTC framework and seek to impose an alternative that in many ways is the polar opposite? This rejection of the FTC's approach would be heavily featured in any lawsuits trying to invalidate Privacy Shield.

The Commission can protect consumers without providing ammunition to opponents of Privacy Shield. The Consensus Privacy Framework outlined above is consistent with the FTC and Administration approach to privacy, and reaffirms the Administration's position that the FTC can play the important role designated for it under the Privacy Shield regime.

V. THE PROPOSED RULES ARE UNLAWFUL.

The Commission's proposals are unlawful in at least three respects. First, the Communications Act does not support the Commission's proposals. Second, the proposals violate ISPs' First Amendment commercial speech rights. And third, adopting these proposed rules would be a textbook example of arbitrary and capricious rulemaking.

A. The Commission Does Not Have the Statutory Authority to Adopt Its Proposed Privacy Regime.

In adopting Section 222, Congress gave the Commission authority to adopt reasonable privacy protections for consumers and competitors using telephone services. But the Commission has proposed a regime that goes far beyond the authority that Congress has granted it in the Act.

1. None of the statutory provisions cited in the NPRM give the Commission authority to adopt the proposed regime.

The Commission does not have the authority to regulate ISPs' use of, access to, or disclosure of information that they obtain from their customers under the Communications Act. Section 222 does not grant that authority. Congress never intended that Section 222 would apply to ISPs' customer information, and certainly never intended it to be used in the far-reaching manner the Commission proposes. Rather, Section 222 was intended to govern a narrow set of

customer information to which *telephone companies* have access known as CPNI.[178] As the Commission itself has recognized, Section 222's origins were in a bill sponsored by then-Rep. Markey, entitled the "Telephone Consumer Privacy Protection Act of 1993."[179]

The plain language of Section 222 clearly evinces Congress's intent to focus on telephony. Section 222 is littered with telephone-specific references. For example, there are references to different types of telephone service, such as "telephone toll service" and "telephone exchange service,"[180] and telephone providers, such as requirements specific to local exchange carriers.[181] Multiple provisions relate directly to ensuring information is available for the publication of telephone directories.[182] There is no equivalent in the Internet ecosystem to a phonebook listing the name, address, and contact information, such as an email address or IP address, for broadband customers.

Moreover, the 1996 Telecommunications Act included specific provisions regarding broadband Internet services that underscored Congress's clear intent to have the FCC regulate the Internet *less*, not more. Notably Section 230 directed the Commission "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation."[183] Merely because the FCC has reclassified ISPs as telecommunications carriers does not magically expand Section 222's scope

---

[178] H.R. Rep. No. 104-458, at 205 (1996) (stating that Congress enacted Section 222 "to balance both competitive and consumer privacy interests with respect to *CPNI*") (emphasis added).

[179] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, n.3 (1998) ("*1998 CPNI Order*").

[180] *See* 47 U.S.C. §§ 222(e), 222(g), 222(h)(1).

[181] *See id.* § 222(c)(3).

[182] *See id.* §§ 222(c)(1), 222(e), 222(h)(3).

[183] *Id.* § 230(b)(2).

and intent from its clear and targeted focus on telephone companies and their CPNI to ISPs. The law is clear that an agency cannot "use its definitional authority to expand its own jurisdiction."[184] Nor does it give the FCC license to ignore the marketplace facts that have characterized this industry for decades, notably:

- A highly successful FTC privacy framework that has consistently made clear there is no basis for treating ISPs differently and rather that a technology-neutral privacy regime is required,
- No evidence of consumer privacy harm from ISPs,
- FCC precedent recognizing the enhanced incentives ISPs have to protect consumers' privacy and honor their privacy commitments, and
- A booming Internet ecosystem.[185]

Regardless, Section 222 represents the *maximum* privacy authority the Commission has under the Act; it cannot look to other more general provisions to go *further* than what Congress authorized in this specific provision it adopted to address privacy. Under the generally accepted canons of statutory interpretation, an agency may not adopt rules pursuant to a general provision that alter the balance established by Congress in a more specific provision of the statute.[186] This

[184] *Am. Bankers Ass'n v. SEC*, 804 F.2d 739, 754-55 (D.C. Cir. 1986).

[185] *See supra S*ection I.

[186] *See D. Ginsberg & Sons v. Popkin*, 285 U.S. 204, 208 (1932) (holding that general language of a statute will not be held to apply to a matter specifically dealt with in another part of the same statute); *AT&T Co. v. FCC*, 487 F.2d 865, 872, 876 (2d Cir. 1973) (holding that a Commission order refusing AT&T permission to file tariff revisions was invalid because the requirement violated the statutory scheme governing ratemaking, which when Congress enacted it, "struck a 'careful balance of interests'" and "to permit the imposition of a special permission requirement on the basis of the Commission's claimed broad inherent power to regulate the communications and broadcasting industries would frustrate the specific Congressional purpose sought to be achieved by the Act's precise statutory scheme") (quoting *United States v. Students Challenging Regulatory Agency Procedures*, 412 U.S. 669, 697 (1973)); s*ee also RadLAX Gateway Hotel, LLC v. Amalgamated Bank*, 132 S. Ct. 2065, 2071 (2012) (While this canon "is perhaps most frequently applied to statutes in which a general permission or prohibition is contradicted by a specific prohibition or permission," it "has full application as well to statutes . . . in which a general authorization and a more limited, specific authorization exist side-by-side."). In such cases, an agency may not rely on a general grant of authority to "circumvent or ignore" the balance struck by Congress by imposing requirements on the regulated firm that are not authorized under the "specific scheme" established by statute. *AT&T.*, 487 F.2d at 880.

principle precludes the Commission from relying on any of the general provisions of the Act, such as Sections 201(b), 705, or 706, as the basis for adopting privacy rules are inconsistent with the framework set forth in Section 222. Doing so would upset the balance established by Congress between protecting consumer privacy and providing telecommunications carriers with the flexibility to engage in marketing and advertising.

Indeed, the Commission itself has applied this canon in the specific context of Section 222, holding that the specific consumer privacy and consumer choice protections established in section 222 supersede the general protections identified in sections 201(b) and 202(a) and other statutory provisions:

> In enacting section 222, Congress carved out very specific restrictions governing consumer privacy in CPNI and consolidated those restrictions in a single, comprehensive provision. We believe that the specific requirements governing CPNI use are contained in that section and we disfavor, accordingly, an interpretation of section 272 that would create constraints for CPNI beyond those embodied in the specific provision delineating those constraints.[187]

The FCC concluded "*that the specific consumer privacy and consumer choice protections established in section 222 supersede the general protections identified in sections 201(b) and 202(a).*"[188]

Further, the terms of the cited provisions and the Commission's own precedent give the Commission little – if any – authority to adopt the rules it has proposed.

The Commission has explained that the general conduct standard it adopted in the 2015 Open Internet Order governs the application of Section 201(b) to broadband Internet access

---

[187] *Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd. 14409, ¶ 142 (1999) ("*1999 CPNI Recon. Order*") (emphasis added). The D.C. Circuit has likewise held that Section 706 must be interpreted in accord with this basic canon of statutory interpretation. *Verizon v. FCC*, 740, F.3d 623, 649-50 (D.C. Cir. 2014) (citing *Ginsberg*, 285 U.S. at 208).

[188] *1999 CPNI Recon. Order* ¶ 153.

service.[189] Even a cursory analysis of these proposed rules in the context of the general conduct standard shows that they do not meet the threshold for Commission action under this section. None of the behaviors that would be regulated under the Commission's proposal can reasonably be said to "unreasonably interfere with . . . end users' ability to select, access, and use broadband Internet access service or the lawful Internet content, applications, services, or devices of their choice."[190]

The Commission's authority to adopt privacy rules under Section 705 is extremely narrow. At most, Section 705(a) gives the Commission authority to adopt rules designed to prevent ISPs from "divulg[ing] or publish[ing]" certain consumer information. The Commission cannot rely on Section 705(a) to regulate the use of customer communications. For example, delivering an ad to a customer based on information learned from a customer's web traffic does not qualify as publishing or divulging the contents or even existence of the communication because the ad is served directly to the customer whose interest it is based on.

Finally, the Commission cannot rely on Section 706 to regulate privacy. That provision states that the Commission shall, in certain circumstances, adopt regulations to "encourage the deployment on a reasonable and timely basis of advanced telecommunications capability."[191] But the Commission offers no basis in the NPRM for concluding that onerous privacy rules applicable only to ISPs would promote the deployment of advanced services. If anything, as

---

[189] *2015 Open Internet Order* ¶ 137 ("We note that the [no unreasonable interference/disadvantage] standard we adopt today represents our interpretation of sections 201 and 202 in the broadband Internet access context").

[190] *See* 47 C.F.R. § 8.11. Most studies show that there is very little correlation between privacy concerns and Internet usage. For example, a 2014 study by Ericsson of individuals in six countries found that while 56% of respondents are concerned with privacy issues, only 4% said that they have reduced their Internet usage due to security concerns. Ericsson ConsumerLab, *Privacy, Security and Safety Online: Consumer Perspectives and Behavior*, at 4 (Feb. 2014), http://www.ericsson.com/cy/res/docs/2014/privacy-security-safety-online.pdf.

[191] *See* 47 U.S.C. § 1302(a).

shown above, it is more likely that they would have the effect of *slowing* the deployment of advanced services by diminishing the extent to which ISPs can efficiently advertise bundles, thereby depressing the ISP's incentive and ability to invest in additional broadband deployment, upgrades, and innovations.[192]

In the end, the Commission is left with no authority to regulate ISP privacy, but even assuming it has any such authority, it is limited to the provisions in Section 222 and the very narrow and targeted focus of this statute in terms of the limited data and activities covered, as discussed in the following sections.

2. Even assuming Commission authority here, the Commission may only regulate information that qualifies as CPNI under Section 222.

Even if Section 222 can be read to apply to information ISPs obtain from their customers, the Commission only has authority under that provision to regulate ISPs' customer information that meets the statutory definition of CPNI. In particular, the Commission may not rely on Section 222(a) to regulate information that does not qualify as CPNI. The term "proprietary information" was used in Section 222(a) simply because the provision covers information

---

[192] *See supra* Section IV.B. Despite claims that NTIA's new study demonstrates that privacy concerns will limit broadband adoption, see Andrea Peterson, Why a staggering number of Americans have stopped using the Internet the way they used to, Washington Post, May 13, 2016, consumers do not often cite privacy and security concerns as key factors for why they don't use the Internet. For example, Scott Wallsten reports that in response to questions about whether privacy concerns keep consumers offline, the Current Population Survey Computer and Internet Supplement results for 2011, 2013, and 2015 show that "[i]n each year, less than one percent of those who do not use the Internet cited privacy as the main reason they stay offline." Scott J. Wallsten, *No, The NTIA's Survey Data Do Not Show a "Tipping Point" in Behavior Due to Privacy Concerns*, Technology Policy Institute Blog (May 15, 2016), https://techpolicyinstitute.org/2016/05/15/no-the-ntias-survey-data-do-not-show-a-tipping-point-in-behavior-due-to-privacy-concerns/. A 2014 study by NTIA similarly found that only one percent of survey respondents said that privacy or security concerns were responsible for their decision not to adopt Internet services. NTIA, *Exploring the Digital Nation: Embracing the Mobile Internet*, at 26 (Oct. 2014), *available at* http://www.ntia.doc.gov/files/ntia/publications/exploring_the_digital_nation_embracing_the_mobile_internet_10162014.pdf. NTIA's Digital Nation Data Explorer, which provides statistics related to computer and Internet use based on the CPS Computer and Internet Supplement, shows that the top two reasons why a household does not have Internet at home are (1) that the respondent does not need or is not interested in getting an Internet connection (55.2% of respondents) and (2) that the respondent considers an Internet connection to be too expensive (23.5% of respondents). NTIA, Digital Nation Data Explorer (Mar. 21, 2016), https://www.ntia.doc.gov/other-publication/2016/digital-nation-data-explorer.

exchanged with three different types of entities – customers, telecommunications carriers, and equipment manufacturers – and so using the term "CPNI," a term that applies solely to *customers* as addressed in Section 222(c), would not have been appropriate. But Congress's use of the term "proprietary information" in Section 222(a) cannot reasonably be viewed, as the NPRM suggests, as a basis for creating a new and extremely expansive category of "customer proprietary information" to which all obligations under Section 222(c) and other provisions apply.

The Commission ignores this plain meaning and clear congressional intent and instead reads the term "proprietary information" in Section 222(a) as an incredibly broad source of authority for it to regulate a breathtaking amount of customer proprietary information in the most restrictive ways imaginable – certainly far beyond what the FTC privacy framework allows.

The Commission's attempt to rely on Section 222(a) as an independent grant of authority is inconsistent with the language and statutory structure of Section 222, as well as with Commission precedent. First, the above analysis and conclusion regarding the intent behind using "proprietary information" in Section 222(a) is reinforced by the fact that Section 222(b), which focuses solely on the exchange of information between telecommunications carriers uses the term "proprietary information,"[193] whereas Section 222(c), which focuses on the use and disclosure of *customer data* by a telecommunications carrier uses the term "customer proprietary network information."

Second, Section 222(e) requires that carriers "provide subscriber list information . . . on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and

[193] 47 U.S.C. § 222(b) ("Confidentiality of carrier information. A telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts.").

conditions, to any person upon request for the purpose of publishing directories in any format," "[n]otwithstanding subsections (b), (c), and (d) of [Section 222]."[194] If Congress had intended Section 222(a) to confer an independent grant of authority, then it would have listed subsection (a), along with subsections (b)-(d) as sections whose requirements are superseded by the requirements of Section 222(e) to prevent the requirements of Section 222(a) from conflicting with the Section 222(e).

Third, Section 222(d) defines the circumstances under which a carrier may use, disclose, or provide access to CPNI without seeking customer approval.[195] This includes such non-controversial uses as billing the customer for the service, and providing information to emergency service providers.[196] Interpreting Section 222(a) as conferring protection on categories of information *beyond* CPNI would produce the nonsensical result of restricting ISPs from using these additional categories of information, such as a customer's name and address, for the purposes specified in Section 222(d). For example, ISPs potentially would not be able to send a subscriber's unpaid bill into receivership without specifically seeking and receiving the customer's approval. And ISPs would be prevented from sharing potentially life-saving information about a customer under these serious circumstances without first obtaining the customer's approval. This interpretation of Section 222(a) is irrational and, under established canons of statutory interpretation, cannot stand.

---

[194] *Id.* § 222(e). Section 222(h)(3) defines "subscriber list information" as "information identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications." *Id.* § 222(h)(3). Customer names, addresses, and telephone numbers are among the categories of information the Commission has proposed to protect under its interpretation of Section 222(a). *See NPRM* ¶¶ 56, 62.

[195] 47 U.S.C. § 222(d) ("Nothing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to *customer proprietary network information* obtained from its customers, either directly or indirectly through its agents to . . . .") (emphasis added).

[196] *Id.* § 222(d)(1), (d)(4)(A).

The Commission's proposed interpretation also is inconsistent with the legislative history of Section 222. In conference, Congress eliminated provisions from the House bill's proposed version of Section 222 that would have given the Commission broader authority to regulate customer information. Specifically, the House bill defined CPNI to include a catch-all provision that would have expanded the definition significantly.[197] The Conference Report adopted the House's proposed CPNI definition, but eliminated the catch-all provision from the CPNI definition ultimately codified in Section 222.[198] Had Congress intended Section 222 to apply to a broader set of information, it would have chosen either the catch-all provision from the House bill or otherwise broadened the definition. It did neither.

Finally, the NPRM's proposed expansive interpretation of Section 222(a) is at odds with well-established Commission precedent. Until recently, the Commission had consistently interpreted the statute to mean that CPNI was coextensive with the scope of customer information to be protected:

> Congress laid out a framework for carriers' use of customer information based on the sensitivity of the information. In particular, the statute allows easier dissemination of information beyond the existing customer-carrier relationship where information is not sensitive, or where the customer so directs. Thus, section 222 establishes three categories of customer information to which different privacy protections and carrier obligations apply: (1) individually identifiable CPNI, (2) aggregate customer information, and (3) subscriber list information.[199/]

Nowhere in the above summary of the scope of Section 222 or in the many orders addressing the voice CPNI rules did the Commission ever interpret Section 222(a) as it does in the NPRM as a

---

[197] *See* H.R. Rep. No. 104-204, at 22-23 (1995); H.R. Rep. No. 104-458, at 97-98 (1995).

[198] *See* H.R. Rep. No. 104-458, at 97-98.

[199] *2002 CPNI Order* ¶ 6 (2002); *see also 1998 CPNI Order*, at ¶ 2 ("Section 222 sets forth three categories of customer information to which different privacy protections and carrier obligations apply -- individually identifiable CPNI, aggregate customer information, and subscriber list information. CPNI includes information that is extremely personal to customers. . .").

font of unfettered authority to go well beyond regulation of CPNI. Why did the Commission limit its voice rules solely to CPNI if there was this additional source of authority in Section 222(a) to dramatically expand the scope of data covered? The Commission's expansive interpretation of Section 222(a) as covering an entirely new set of data well beyond CPNI is even more implausible in light of the fact that it took the Commission 20 years to discover such authority. The Supreme Court has cautioned that an agency's attempt to glean sweeping authority from a statute *decades after its enactment* generally indicates that the statute does not, and never did, contain the newfound delegation of authority.[200]

3. The scope of CPNI is narrowly defined by the statute and does not encompass IP addresses.

a. CPNI does not include any data acquired by the ISP *other than* from the customer.

CPNI is defined in section 222(h)(1) of the statute as follows:

> **Customer proprietary network information.** The term "customer proprietary network information" means— **(A)** information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and **(B)** information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.

For purpose of the present analysis, subpart (B) is not relevant as it applies solely to telephone exchange service or telephone toll service (although we nonetheless show below how it clearly does not apply here). Subpart (A) applies to a narrow list of specified data elements "that [are] made available to the carrier by the customer solely by virtue of the carrier-customer

[200] *Util. Air Regulatory Grp. v. EPA*, 134 S. Ct. 2427, 2444 (2014) ("When an agency claims to discover in a long-extant statute an unheralded power to regulate a significant portion of the American economy," courts will "greet [such] announcement[s] with a measure of skepticism" because courts expect "Congress to speak clearly if it wishes to assign to an agency decisions of vast economic and political significance.") (quotation marks and citation omitted).

relationship." Thus, it does not include any data that the carrier may obtain *outside* of this relationship, such as from a third party.

Section 222(c) reinforces this conclusion.[201] And the FCC has interpreted this provision to exclude from the statute's scope any information obtained by the carrier *outside* its provision of telecommunications service:

> Section 222(c)(1) prohibits the use of CPNI only where it is derived from the provision of a telecommunications service. Consequently, ***we find that information that is not received by a carrier in connection with its provision of telecommunications service can be used by the carrier without customer approval***, regardless of whether such information is contained in a bill generated by the carrier. Therefore, consistent with the *Clarification Order*, customer information derived from information services that are held not to be telecommunications services may be used, even if the telephone bill covers charges for such information services.[202]

The NPRM asks whether "a broadband provider [should] obtain some form of consumer consent before combining data acquired from third-parties with information it obtained by virtue of providing the broadband service?"[203] Based on the above clear statutory language and Commission precedent, the answer is no. The statute does not cover such third-party information or any other information obtained by the carrier other than from the customer "solely by virtue of

---

[201] The restrictions on use, disclosures, and access are limited solely to "a telecommunications carrier that receives or obtains customer proprietary network information *by virtue of its provision* of a telecommunications service." 47 U.S.C. § 222(c) (emphasis added).

[202] *1999 CPNI Recon. Order* ¶ 159 (emphasis added); *see also Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Declaratory Ruling, 28 FCC Rcd. 9609, ¶ 28 (2013) ("In addition, modern mobile operating systems enable consumers to install applications developed by third parties that can collect sensitive personal information. Such third-party applications may raise privacy concerns. They are, however, generally beyond the scope of section 222 and our rules. For example, third-party applications might collect the same or different kinds of data, some of which might be CPNI if collected at the carrier's direction; where such information is not collected by or at the direction of a carrier or its agent, it is not 'made available to the carrier . . . by virtue of the carrier-customer relationship.' Furthermore, information stored on a mobile device that is not under the carrier's control and not intended to be transmitted to the carrier or otherwise not accessible by the carrier, as may be the case with a contact list or call log, is not CPNI because it is not 'made available to the carrier,' even if it would otherwise satisfy the definition of CPNI if made available to the carrier.").

[203] *NPRM* ¶ 138.

the carrier-customer relationship" or outside the ISP's "provision of a telecommunications service."

b. The IP address an ISP assigns to its customer is not CPNI.

The IP address assigned by the ISP to the customer's modem does not qualify as CPNI under subpart (A) of the statutory definition.[204] As an initial matter, a customer's IP address is not "made available to the carrier by the customer," as required by subpart (A) of the CPNI definition. In fact, the opposite is true: the ISP *assigns the IP address to the customer premise device*. As such, the IP address assigned to the customer's modem fails to meet this elementary requirement in subpart (A) of the CPNI definition.

Even if it could overcome this threshold point, the IP address assigned to the customer by the ISP does not meet the other requirements of subpart (A). Specifically:

- *Quantity*. The IP address provides no indication as to the "quantity" of Internet service purchased by a customer. A customer can use the same IP address regardless of the volume of data the customer downloads or the capacity of the service to which the customer subscribes.

- *Amount.* Likewise, the IP address does not relate to the "amount" of telecommunications purchased by a customer. As explained with regard to "quantity," a customer's IP address bears no relationship with the customer's volume of Internet usage.

- *Technical Configuration.* The IP address which is assigned to the customer does not relate to the "technical configuration" of the services purchased by a customer. All technical configurations of Internet access service provisioned by ISPs utilize IP addresses in essentially the same way. And any changes to the configuration of the consumer's home network (e.g., replacing a WiFi router) are largely irrelevant to the IP address assigned to the customer by the ISP.

[204] As originally adopted in 1996, the definition of CPNI did not include "location." *See* Telecommunications Act of 1996, Pub. L. No. 104-104, § 222, 110 Stat. 56 (1996). That language was added in 1999 along with two other Section 222 provisions related to the physical location of mobile wireless service and IP-enabled voice service users. *See* Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, § 5, 113 Stat. 1286 (1999). The legislative history indicates that the purpose of the amendment was "to address the need for use of, disclosure of, and access to certain information in the provision of emergency services." S. Rep. No. 106-138, at 7-8 (1999).

- *Type.* IP addresses do not relate to the "type" of service purchased by a customer. The IP address that has been assigned to a particular customer conveys nothing about the type of Internet service to which the customer has subscriber, whether it be a standard best-efforts Internet service or a dedicated wireline Ethernet Internet access service.

- *Destination.* The IP address which is assigned to a customer does not relate to the "destination" of communications purchased by a customer. The IP address assigned to the customer merely identifies the device from which the customer *originates* Internet traffic and at which the customer *receives* Internet traffic. It does not convey any information whatsoever about the "destination" of the customer's communications.

- *Location.* The IP address assigned to the customer does not relate to the "location" of the service purchased by the customer. The legislative history of Section 222 indicates that Congress intended the term location to mean the geographic location of a customer.[205] While IP addresses identify the "logical" location of a device for purposes of routing Internet traffic, they do not generally identify the specific geographic location of the device.[206] Thus, the IP address are not related to a customer's location.

Customer IP addresses also do not qualify as CPNI under subpart (B) of the definition.

To qualify as CPNI under subpart (B), the information must be contained in bills pertaining to

[205] *Supra* note 208.

[206] In fact, it is quite difficult to associate an IP address with a particular name and geographic address without more information. *See, e.g.*, *Can You Be Tracked Down Just by Your IP Address*, WhatIsMyIPAddress.com, http://whatismyipaddress.com/find-me (last visited. Apr. 29 2016) ("[T]he most information that the average curious person can find out about you with only your IP address (and nothing else) is what region, city and town you are in when you're on the Internet. They won't know anything about you (such as your name, etc.) or the computer you're using. And actually, what they'll find out isn't really about YOU, more than it is about your online connection."); *Can Someone Find Me with My IP Address*, WhatISMyIP.com, https://www.whatismyip.com/can-someone-find-me-with-my-ip-address/ (last visited Apr. 29, 2016) ("While [an IP] address is used to route internet traffic to your computer it does not reveal your location. If someone was able to get your IP address they could learn a bit about your internet service, such as which provider you use to connect to the internet, but they really can't locate you, your home, or your office.").

telephone exchange service[207] or telephone toll service,[208] but broadband Internet access service does not fit the definition of either of these services and, in all events, it is highly unlikely that customer IP addresses would appear in customer bills. For example, the language in the definition of "telephone exchange service" indicates that the term is intended to encompass only voice telephony services.[209]

Broadband Internet service also does not qualify as telephone toll service because it is not a "telephone service" and does not include a separate charge for the transmission of traffic between stations in different exchange areas.[210] And even if the Commission were to somehow decide that broadband Internet service meets the definition of either telephone exchange service or telephone toll service, the IP address would only qualify as CPNI if it is included in customer bills.

---

[207] The definition of "telephone exchange service" in the Act is as follows:

> (A) service within a telephone exchange, or within a connected system of telephone exchanges within the same exchange area operated to furnish to subscribers intercommunicating services of the character ordinarily furnished by a single exchange, and which is covered by the exchange service charge, or (B) comparable service provided through a system of switches, transmission equipment, or other facilities (or combination thereof) by which a subscriber can originate and terminate a telecommunications service.

47 U.S.C. § 153(54).

[208] That term is defined in the Act as follows: "telephone service between stations in different exchange areas for which there is made a separate charge not included in contracts with subscribers for exchange service." *Id.* § 153(55).

[209] 47 U.S.C. § 153(54). Specifically, under subpart (A) of the definition, a service must be provided "within a telephone exchange, or within a connected system of telephone exchanges." *Id.* Moreover, to qualify under subpart (A), a service must also be subject to the "exchange service charge." *Id.* These are terms used in the context voice telephony services, and charge that customers pay for the ability to make *local telephone calls*. Broadband Internet service also does not qualify as telephone exchange service under subpart (B) of the definition because it is not remotely "comparable" to local voice service described in subpart (A): broadband Internet service is not a voice service, it does not utilize telephone numbers, and neither telephone service boundaries nor any other service boundaries are relevant to the manner in which it is provisioned.

[210] *Id.* § 153(55).

The Commission's prior application of the definition of CPNI to telephone numbers further supports the conclusion that the IP addresses assigned to customer modems are not CPNI. As the NPRM concedes, telephone numbers are closely analogous to IP addresses.[211] *But the Commission has consistently held that none of the categories of information enumerated in the definition of CPNI encompasses the customer's telephone numbers*.[212] Thus, the Commission's own analogy confirms that a subscriber's IP address may *not* be defined as CPNI under Section 222.[213]

In fact, after Congress added "location" to the definition of CPNI, the Commission expressly reaffirmed the outcome of its pre-amendment CPNI orders, including the exclusion of telephone numbers from the definition of CPNI.[214] The Commission's reasoning then is just as applicable to IP addresses today: both IP addresses and telephone numbers identify the "logical" routing point for a customer's traffic, but not the geographical location of the end user.[215] The

---

[211] *NPRM* ¶ 45. The Commission also equated IP addresses and domain names to telephone numbers in the *2015 Open Internet Order* and recognizes that IP addresses identify a "logical" location rather than a physical one. *Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd. 5601, ¶ 361 (2015) ("Although Internet users often do not know the geographic location of edge providers or other users, there is no question that users specify the end points of their Internet communications. Consumers would be quite upset if their Internet communications did not make it to their intended recipients or the website addresses they entered into their browser would take them to unexpected web pages. Likewise, numerous forms of telephone service qualify as telecommunications even though the consumer typically does not know the geographic location of the called party. These include, for example, cell phone service, toll free 800 service, and call bridging service. In all of these cases, the user specifies the desired endpoint of the communication by entering the telephone number or, in the case of broadband Internet access service, the name or address of the desired website or application.").

[212] *1999 CPNI Recon. Order* ¶¶ 146-47. The Commission engages in sleight-of-hand when it says that "the Commission has previously held telephone numbers dialed to be CPNI" and then proposes to treat both source and destination IP addresses as CPNI. While it may be true that telephone numbers *dialed* are considered CPNI, the *customer's* telephone number is *not* CPNI. *1998 CPNI Clarification Order* ¶ 8. As such, the Commission's analogy only supports, at most, the notion that destination – not source – IP addresses may be considered CPNI.

[213] Nor should destination IP addresses of a broadband customer, by themselves, be considered CPNI, *see NPRM* ¶ 41, absent their association with individually identifiable information about that subscriber.

[214] *1998 CPNI Clarification Order* ¶ 9 n.18; *1999 CPNI Recon. Order* ¶¶ 146-47 (adopting the Common Carrier Bureau's holdings in the *1998 CPNI Clarification Order*).

[215] *See 1998 CPNI Clarification Order* ¶ 9 n.18.

Commission's determination that customer telephone numbers do not qualify as relating to the "location" of the customer's telephone service supports the conclusion that a customer's IP address does not qualify as CPNI.

Finally, in addition to being beyond the statute, it makes no sense as a matter of policy to classify IP addresses as CPNI. ISPs have little to no systematic advantage over any other entity in the Internet ecosystem by virtue of having access to a customer's IP address. As demonstrated above, any website or app that a consumer visits must know the IP address over which the consumer is accessing the website in order to connect to the customer's device.[216] And any time a customer sends an email, it is sending his/her IP address to the recipient. Given the ease with which entities can obtain IP addresses of their customers and the many ways in which such entities use IP addresses, imposing the limits of Section 222 on ISPs' access, use, and disclosure of IP addresses would not materially alter the extent to which customer IP addresses are protected.[217]

4. The Commission may only regulate ISPs' customer information that does not qualify as CPNI in order to "protect" the confidentiality of that information.

Even if Section 222(a) confers an independent grant of authority, it is only the authority to adopt rules that "protect the confidentiality of" proprietary information. This means that any authority the Commission may have under this provision is limited to preventing proprietary information from being exposed without authorization and does not extend to defining its permissible uses such as for marketing or advertising.

---

[216] *See supra* Section III.

[217] For similar reasons to those discussed above, Media Access Control (MAC) addresses and other device identifiers also cannot be deemed to be CPNI.

Other agencies implementing privacy statutes with structures similar to Section 222 have limited the rules promulgated pursuant to the "protection" portion of the statute to ensuring the integrity, security, and confidentiality of customer information. For example, Section 501(a) of the Gramm-Leach-Bliley Act ("GLBA") establishes a policy that financial institutions have "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information,"[218] and Section 501(b) requires agencies to establish standards that implement this policy.[219] Section 502 of GLBA specifies the circumstances under which a financial institution may disclose nonpublic personal information to nonaffiliated third parties.[220] The FTC's rules implementing Section 501(b) are purely related to safeguarding customer information, consistent with the plain language of the statute.[221] If the FCC persists in its belief that Section 222(a) grants it authority to adopt any rules – which it does not – that authority is circumscribed and the Commission should follow the examples established by other agencies implementing similar language in their statutes.

5. The proposed extension of the rules to affiliates is contrary to the statute.

The Commission may not extend its proposed framework to cover the use of customer information by non-telecommunications carrier affiliates. In the NPRM, the Commission expresses concern that its proposals may "inadvertently encourage corporate restructuring and gamesmanship" to avoid stricter customer data use and disclosure requirements and seeks to

[218] 15 U.S.C. § 6801(a).

[219] *Id.* § 6801(b).

[220] *Id.* § 6802.

[221] *See* 16 C.F.R. pt. 314.

avoid such activity by "treating use by an affiliate as subject to the same limits as use by a BIAS provider."[222] This would be patently unlawful.

The Commission itself has repeatedly asserted – and as Chairman Wheeler reiterated during the May 11, 2016 Senate Judiciary Committee hearing – that it lacks the authority to regulate "edge services."[223] If that is the case, it cannot reach the affiliates of telecommunications carriers that only provide "edge services."

Moreover, the plain language of Section 222 is clear that it only applies to telecommunications carriers. If Congress had intended for Section 222(c) to apply to affiliates, it would have done so explicitly – as it did, for example, in Sections 260 and 275.[224] It cannot and should not stretch its jurisdiction, even on an ancillary basis, to impose privacy requirements under Section 222 or any other statutory provision on entities that would not otherwise be regulated by the Act.[225]

---

[222] *NPRM* ¶ 124.

[223] *See* 47 U.S.C. § 152(a); *2015 Open Internet Order* ¶¶ 190-92 (limiting the scope of entities to which the Open Internet rules apply); *see also Examining the Proposed FCC Privacy Rules: Hearing Before the Subcomm. on Privacy, Technology and the Law of the Senate Comm. on the Judiciary*, 115th Cong. (May 11, 2016) (statement of Tom Wheeler, Chairman, FCC), http://www.c-span.org/video/?409389-1/fcc-commissioners-testify-proposed-internet-privacy-rules (starting at 00:41:21) ("I said we will not be regulating edge providers. . . .We do not intend to regulate the edge.").

[224] 47 U.S.C. § 260(b) ("If the complaint contains an appropriate showing that the alleged violation occurred, the Commission shall, within 60 days after receipt of the complaint, order the local exchange carrier and any affiliates to cease engaging in such violation pending such final determination."); *id.* § 275(a) ("No Bell operating company or affiliate thereof shall engage in the provision of alarm monitoring services before the date which is 5 years after February 8, 1996.").

[225] *FCC v. Midwest Video Corp.*, 440 U.S. 689, 708-09 (1979) (prohibiting the Commission from adopting rules under its ancillary authority that it was prohibited from adopting under its express authority); *United States v. Midwest Video Corp.*, 406 U.S. 649, 676 (1972) (Burger, C.J., concurring) (admonishing that the Commission's interpretation of the limits of its jurisdiction permitting it to adopt a program-origination rule "strains the outer limits of even the open-ended and pervasive jurisdiction" the Commission possesses).

6. The proposed treatment of de-identified and aggregated data is contrary to the statute and good public policy.

In the NPRM, the Commission proposes to exempt de-identified information from the customer approval requirements described in its proposal only if, among other requirements, the information is "aggregated" and information that is reasonably linkable to a specific "device" is removed.[226] These two proposed requirements are inconsistent with the terms of Section 222 and with sound public policy. The Commission should not therefore adopt either requirement.

Section 222 excludes two independent categories of information from its restrictions. First, Section 222(c)(3) states that the carriers need not obtain customer approval to use, disclose, or permit access to "aggregate customer information."[227] Section 222(h)(2) defines aggregate customer information ("ACI") as "collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed."[228] The phrase "individual customer identities and characteristics" refers to information that could be used to identify a particular person and that particular individual's characteristics. However, aggregate information about customers' characteristics, such as the percentage of a group of customers that is male or female, may be included in ACI as long as the characteristics are not reasonably linkable to a particular individual.

Contrary to the Commission's proposal, ACI may include information that is reasonably linkable to a "device." The statutory definition does not include any suggestion that ACI must

---

[226] *See NPRM* ¶ 154 (proposing that information qualify as de-identified if "the provider (1) determines that the aggregated customer PI is not reasonably linkable to a specific individual or device; (2) publicly commits to maintain and use the aggregate data in a non-individually identifiable fashion and to not attempt to re-identify the data; (3) contractually prohibits any entity to which it discloses or permits access to the aggregate data from attempting to re-identify the data; and (4) exercises reasonable monitoring to ensure that those contracts are not violated").

[227] *See* 47 U.S.C. § 222(c)(3).

[228] *See id.* § 222(h)(2).

not be reasonably linkable to a device. Importantly, Congress has included the term "device" in numerous provisions of the Communications Act that were adopted in the 1996 amendments, along with Section 222.[229] The Commission must infer that Congress intentionally excluded a reference to devices from the statutory definition of ACI.[230]

In addition, information that is associated with or identifies a device, such as an IP address or a MAC address, is not reasonably linkable to an individual. As Google has explained, device identifiers such as IP addresses are simply strings of numbers that cannot be used to identify an individual unless they are linked to other information, such as a customer's name or address, that can be used for this purpose.[231] Thus, aggregated data sets that include IP addresses or MAC addresses but that do not include information such as names or addresses that identify a particular individual must qualify as ACI.

Second, the requirement that carriers obtain customer approval to use, disclose, or permit access to CPNI in Section 222(c)(1) applies only to "individually identifiable" CPNI.[232] The

---

[229] *See, e.g., id.* § 255(d) ("Whenever the requirements of subsections (b) and (c) of this section are not readily achievable, such a manufacturer or provider shall ensure that the equipment or service is compatible with existing peripheral *devices* or specialized customer premises equipment commonly used by individuals with disabilities to achieve access, if readily achievable.") (emphasis added); *id.* § 256(a)(1)(B) ("It is the purpose of this section to promote nondiscriminatory accessibility by the broadest number of users and vendors of communications products and services to public telecommunications networks used to provide telecommunications service through . . . public telecommunications network interconnectivity, and interconnectivity of *devices* with such networks used to provide telecommunications service. . . .") (emphasis added); *id.* § 275(e) ("The term 'alarm monitoring service' means a service that uses a *device* located at a residence, place of business, or other fixed premises to receive signals from other devices located at or about such premises . . . .") (emphasis added).

[230] *Keene Corp. v. United States*, 508 U.S. 200, 208 (1993) ("[W]e have only to say that § 1500 speaks of 'jurisdiction,' without more, whereas some nearby sections of title 28 use the longer phrase. This fact only underscores our duty to refrain from reading a phrase into the statute when Congress has left it out. '[W]here Congress includes particular language in one section of a statute but omits it in another . . . , it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion.'" (quoting *Russello v. United States*, 464 U.S. 16, 23 (1983))).

[231] *See* Google Public Policy Blog, *Are IP Addresses Personal?* (Feb. 22, 2008), http://googlepublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html (last visited May 25, 2016).

[232] *See* 47 U.S.C. § 222(c)(1). As explained, information such as IP addresses and MAC addresses are not, by themselves, reasonably linkable to a particular individual person. Accordingly, even if the definition of CPNI were

logical inference is that carriers are free to use, disclose, or provide access to CPNI that is not "individually identifiable" without obtaining customer approval. While the phrase "individually identifiable" is not defined in Section 222, it must be interpreted to mean what it says – information that is reasonably linkable to a particular *individual person.*

Information need not be aggregated in order to qualify as CPNI or to qualify as not individually identifiable. Indeed, it is entirely possible for a carrier to remove information from a *single customer's* CPNI such that the information is not reasonably linkable to the individual customer. For example, although the duration of a customer's telephone calls qualifies as CPNI, such information would qualify as not individually identifiable if all information that could be used to identify the individual customer is removed. It follows that the Commission must remove from its proposed definition of de-identified information the requirement that the information be aggregated.

Finally, the Commission's broad prohibition on *both* the use and sharing of individually identifiable information is contrary to good public policy. The FTC's 2012 Privacy Report recognized that use and sharing present two very different sets of concerns.[233] This also has been the case with respect to the FCC's voice CPNI rules, where the main justification for differentiating between first- and third-party marketing is that there are fewer concerns with respect to use by the covered entity for first-party marketing than for sharing with third parties for them to market on their own behalf.[234]

---

interpreted to encompass IP addresses or MAC addresses, they do not qualify as individually identifiable CPNI and are therefore not subject to the customer consent requirements of Section 222(c)(1).

[233] *See 2012 FTC Privacy Report* at 38-42. Use of individually identifiable information for first-party marketing – in this context, marketing by the ISP of either the ISP's services and products or another party's services and products – is subject to a much lower bar.

[234] The Commission created the "communications-related services" category in 2002 after the Tenth Circuit held that the broad "opt-in" regime adopted by the Commission in its 1998 CPNI Order violated the First Amendment.

7. The rules should recognize a distinction between independent third parties and contracted agents/vendors acting on behalf of the ISP.

The NPRM asks whether the Commission should treat third parties acting as contractors and performing functions for or on behalf of an ISP differently than other types of third parties.[235] This is an important question that the Commission must get right, since ISPs, like virtually all companies, use trusted third-party vendors to perform various services that the ISP or other company cannot or does not perform "in-house." For example, many companies typically hire a third-party email vendor to coordinate their email marketing campaigns, as such companies are built specifically to manage the process efficiently, economically and securely, keep accurate track of consumer opt-outs, provide helpful reports to the company on the success of the campaign, and so forth. Likewise, in the online advertising marketplace, companies typically contract with ad networks or other vendors to help a company develop and deliver tailored ads to certain websites.[236]

See 2002 CPNI Order ¶ 2 & n.4. The Commission concluded that it was appropriate to apply the less onerous opt-out requirement to telecommunications carriers' use of CPNI to market bundled packages of "communications-related services" because (1) the Commission believed these were the services for which carriers were likely to engage in intra-company marketing (i.e., to engage in protected commercial speech) and (2) customers would benefit from such marketing. *Id.* ¶ 35. In contrast to intra-company marketing, the Commission found that telecommunications carriers had expressed no desire to share CPNI with third parties to market services. *Id.* ¶ 50. While the Commission's beliefs may have been true in 2002 as applied to telephone companies, there is no basis for them in today's Internet marketplace. Limiting opt-out approval to only "communications-related services" is an anachronistic construct that may have been acceptable for the purpose for which it was created, but whose usefulness is no longer applicable or tenable.

[235] *NPRM* ¶ 126.

[236] *See, e.g.*, Experian Marketing Services, Targeted Display Advertising, http://www.experian.com/marketing-services/online-display-advertising.html (last visited May 25, 2016) (providing information on Experian's digital advertising platform, Audience IQ, which helps companies leverage their own data to target advertising and marketing campaigns to consumers); Neustar, Audience Targeting Solutions for Display Advertising, https://www.neustar.biz/resources/product-literature/advertising-ip-targeting-brochure (last visited May 25, 2016) (providing information on Neustar's iP intelligence platform, which helps companies to target their products to consumers by creating customer campaigns, running the advertising campaigns, and providing metrics on their effectiveness); Google Display Network, Targeting Tools, https://www.google.com/ads/displaynetwork/manage-your-ads/targeting-tools.html (last visited May 25, 2016) (providing information on Google's ad placement and targeting products that deliver ads to consumers based on the content they consume while they surf the Internet).

Fortunately, there is considerable guidance available on how to do so, since all privacy laws do make an important distinction between independent third parties who may use data they obtain for their own purposes versus vendors or service providers acting solely on behalf of a company with no independent rights to use the data for any purpose other than as instructed by the company.[237]

For example, under Gramm-Leach-Bliley, the opt-out requirements do not apply to the sharing of "nonpublic personal information to a nonaffiliated third party" to perform various services or functions on behalf of the financial institution, provided that the customer is notified of the sharing and there is a contractual arrangement in place that "prohibits the third party from disclosing or using the information other than to carry out the purposes for which" the information was disclosed.[238] Importantly, this exception explicitly contemplates the use of third-party vendors to assist in marketing efforts.[239] In fact, the Commission's legacy voice CPNI rules also permit telecommunications carriers to share CPNI with their agents on an opt-out basis and thus recognize that there is a distinction between third parties generally and third parties that perform services or functions under contract on behalf of the carrier.[240]

---

[237] *See, e.g.*, European Union, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, at (30) (providing "whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies"); 45 C.F.R. § 164.502(e) (permitting a covered entity under HIPAA to disclose protected information to "business associates" or allow the business associate to handle information on its behalf if the covered entity "obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.").

[238] 12 C.F.R. § 1016.13.

[239] *See id.* § 1016.13(b).

[240] 47 C.F.R. § 64.2007.

Moreover, under Section 217 of the Communications Act, when third parties act for an ISP, their actions are treated by operation of law as actions of the ISP itself. Specifically, Section 217 provides that the acts, omissions, or failure of any such "agent" or "other person" acting for a common carrier are deemed to be the act, omission, or failure of the common carrier.[241] There is no justification for departing from the Commission's own well-established precedent in this area, or from other similar privacy law precedents, by treating ISPs' third-party agents here differently from employees of the ISP for purposes of enforcing Section 222 and the proposed privacy rules.[242] Besides placing undue burdens on ISPs, such an approach would severely hamper the ability of vendors who offer marketing and advertising management and design services from doing business with ISPs, harming those entities, as well.

So in answer to the NPRM's questions, the rules *should* treat third-party agents/vendors differently from other third parties. The key distinction is that the Commission's rules should treat use of customer data by a contracted vendor as if it is an internal use of the data by the ISP or its affiliates.

B. The Commission's Proposed Regime – And Particularly the Proposed Opt-In Requirement – Would Violate the Constitution.

Under the NPRM's proposed opt-in regime, ISPs would be unconstitutionally restricted from engaging in protected commercial speech with customers. At a minimum, the Commission

[241] 47 U.S.C. § 217. In the 2015 Open Internet Order, the Commission declined to forebear from Section 217 and thus this provision applies to ISPs and their affiliate/agent relationships. *2015 Open Internet Order* ¶ 453.

[242] The D.C. Circuit's discussion in *NCTA v. FCC* of the risk posed by disclosure of customer information to third parties not subject to Section 222 is inapplicable here. *See* 555 F.3d 996, 1002 (D.C. Cir. 2009). The court's analysis there only addressed termination of a carrier's contractual relationship with a third-party in the event of a privacy breach. The court concluded that these "after a breach" contractual safeguards were insufficient to protect consumers. *Id.* The court did not consider or address the agency law principles embodied by Section 217 or the legacy CPNI rules at all. But those authorities plainly address the court's concerns by making an ISP fully subject to Section 222 and the FCC's privacy rules for the conduct of its affiliates and agents when using customer information on the ISP's behalf.

may not regulate lawful commercial speech unless the regulation meets the three-prong standard established in *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*.[243] In the more recent *Sorrell v. IMS Health, Inc*. decision,[244] the Supreme Court left open the question whether restrictions on such expression should receive *stricter* First Amendment scrutiny than the intermediate standard applied in *Central Hudson*. The proposed opt-in regime fails under either standard.

Courts have confirmed that the government's decision to impose opt-in, rather than opt-out, rules regarding use of customer data for marketing and advertising messages implicates the basic *Central Hudson* analytical framework for regulatory restrictions on commercial speech.[245] Under this framework, the Commission faces insurmountable challenges in demonstrating that its proposed restrictions on ISPs' commercial speech will materially advance a substantial government interest or are narrowly tailored to address specific, non-conjectural harms to consumer privacy. Indeed, the record demonstrates that prior to reclassification, the Internet

---

[243] *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 557 (1980); *see also U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1232-33 (10th Cir. 1999); *NCTA v. FCC*, 555 F.3d 996 (D.C. Cir. 2009); *Verizon Nw., Inc. v. Showalter*, 282 F. Supp. 2d 1187, 1191 (W.D. Wash. 2003).

[244] 564 U.S. 552 (2011).

[245] *See U.S. West, Inc.*, 182 F.3d at 1232-33; *NCTA*, 555 F.3d 996; *Verizon Nw.*, 282 F. Supp. 2d at 1191. The D.C. Circuit's 2009 decision in *NCTA v. FCC* is not controlling here. The NCTA court did not explain the government's substantial interest. Instead, it simply asserted in dicta that there was a substantial government interest because, "in an analogous context, [] protecting privacy of consumer credit information is a substantial government interest." *NCTA*, 555 F.3d at 1001 (internal quotation marks omitted). But that context is not analogous because it does not involve an opt-in regime. Therefore, that case inapposite. The *NCTA* court, again in dicta, stated without support that restricting carriers' disclosure of CPNI protects CPNI, but even if that were the case in 2009, restricting broadband providers from disclosing customer proprietary information or CPNI would not materially protect that information now because these providers represent such a tiny fraction of the total collection and use of such information. *See id.* Finally, the issue in *NCTA v. FCC* involved carriers sharing CPNI with unaffiliated third parties. As such, even if it could be read to support the Commission's proposed treatment of information that might otherwise be shared with third parties, it cannot be read to support an onerous opt-in regime applied to information that the broadband provider itself uses to market its own products or to help others market their products. None of the concerns that drove the Commission's decision at issue in *NCTA* – loss of carrier control; increased likelihood of unauthorized access; etc. – are present in a situation such as this, where the broadband provider retains control over the information.

ecosystem functioned effectively to protect consumer privacy *without* the onerous default opt-in regime and restrictions on use of de-identified data proposed in the NPRM.

As a threshold matter, in evaluating the constitutionality of a regulation of commercial speech under the First Amendment, a court must determine whether the commercial speech concerns lawful activity that is not misleading.[246] Under the *Central Hudson* test, if the speech is lawful and not misleading, then the government may not restrict the speech unless: (1) the government has a substantial interest in regulating the speech, (2) the regulation directly and materially advances that interest, and (3) the regulation is narrowly drawn.[247] The proposed regulations are unconstitutional because the commercial speech in question here is lawful and not misleading, and the government cannot satisfy any of the remaining *Central Hudson* factors.

1. There Is No Substantial Government Interest.

First, there is no question that privacy is a substantial government interest,[248] but privacy writ large is not the issue here. The relevant question is whether consumers expect or want the privacy of the data they share on the Internet protected through an opt-in approval regime. The Commission has failed to present any evidence that this is something that consumers want or need. ISPs have operated and served customers for over two decades and there is no evidence of any significant consumer unhappiness, harms, or abuses relating to privacy that would establish a compelling governmental interest to impose such onerous new rules. Nor can the Commission do so in light of the fact that so much of the information that would be subject to the proposed opt-in regime for ISPs would be subject to *no* consent requirement or, at most, opt-out consent

[246] *U.S. West, Inc.*, 182 F.3d at 1232-33; *NCTA*, 555 F.3d at 1000.

[247] *Cent. Hudson*, 447 U.S. at 563-66.

[248] *Fla. Bar v. Went for It, Inc.*, 515 U.S. 618, 625 (1995).

requirements for non-ISPs (as well as for different divisions of the ISP's own company operating websites, edge services, etc.), and consumers continue to use those services.

"It is well established that the party seeking to uphold a restriction on commercial speech carries the burden of justifying it."[249] Accordingly, "mere speculation or conjecture will not suffice; rather the State must demonstrate that the harms it recites are real and that its restriction will in fact alleviate them to a material degree."[250] Furthermore, the Commission has the burden of showing that "more limited speech regulation would be ineffective . . . ."[251] This is not a "least restrictive means test," but, rather, a requirement that the regulation be "'narrowly tailored' to serve a significant governmental interest."[252]

There is no evidence that customers want or need to give opt-in approval before an ISP may share customer proprietary information or CPNI with affiliates providing communications-related services for purposes other than marketing those services; no evidence that customers want or need to give opt-in approval before an ISP may use customer proprietary information or CPNI to market its own services that are not communications-related; and, further, no evidence that customers want or need to give opt-in approval for other internal or marketing/advertising uses of the data, especially in ways that would enhance competition, lower consumer prices, and generate innovative new services. In fact, the record show the opposite: the marketplace has demonstrated that consumers are amenable to these types of sharing arrangements when they

[249] *Edenfield v. Fane*, 507 U.S. 761, 770 (1993) (quoting *Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 71, n.20 (1983)) (internal quotation marks omitted).

[250] *Ibanez v. Fla. Dep't of Bus. & Prof'l Regulation, Bd. of Accountancy*, 512 U.S. 136, 143 (1994) (quoting *Edenfield*, 507 U.S. at 770, 771) (internal quotation marks omitted).

[251] *Central Hudson*, 447 U.S. at 571.

[252] *Bd. of Trustees of State Univ. of N.Y. v. Fox*, 492 U.S. 469, 476–81 (1989).

receive value in return. Thus, there is no indication that a substantial government interest exists here.

Moreover, what the Commission does cite as the government's interest – disclosure of "sensitive and very personal information that could threaten a person's financial security, reveal embarrassing or even harmful details of medical history, or disclose to prying eyes the intimate details of interests, physical presence, or fears"[253] and other "intimate, personal details"[254] – reveals a fundamental disconnect between the narrow *asserted* interest and the *actual* breadth and scope of rules. In particular, the interests cited by the Commission all focus on the *disclosure* of information to parties that should not have the information, but the proposed rules would impose significant restrictions on the mere *use* of information to which ISPs already have access.

In addition, and as discussed above, the Commission's proposal goes far beyond the four corners established by Congress in Section 222 of the Communications Act:

- First, the proposed interpretations of CPNI and customer proprietary information would unquestionably expand the scope of Section 222.[255]
- Second, as a practical matter, an opt-in approval regime does not just chill commercial speech, it effectively bans it.[256] The government has no substantial interest in banning commercial speech – as the Commission concedes, there are important consumer benefits to this speech.[257] The proposed rules would violate that constitutional principle, as well.

[253] *NPRM* ¶ 2.

[254] *Id.* ¶ 3.

[255] *See supra* Section V.A.2.

[256] *See supra* Section V.B.

[257] *NPRM* ¶ 12. And even if the commercial speech in question here was not completely banned by the Commission's rules, the Supreme Court has held that "'the distinction between laws burdening and laws banning speech is but a matter of degree' . . . . [l]awmakers may no more silence unwanted speech by burdening its utterance

- Finally, Congress enacted Section 222 in February 1996 to regulate telephony services, not broadband Internet services.[258]

Therefore, there is no clear Congressional statement that would indicate that the Commission should try to shoehorn ISPs into this statutory regime, and then promulgate onerous rules that go far beyond what the statute requires and would effectively ban lawful commercial speech.

2. There Is No Direct And Material Advancement of a Substantial Government Interest.

Second, the Commission's proposed rules do not directly and materially advance the purported government interest in promoting customer privacy and competition. Under *Central Hudson*, the Commission must "demonstrate that the challenged regulation advances the Government's interest in a direct and material way."[259] A "regulation may not be sustained if it provides only ineffective or remote support for the government's purpose."[260] To meet the direct and material advancement requirement, the government must demonstrate that "the harms it recites are real and that its restriction will in fact alleviate them to a material degree."[261] "A prohibition that makes only a minute contribution to the advancement of a state interest can hardly be considered to have advanced the interest 'to a material degree.'"[262]

Even assuming, *arguendo*, that there is a substantial government interest here (which there is not), the Commission must present evidence showing that its proposed rules will

---

than by censoring its content." *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 565-66 (2011) (quoting *United States v. Playboy Entm't Grp., Inc.*, 529 U.S. 803, 812 (2000)).

[258] *See supra* Section V.A.1-2.

[259] *Verizon Nw.*, 282 F. Supp. 2d at n.115 (internal quotation marks omitted).

[260] *Central Hudson*, 447 U.S. at 564.

[261] *Bad Frog Brewery, Inc. v. N.Y. State Liquor Auth.*, 134 F.3d 87, 98 (2d Cir. 1998) (internal quotation marks omitted) (quoting *Edenfield*, 507 U.S. at 771).

[262] *Id.* at 99 (quoting *Edenfield*, 507 U.S. at 771).

materially advance the government's purported interest. The record again shows that the Commission cannot satisfy that requirement. Foremost, the proposed rules apply only to ISPs, which are only a small part of the relevant marketplace.[263] Non-ISPs collect the same –and more – customer data, and account for the vast majority of its use for online advertising and other purposes.[264] The exclusion of such providers from these highly restrictive rules – by mere virtue of the fact that the Commission does not have the authority to regulate them means that these restrictions would, at most, constitute a "minute contribution" to the Commission's purported interest. As such, they cannot be justified under the First Amendment.

For example, in *Sorrell*, the Supreme Court held that a Vermont statute was unconstitutional because the burden placed on protected commercial speech could not be justified by the State's purported interests, and because the statute did not materially advance the State's policy goals.[265] The Vermont statute at issue allowed pharmacy records that revealed the prescribing practices of individual doctors to be "studied and used by all but a narrow class of disfavored speakers. Given the information's widespread availability and many permissible uses, the State's asserted interest in physician confidentiality does not justify the burden that [the statute] places on protected expression."[266]

Similarly here, the Commission's proposed rules would only prohibit ISPs from using customer information while leaving that and similar data widely available to edge providers for many permissible uses under the FTC's privacy regime. Further, the proposed rules would

[263] *See generally supra* Section III.

[264] *Swire Paper* at 3-4.

[265] *Sorrell*, 564 U.S. at 580.

[266] *Id.* at 573.

permit ISPs to use customer information to market narrowly defined "communications-related services," but effectively ban the use of this same information for marketing "non-communications-related services" and other lawful commercial speech. The proposed rules also draw arbitrary distinctions between corporate affiliates of ISPs depending on the particular service they provide, and between ISP affiliates and independent contractors, even if all these speakers are subject to the same confidentiality restrictions and requirements.

Moreover, as shown above, Section 217 of the Communications Act deems the acts or omissions of affiliates and third-party agents, when acting for an ISP, as acts or omissions of the ISP itself. The Commission's own legacy CPNI rules likewise treat affiliates/agents differently from other third parties by requiring a less strict form of approval for the use of CPNI by these entities.[267] And other privacy laws similarly recognize the fundamental difference between an independent third party acting on its own behalf and a vendor/agent acting for a regulated entity; including, for example, HIPAA, which covers much more sensitive information than is handled by an ISP.[268] The Commission has asserted no justification for departing from these well-established precedents by drawing arbitrary distinctions between affiliates and third parties in the use of customer information when done on behalf of an ISP.[269] As in *Sorrell*, therefore, this is "a case in which the government is prohibiting a speaker from conveying information that the speaker already possesses" and imposing clear content- and speaker-based restrictions.[270]

---

[267] *See* 47 C.F.R. § 64.2007(b) ("A telecommunications carrier may, subject to opt-out approval or opt-in approval, disclose its customer's individually identifiable CPNI, for the purpose of marketing communications-related services to that customer, *to its agents and its affiliates* that provide communications-related services.") (emphasis added).

[268] *See supra* notes 242-244.

[269] As shown in note 249 *supra*, *NCTA v. FCC* does not affect this analysis.

[270] *Sorrell*, 564 U.S. at 568.

These attributes of the Commission's rules justify even greater scrutiny under the *Central Hudson* factors, for the reasons explained in *Sorrell*.[271] Foremost, because the Commission has assured the public that it is *not* regulating non-ISPs and other entities that create, collect, or compile customer proprietary information, leaving them free to engage in extensive use of such data,[272] the Commission cannot justify the burden its proposed rules would impose on ISPs alone, let alone demonstrate that these rules "are part of a substantial effort to advance a valid state interest."[273]

In sum, the proposed rules will not have the effect of directly and materially advancing consumer privacy, but will almost certainly have the effect of confusing consumers. ISPs represent a tiny slice of all of the entities that collect this information, such that it is not possible for the Commission to claim that the onerous content-based restrictions proposed in the NPRM will directly and materially advance the purported government interest.

3. The Rules are Not Narrowly Tailored.

Third, the Commission's proposed regulations are not narrowly tailored. In addition to being under-inclusive, the proposed rules are also impermissibly over-inclusive. *Central*

---

[271] *See generally Sorrell*, 564 U.S. 565 (finding that where a statute imposes specific, content-based burden on protected expression that only applies to certain speakers, heighted judicial scrutiny is warranted). *Cf. id.* at 585-86 (Breyer, J., dissenting). Notably, the dissent's arguments disputing the need for heightened scrutiny in *Sorrell* included that the challenged Vermont statute's restrictions: (a) did not forbid or require anyone to say anything or make any form of symbolic speech; (b) were part of a traditional regulatory regime; and (c) directed toward information that exists only by virtue of government regulation. *See id.* Here, the Commission's proposed rules would burden and suppress lawful speech, including both content- and speaker-based restrictions, similar to the unconstitutional Vermont statute. Nor can the Commission seriously contend that the proposed rules are part of a traditional regulatory regime; to the contrary, the Commission proposes to deviate significantly from the traditional FTC privacy regime that has been in place for decades, as well as from other federal privacy regimes. And, the information covered by the Commission's proposed rules is not collected solely by virtue of government regulation, as in *Sorrell*, but rather ISPs collect it for their own legitimate business purposes. Therefore, even if the dissent's viewpoint had prevailed in *Sorrell*—which it did not—it would not be persuasive here.

[272] As previously shown, the FTC requires *opt-out* approval for many of the categories of information for which the Commission would require *opt-in* approval.

[273] *Verizon Nw.*, 282 F. Supp. 2d at 1193.

Hudson's narrow tailoring criterion "requires consideration of whether the prohibition is more extensive than necessary to serve the asserted state interest."[274] The least restrictive means of regulation need not be adopted, but "the means must be reasonable and represent a disposition 'whose scope is in proportion to the interest served.'"[275] Narrow tailoring thus requires that the government's speech restriction reflects a careful calculation of the costs and benefits associated with the burden on speech imposed by its prohibition.[276] "The availability of less burdensome alternatives to reach the stated goal signals that the fit between the legislature's ends and the means chosen to accomplish those ends may be too imprecise to withstand First Amendment scrutiny."[277]

For example, in *Verizon Northwest*, the Washington Utilities and Transportation Commission ("WUTC") argued that opt-in approval was the only approach that would adequately protect CPNI, but the court disagreed.[278] The court held that the evidence upon which WUTC relied did not invalidate opt-out approaches, but rather found that "the *presentation* and *form* of opt-out notices is what determines whether an opt-out campaign enables consumers to express their privacy preferences."[279] As the court observed, "Verizon's experience [in Washington State] strongly suggests that properly controlled opt-out campaigns can protect consumers from the unauthorized use of CPNI without impacting speech to the extent that the current [opt-in] rules do. . . . regulations that address the form, content and timing of opt-

[274] *Bad Frog Brewery, Inc.*, 134 F.3d at 101.

[275] *Bd. of Trustees of State Univ. of N.Y.*, 492 U.S. at 480.

[276] *Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 417 (1993).

[277] *44 Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 529 (1996).

[278] *Verizon Nw.*, 282 F. Supp. 2d at 1194.

[279] *Id.* (emphasis in original).

out notices, when coupled with a campaign to inform consumers of their rights, can ensure that consumers are able to properly express their privacy preferences."[280]

Here, the proposed rules would be over-inclusive because the Commission has chosen to propose the most onerous possible limitations on the use of this information and on the broadest definition of covered customer proprietary information. In contrast, the experience of the past decades has shown that a significantly less speech-suppressing regime administered by the FTC (i.e., a robust opt-out mechanism and heightened protections for particularly sensitive consumer information) can still accomplish the Commission's purported objectives. This is a prudent, more narrowly tailored approach that reasonably balances the concerns regarding consumer privacy without overburdening lawful commercial speech.[281] It is also Constitutionally required. Because the proposed rules are not narrowly tailored to achieve the Commission's stated purposes, and in fact, may only serve to achieve certain edge providers' objectives—seeking to preclude ISPs from competition in the online advertising markets—they plainly violate the First Amendment on this additional ground, as well.

4. The Constitutional Avoidance Doctrine Requires that the Commission Abandon Its Opt-In Proposal.

Under the constitutional avoidance doctrine, the Commission must avoid statutory interpretations that unnecessarily raise constitutional issues. "[W]here an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the

---

[280] *Id.* at 1195; *see also 44 Liquormart*, 517 U.S. at 507 ("[E]ducational campaigns may be more effective at advancing state interest than speech-restricting regulation"); *Linmark Assocs., Inc. v. Willingboro Twp.*, 431 U.S. 85, 97 (1977) ("[G]overnment is free to engage in its own speech and engage in widespread publicity to educate the public about the interest being advanced").

[281] Exec. Order No. 13725, *Steps to Increase Competition and Better Inform Consumers and Workers to Support Continued Growth of the American Economy* (Apr. 15, 2016), https://www.whitehouse.gov/the-press-office/2016/04/15/executive-order-steps-increase-competition-and-better-inform-consumers.

statute to avoid such problems unless such construction is plainly contrary to the intent of Congress."[282] Furthermore, "'[t]he elementary rule is that every reasonable construction must be resorted to, in order to save a statute from unconstitutionality.'"[283]

For the reasons shown above, interpreting Section 222 as authority to impose a general opt-in requirement applicable to either customer proprietary information under Section 222(a) or CPNI under Section 222(c) raises substantial First Amendment questions, and, in fact, would fail under either *Central Hudson* or *Sorrell*. The Commission therefore should reject that interpretation and instead implement the statute in a way that does not violate the Constitution.

C. The Proposed Rules Are Arbitrary and Capricious.

Even if the Commission's proposal does fall within the scope of the authority granted in the Communications Act and does not violate ISPs' commercial speech First Amendment rights, it is still unlawful because it is arbitrary and capricious.[284] The analysis underpinning the Commission's proposed requirements ignores important factors and misreads the evidence before the Commission to reach a result that is completely divorced from the Commission's ostensible purpose.[285]

---

[282] *Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575 (1988).

[283] *Id.* (quoting *Hooper v. California*, 155 U.S. 648, 657 (1895)).

[284] 5 U.S.C. § 706; *see also Allentown Mack Sales & Serv., Inc. v. NLRB*, 522 U.S. 359 (1998). The APA arbitrary and capricious standard requires courts to "hold unlawful and set aside agency action, findings, and conclusions found to be . . . arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706.

[285] "'Not only must an agency's decreed result be within the scope of its lawful authority, but the process by which it reaches that result must be logical and rational.' It follows that agency action is lawful only if it rests 'on a consideration of the relevant factors.'" *Michigan v. E.P.A.*, 135 S. Ct. 2699 (2015) (quoting *Allentown Mack Sales*, 522 U.S. at 374; *Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Automobile Ins. Co.*, 463 U.S. 29, 43 (1983)). "[A]gency decisions must make sense to reviewing courts." *P.R. Sun Oil Co. v. U.S. EPA*, 8 F.3d 73, 77 (1993); *see also Del. Dep't of Nat. Res. and Envtl. Control. v. EPA*, 785 F.3d 1, 13-14 (D.C. Cir. 2015) (finding that the EPA acted arbitrarily and capriciously when it adopted a rule that would have "the opposite effect" of the stated purpose).

"When an administrative agency sets policy, it must provide a reasoned explanation for its action."[286] An agency rule is arbitrary and capricious if, among other things, the agency has "entirely failed to consider an important aspect of the problem, [or] offered an explanation for its decision that runs counter to the evidence before the agency."[287]

As explained, the FCC's proposed rules would not improve the protections established by the FTC's regime and it would affirmatively harm consumers. First, there is simply no evidence that the Commission's proposal will enhance consumer privacy. The Commission completely ignores the fact that the information it seeks to regulate when it is in the possession of ISPs is widely available to virtually anybody else who is willing to collect or purchase it. Those other entities would not be subject to the FCC's rules and would therefore be able to use and disclose ISPs' customer information in ways that the FCC seeks to prevent. The Commission assumes that consumers support the need to increase privacy protections applicable only to ISPs, but the available consumer survey data demonstrates otherwise. In addition, the Commission's proposal would impose extraordinarily restrictive privacy rules on the very class of firms that have a strong record of protecting consumer privacy in the absence of the proposed new rules and that the Commission has found to have strong incentives to protect consumer privacy.

At the same time, the proposed rules would harm consumers in myriad ways. They would introduce new privacy requirements applicable to only a subset of Internet companies, thereby confusing consumers. The rules would deprive consumers of information about valuable new promotions and discounts, including bundles that include non-communications related services such as alarm monitoring. And, they would erect an artificial barrier to ISP entry into

[286] *Judulang v. Holder*, 132 S. Ct. 476, 479 (2011).

[287] *Motor Vehicle Mfrs. Ass'n*, 463 U.S. at 43.

the highly-concentrated online advertising market, thereby harming consumers across many sectors of the economy. The NPRM's complete lack of recognition of these facts demonstrates that its proposal is not based on reasoned analysis and that the Commission is proceeding with willful ignorance of important aspects of the problem it purportedly is trying to address. This is, therefore, a textbook example of arbitrary and capricious rulemaking.

D. The Commission Cannot and Should Not Limit the Extent to Which ISPs Can Use Arbitration Clauses in Their Customer Contracts.

In the NPRM, the Commission seeks comment on whether it should prohibit ISPs from including provisions in customer contracts that call for arbitration for the resolution of privacy disputes.[288] There is no basis in law or policy for such a prohibition. First, the Commission simply does not have the authority to prohibit such clauses. The NPRM cited no sources of authority for this proposition, because there are none. Second, such a prohibition would be affirmatively harmful. Arbitration provisions benefit both customers and carriers because arbitration reduces the cost of and time commitment of dispute resolution for both parties, while simultaneously ensuring an impartial dispute resolution process that is more likely to provide the customer with more targeted and timely relief than a class action lawsuit.[289]

The Commission lacks the authority to prohibit the inclusion of, or limit the application of, arbitration provisions in customer contracts. Under the Federal Arbitration Act ("FAA"), agreements to arbitrate cannot be preempted by rules that contravene the objectives of the FAA,[290] "unless the FAA's mandate has been 'overridden by a contrary congressional

---

[288] *NPRM* ¶ 274.

[289] Jay E. Grenig & Rocco M. Scanza, Case Preparation and Presentation: A Guide for Arbitration Advocates and Arbitrators, at 1-2 (2013).

[290] *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333, 339, 343 (2011) (citing *Doctor's Assocs., Inc. v. Casarotto*, 517 U.S. 681, 687 (1996)).

command.'"[291] This means that an arbitration provision cannot be invalidated by a state law or agency rule that is aimed at discouraging the use of such a provision unless Congress explicitly permits such a rule.

Unsurprisingly, the NPRM does not cite any authority in the Communications Act to adopt such a rule. That is because nowhere in the Communications Act has Congress given the Commission the authority to contravene the FAA by establishing limits on arbitrations; and certainly nothing in Section 222 – which is the subject of this proceeding – even mentions this issue, let alone authorizes the Commission to restrict these contract clauses.[292] Congress clearly knew how to speak to the scope and applicability of arbitration – in Section 252 of the Act, for example, Congress established arbitration procedures for disputes between carriers where the state commission would be the arbitrator.[293] If Congress had wanted to give the Commission such authority, it clearly knew how to do so, and would have done so.

Congress and the Supreme Court have both expressed clear *support* for the use of arbitration in the context of consumer agreements. When Congress enacted the FAA, it established a high threshold for the invalidation of agreements to arbitrate. The Supreme Court

[291] *Am. Express Co. v. Italian Colors Rest.*, 133 S. Ct. 2304, 2309 (2013) (quoting *CompuCredit Corp. v. Greenwood*, 132 S. Ct. 665, 668-69 (2012)) (internal quotations omitted).

[292] *See NPRM*, Dissenting Statement of Commissioner O'Rielly, at 146 ("In addition to the major substantive concerns, I was also alarmed to see the Commission acting on issues that should be completely outside the scope of this proceeding and its jurisdiction. For example, the Commission seeks comment on prohibiting carriers from including mandatory arbitration clauses in contracts with their customers. Here again, the Commission assumes that consumers don't understand the choices they are making and is willing to impose needless costs on companies by mandating how they do business.").

[293] 47 U.S.C. § 252(b); *see also CompuCredit Corp.*, 132 S. Ct. 665 at 672-73 (holding that "[b]ecause the [Credit Repair Organization Act, a federal statute regulating the practice of credit repair organizations] is silent on whether claims under the Act can proceed in an arbitrable forum, the FAA requires the arbitration agreement to be enforced according to its terms").

has "repeatedly described the [FAA] as embod[ying] [a] national policy favoring arbitration."[294] In fact, the Supreme Court has held that "[t]he overarching purpose of the FAA, evident in the text of §§ 2, 3, and 4, is to ensure the enforcement of arbitration agreements according to their terms so as to facilitate streamlined proceedings."[295]

Importantly, the Supreme Court has repeatedly upheld mandatory arbitration clauses in commercial contracts in the face of state laws that seek to invalidate such provisions.[296] In *AT&T Mobility LLC v. Concepcion*, the court found that anti-arbitration laws that create the incentive for class actions suits contravene federal policy favoring arbitration because "the switch from bilateral to class arbitration sacrifices the principal advantage of arbitration—its informality—and *makes the process slower, more costly, and more likely to generate procedural morass than final judgment*."[297] Should the Commission establish rules that prohibit or impinge on carriers' ability to include mandatory arbitration provisions in their commercial contracts for the provision of broadband service, it would contravene express federal law and policy in favor of such agreements.

---

[294] *AT&T Mobility*, 563 U.S. at 346 (internal quotation marks omitted); *Doctor's Assocs., Inc. v. Casarotto*, 517 U.S. 681, 687 (1996).

[295] *AT&T Mobility*, 563 U.S. at 344.

[296] *See, e.g., id.* at 339, 352 (preempting a state law invalidating mandatory arbitration clauses that forbid class action arbitrations as unenforceable); *Nitro-Lift Techs., L.L.C. v. Howard*, 133 S. Ct. 500, 503-04 (2012) (holding that even though the FAA is a more general law, it cannot be overridden by a more specific state law addressing the validity of noncompete clauses in contracts because "[W]hen state law prohibits outright the arbitration of a particular type of claim ,the analysis is straightforward: The conflicting rule is displaced by the FAA." (internal quotation marks and citations omitted)); *Marmet Health Care Ctr., Inc. v. Brown*, 132 S. Ct. 1201, 1203-04 (2012) (determining that "West Virginia's prohibition against predispute agreements to arbitrate personal-injury or wrongful-death claims against nursing homes is a categorical rule prohibiting arbitration of a particular type of claim," and is thus contrary to the FAA); *Southland Corp. v. Keating*, 465 U.S. 1, 10 (1984) (preempting state law requiring a judicial forum for the resolution of claims which the contracting parties agreed to resolve by arbitration).

[297] *AT&T Mobility LLC*, 563 U.S. at 348 (emphasis added).

Contracts between ISPs and their customers for the provision of broadband service fall squarely within the scope of the FAA to the extent they contain agreements to arbitrate privacy-related disputes arising from the service contract. Thus, a Commission rule prohibiting ISPs from including such arbitration provisions regarding privacy-related disputes in their contracts would directly conflict with the FAA by preventing parties from enforcing their contractual commitments to arbitrate under the agreed-upon terms.

Additionally, as the Commission recognizes, "[a]rbitration can be a useful tool in the dispute resolution toolkit."[298] This is for a number of important reasons:

- Arbitration encourages efficiency by allowing parties to work together to quickly resolve disputes in a way that is often more flexible and cost effective than litigation.[299]

- Arbitrations tend to be shorter and cost less than class action litigation. Whereas studies have shown that arbitrations can reach resolution in about 6 or 7 months, pursuing class action litigation can often take more than 20 months.[300]

- Arbitrations also tend to provide individuals with a statistically better chance of recovery than class action litigation. Studies have shown that complainants in arbitrations tend to succeed in receiving some relief over half the time.[301] In contrast, a study by Mayer Brown found that only one-third of the class actions brought during the study period were settled on a class basis and "[f]or those cases that do settle, there is often little or no benefit for class members.[302] A study by the Consumer

---

[298] *NPRM* ¶ 274.

[299] Jay E. Grenig and Rocco M. Scanza, Case Preparation and Presentation: A Guide for Arbitration Advocates and Arbitrators, at 1-2 (2013).

[300] *See* Northwestern University School of Law, Searle Civil Justice Institute, *Consumer Arbitration Before the American Arbitration Association, Preliminary Report*, at 109 (Mar. 2009) ("*Searle Arbitration Report*") ("The average time from filing to final award for the AAA consumer arbitration cases in the case file sample was 207 days (6.9 months)."). In comparison, a study by Mayer Brown found that 14% of the class actions studied remained pending more than 44 months. *See, e.g.*, Mayer Brown LLP, *Do Class Actions Benefit Class Members? An Empirical Analysis of Class Actions*, at 4 (2013), https://www.mayerbrown.com/files/uploads/Documents/PDFs/2013/December/DoClassActionsBenefitClassMembers.pdf ("*Mayer Brown Report*").

[301] *Searle Consumer Arbitration Report* at 109 ("Of the cases in the case file sample, consumer claimants won some relief in 53.3% of the cases (128 of 240) they brought.").

[302] *Mayer Brown Report* at 2.

Financial Protection Bureau found that "[o]nly 15 percent of the class actions studied . . . resulted in settlements that provided monetary benefits to class members.[303]

- Individual recoveries in class actions also tend to be small as the proportional amount each individual recovers when the suit settles is extremely small.[304] In contrast, with respect to arbitrations, "[o]n average, successful consumer claimants were awarded $19,255 in compensatory damages and recovered 52.1% of the amount they sought; the median amount awarded was $5000 and the median percent recovery was 41.7%."

- Arbitration clauses also lead to lower costs for consumers. In particular, the reduced time and cost of arbitration with respect to dispute resolution should reduce the transaction costs that businesses bear more generally in the judicial system. Basic economic principles teach that some portion of those cost savings will be passed along to consumers.[305]

In other words, the flexibility, length, efficiency, likelihood of success, and lower expenses of arbitration make arbitration a much more consumer-friendly option than forcing consumers to seek redress through the already crowded court system.[306] As such, even if the Commission could invalidate mandatory arbitration claims in consumer contract as a matter of law (which it cannot), it should refrain from doing so as a matter of sound public policy.

VI. THE COMMISSION MAY NOT APPLY THE ISP PRIVACY RULES TO CABLE SERVICES UNDER SECTION 631 OF THE COMMUNICATIONS ACT.

In the NPRM, the Commission seeks comment on whether it should apply the privacy rules it has proposed for ISPs to cable operators pursuant to Section 631. The Commission has

---

[303] Jessica Karmasek, *Attorney says New York Times report 'unfairly portrayed' arbitration clauses*, Legal Newsline (Nov. 9, 2015), http://legalnewsline.com/stories/510646919-attorney-says-new-york-times-report-unfairly-portrayed-arbitration-clauses.

[304] *See, e.g., Mayer Brown Report* at 2 ("But of the six cases in our data set for which settlement distribution data was public, five delivered funds to only miniscule percentages of the class: 0.000006%, 0.33%, 1.5%, 9.66%, and 12%. Those results are consistent with other available information about settlement distribution in consumer class actions.").

[305] *See* Stephen J. Ware, *The Case for Enforcing Adhesive Arbitration Agreements—With Particular Consideration Of Class Actions and Arbitration Fees*, 5 J. Am. Arbitration 251 (2006) ("In the case of consumer arbitration agreements, this benefit to businesses is also a benefit to consumers. That is because whatever lowers costs to businesses tends over time to lower prices to consumers.").

[306] *See, e.g.*, Judicial Council of Cal., 2016 Budget Snapshot: County of Los Angeles (Feb. 2016), http://www.courts.ca.gov/partners/documents/County_Budget_Snapshot_LosAngeles_2016.pdf.

no authority to do so, nor should it do so, and should instead stay true to what it has been telling the world for over a year: that the focus of this proceeding would be on the application of Section 222 to broadband Internet services. The structure of the Act and the terms of Section 631 preclude the Commission from applying the regime proposed in the NPRM to cable services, and there is no policy basis for doing so.[307]

The terms and structure of the Communications Act make it crystal clear that Congress intended that the privacy regime for cable services would be different from the privacy regime for telecommunications services. Section 631 establishes a specific and comprehensive regime governing cable services that differs in numerous fundamental respects from the regime established in Section 222. For example, Section 631 applies to the company's collection and disclosure of personally identifiable information ("PII"), whereas Section 222 does not even mention PII and focuses instead on the use, disclosure, and access to CPNI.[308] Section 631

[307] The Commission's complete disregard for the incredible complexity of this proceeding in its outright rejection of numerous requests for extension is a staggering example of willful ignorance. *See Protecting the Privacy of Customer of Broadband and Other Telecommunications Services*, Order, DA 16-473 (Apr. 29, 2016) (denying extension requests filed by Association of National Advertisers, the State Privacy & Security Coalition, Inc., the American Advertising Federation et al., and the American Cable Associations et al.). As Commission Pai has aptly noted, "I don't think it is too much to ask for a couple extra weeks to allow the numerous stakeholders, some of which are trade associations with hundreds of members who have to be canvassed, to weigh in on these many many questions. I think Commissioner Rosenworcel, my colleague got it exactly right, that there are some contradictions here that make privacy complicated and this rulemaking asks questions, lots and lots of questions. It's extremely important for the FCC to act, if indeed it's going to have a full and impartial rulemaking to act on the basis of a fully developed record. We can't do that if we don't give people enough time to comment." *Examining the Proposed FCC Privacy Rules: Hearing Before the Subcomm. on Privacy, Technology and the Law of the Senate Comm. on the Judiciary*, 115th Cong. (May 11, 2016), http://www.c-span.org/video/?409389-1/fcc-commissioners-testify-proposed-internet-privacy-rules (starting at 01:19:27). Moreover, "[e]ven if one could have foreseen the extensive and complex issues that would be raised in the *Notice* with respect to the proposed rules for BIAS providers . . . the *Notice* goes much further by asking whether these rules should also be extended to legacy voice CPNI rules and cable and satellite providers in the name of 'harmonization' – something which the *Open Internet Order* never contemplated, let alone communicated to the public. These points alone raise entirely new, complex, and disconcerting issues that stakeholders need to study before they can provide thoughtful comment." ACA et al. Motion for Extension of Time, WC Docket No. 16-106, at 7 (filed Apr. 20, 2016).

[308] *Compare* 47 U.S.C. § 551(a), *with id.* § 222(c).

explicitly provides for the destruction of PII, whereas Section 222 does not.[309] Section 631 explicitly provides for a private right of action in the courts by those who have been aggrieved in violation of the statute, whereas Section 222 does not.[310]

When Congress enacted Section 222 in 1996, it could easily have applied to telecommunications services the requirements applicable to cable companies, which had been enacted in 1984.[311] Congress did exactly that when it adopted Section 338(i), which governs the privacy rights of satellite subscribers, in 2004.[312] Alternatively, Congress could have written the statute so that cable services would be subject to the same standards it drafted for telecommunications services, but it did not. This must be construed as an intentional decision to treat privacy rules for telecommunications services differently from those for cable and satellite services.

Other provisions of Title VI support this conclusion. For example, Section 621(c) states that "[a]ny cable system shall not be subject to regulation as a common carrier or utility by reason of providing any cable service."[313] The Commission proposes to adopt the rules described in the NPRM pursuant to Section 222, which applies only to telecommunications carriers. The Commission has interpreted the terms telecommunications carrier and common carrier to mean the same thing.[314] Thus, applying the requirements of Section 222 or the

---

[309] *Compare id.* § 551(e), *with id.* § 222.

[310] *Compare id.* § 551(f), *with id.* § 222.

[311] *See* Cable Communications Policy Act of 1984, Pub. L. No. 98-549, § 631, 98 Stat. 2779 (1984).

[312] *See* Consolidated Appropriations Act, 2005, Pub. L. No. 108-447, § 206(a), 118 Stat. 2809 (2004).

[313] 47 U.S.C. § 541(c).

[314] *See AT&T Submarine Systems, Inc. Application for a License to Land and Operate a Digital Submarine Cable System Between St. Thomas and St. Croix in the U.S. Virgin Islands*, Memorandum Opinion and Order, 13 FCC Rcd. 21585, ¶ 6 (1998) ("As the Commission has previously held, the term 'telecommunications carrier' means essentially the same as common carrier."); *Cable & Wireless, PLC, Application for a License to Land and Operate*

regulations promulgated thereunder, as proposed in the NPRM, to cable services would constitute subjecting cable services "to regulation as a common carrier" in violation of Section 621(c). Conversely, Section 621(b)(3)(A)(ii) prohibits the extension of Title VI regulation to telecommunications services offered by cable operators and their affiliates, thereby further reinforcing the separate treatment of telecommunications services and cable services in the Act.[315]

In addition, Section 624(f)(1) prohibits "[a]ny Federal agency . . . [from] impos[ing] requirements regarding the provision or content of cable services, except as expressly provided in [Title VI]."[316] The Commission is a "Federal agency," and privacy regulations governing cable services constitute "requirements regarding the provision . . . of cable services." Thus, the only section of the Communications Act under which the Commission may regulate privacy practices for cable services is Section 631. Together Sections 621(c), 621(b)(3)(A)(ii), and 624(f)(1) evidence Congress's unmistakable intention that the regulatory requirements, including those applicable to privacy, for cable and telecommunications services should be different. The Commission is bound to honor that intention.

Even if this were not true, the Commission still could not apply the privacy regime proposed in the NPRM to cable services because the terms of Section 631 preclude it from doing so. For example, the Commission would not be able to adopt regulations governing CPNI under Section 631 because that provision only governs PII, a term that the Commission recognized

---

in the United States a Private Submarine Fiber Optic Cable Extending Between the United States and the United Kingdom, Cable Landing License, 12 FCC Rcd. 8516, ¶ 13 (1997).

[315] 47 U.S.C. § 541(b)(3)(A)(ii).

[316] *Id.* § 544(f)(1).

encompasses a different set of information than CPNI.[317] The Commission would not be able to adopt regulations governing the information of prospective customers under Section 631 because that provision only applies to "subscribers," a term that cannot be read to include prospective customers. The list goes on and on, and it makes clear that the Commission may not apply the rules adopted under Section 222 to cable services regulated under Section 631.

Finally, there is no policy basis for altering the current privacy regime for cable services. There is no record of cable company violations of consumer privacy. In fact, there have been very few cases brought against cable companies under Section 631, which governs the privacy of cable service subscribers. The majority of cases invoking Section 631 involve an entity seeking a subpoena to obtain the identity of a cable company's subscriber whom the complaining entity claims violated copyright or another form of law.[318] There have been only a handful of cases even alleging violations of Section 631, much less holding that a cable company had committed a violation. Thus, any suggestion that the privacy rules applicable to cable services should be changed is a solution in search of a problem and should be abandoned.

---

[317] Courts have consistently interpreted the term personally identifiable information in a manner that would exclude most CPNI. *See Scofield v. Telecable of Overland Park, Inc.*, 973 F.2d 874, 876 n.2, 877 (10th Cir. 1992) (identifying PII as including "specific information about the subscriber, or a list of names and addresses on which the subscriber is included. . . ."); *Pruitt v. Comcast Cable Holdings, LLC*, 100 F. App'x 713, 715 (10th Cir. 2004) (determining that certain information stored in cable converter boxes is not PII); *Eichenberger v. ESPN*, No. 14-463, 2015 WL 7252985, at *3 (W.D. Wash. May 7, 2015) (dismissing plaintiff's complaint that the defendant violated the Video Privacy Protection Act because the plaintiff failed to allege the defendant disclosed PII by disclosing the plaintiff's Roku serial number).

[318] *See, e.g., Rotten Records, Inc. v. Doe*, 108 F. Supp. 3d 132 (W.D.N.Y. 2015) (considering whether a copyright holder had good cause to get a subpoena to require the cable company to disclose the identity of an individual who had allegedly infringed on the rightsholder's copyright before the discovery conference).

VII. CONCLUSION

The Commission should not adopt its proposed rules, as they would harm consumers, innovation, broadband investment, and online competition. Instead, assuming Section 222 authorizes the Commission to regulate broadband privacy, it should:

(1) adopt the Consensus Privacy Framework as further explained in these Comments, which will continue to protect consumers, while promoting continued competition, innovation, and investment in the vibrant Internet ecosystem;

(2) consistent with the Consensus Privacy Framework and the FTC and Administration's policies, focus the rules on CPNI, apply opt-in consent solely for sensitive information and implied consent (or at most opt-out consent) for first-party marketing, adopt a reasonable de-identification standard, and maintain a distinction between ISPs' contracted agents/vendors and independent third parties that follows other privacy laws;

(3) permit ISPs to offer price discounts or other benefits to their customers in exchange for their consent to allow the use or disclosure of their data for marketing or advertising;

(4) refrain from banning or imposing any restrictions on arbitration clauses in ISP customer agreements;

(5) refrain from applying the any ISP privacy rules to cable services under Section 631; and

(6) adopt sensible data breach rules that (i) apply only to sensitive personal information; (ii) incorporate reasonable exceptions that are commonplace in other breach rules for encryption, substantial consumer harm, and inadvertent disclosures; and (iii) allow at least 30 days after discovery of the breach to send the notification.

Respectfully submitted,

/s/ *Kathryn A. Zachem*
Kathryn A. Zachem
Mary P. McManus
Regulatory Affairs,
Comcast Corporation

Francis M. Buono
Legal Regulatory Affairs,
Comcast Corporation

Rebecca Arbogast
Rudy N. Brioché
Global Public Policy,
Comcast Corporation

Gerard J. Lewis, Jr.
Chief Privacy Officer,
Comcast Cable Communications

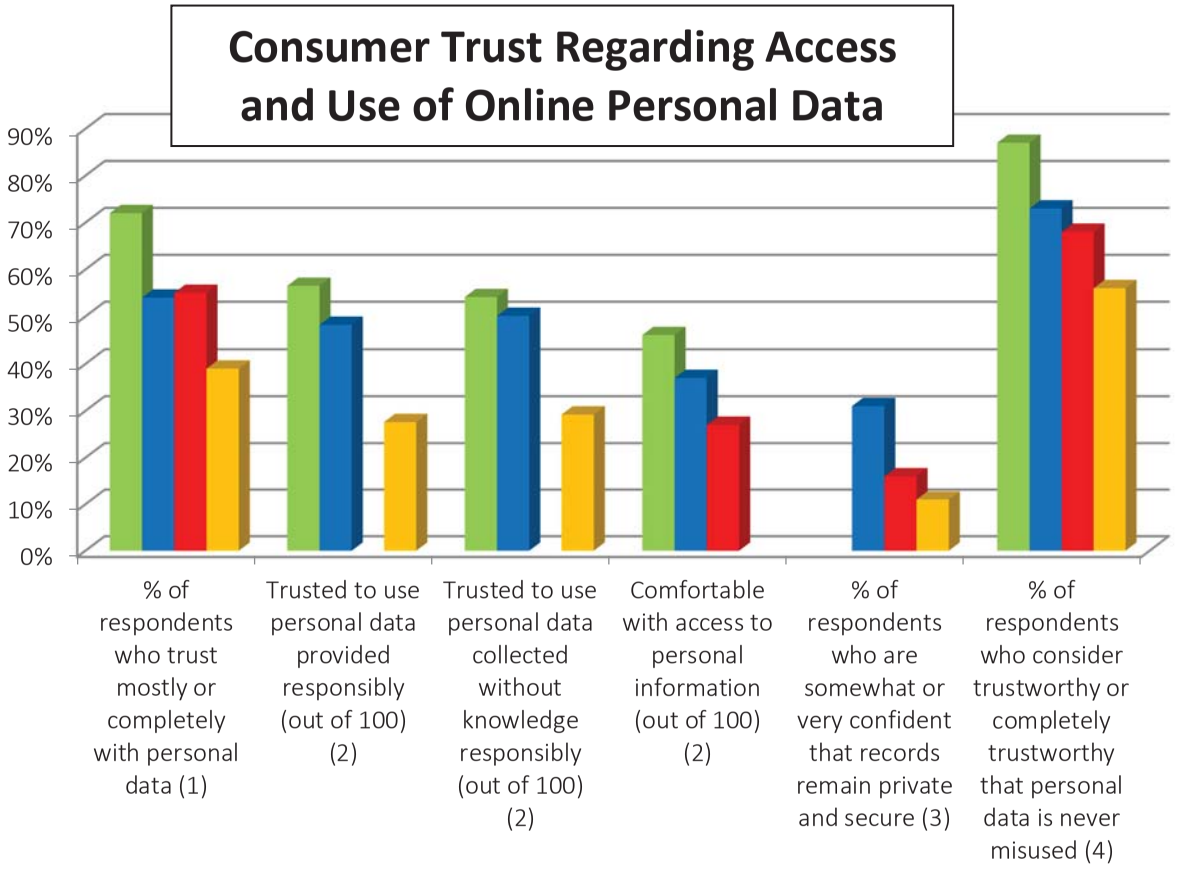
COMCAST CORPORATION
300 New Jersey Avenue, N.W., Suite 700
Washington, DC 20001

WILLKIE FARR & GALLAGHER LLP
1875 K Street, N.W.
Washington, D.C. 20006

Counsel for Comcast Corporation

May 27, 2016

APPENDIX A – CONSUMER TRUST SURVEY DATA



(1) GFK Survey on Data Privacy and Trust, GfK (March 2014), http://docplayer.net/9299896-Gfk-survey-on-data-privacy-and-trust.html

(2) "Perceptions of Privacy Online and in the Digitally Connected World" Data Privacy Research Result Summary, National Cyber Security Alliance, (Released January 28, 2015), http://staysafeonline.org/download/datasets/12472/DPD%20Privacy%20Research%20Results%20Summary%20v3.pdf

(3) Mary Madden, Lee Rainie, Americans' Attitudes About Privacy, Security and Surveillance, Pew Research Center (May 20, 2015), http://www.pewinternet.org/files/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf

(4) Timothy Morey, Theodore "Theo" Forbath, and Allison Schoop, *Consumer Data: Designing for Transparency and Trust,* Harvard Business Review (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust#

***Note**: Not all surveys used the same terms to categorize different providers, and some surveys did not include certain categories. This chart reflects our best reading of the terms and categories used by the different surveys in an effort to normalize results for purposes of comparison.*

APPENDIX B – CONSENSUS PRIVACY FRAMEWORK

March 1, 2016

The Honorable Tom Wheeler
Chairman
Federal Communications Commission
445 12th St. SW
Washington, D.C. 20554

Dear Chairman Wheeler,

Today, the American Cable Association, Competitive Carriers Association, CTIA, National Cable & Telecommunications Association, and USTelecom offer for the Commission's consideration a detailed proposal for a broadband privacy framework. After significant examination and analysis, these associations have developed the attached consensus Privacy Framework setting forth guidelines and principles to protect consumer privacy in a way that is consistent with other privacy laws that apply to companies providing services online. By adopting these principles, the Commission would establish a regime that protects consumer privacy and security while also providing flexibility for providers to implement and update their practices as consumer expectations and technologies evolve.

If the courts determine that the Commission has authority over broadband privacy, the FCC should focus on four privacy principles: (1) transparency; (2) respect for context and consumer choice; (3) data security; and (4) data breach notification. For each of these principles, the FCC should draw from and harmonize with the longstanding Federal Trade Commission unfairness and deception approach to privacy, which, before the FCC's reclassification decision, governed the privacy practices of all companies in the Internet ecosystem and will continue to apply to non-ISPs going forward.

As the Commission develops its approach to broadband privacy, we respectfully request that it seek comment on the entirety of the Privacy Framework we submit today. Because regulation of broadband privacy is a new area for the Commission, it should take the necessary time to build a robust record rather than prejudge the issues by adopting tentative conclusions before there is a public discussion of the consensus Privacy Framework.

We look forward to continuing a conversation with the Commission about the best way to provide privacy and innovation benefits to consumers.

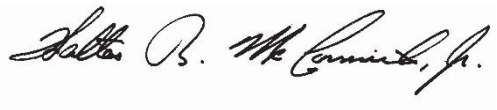
Respectfully submitted,

Matthew M. Polka
President & CEO
American Cable Association

Steven K. Berry
President & CEO
Competitive Carriers Association

Meredith Attwell Baker
President & CEO
CTIA

Michael Powell
President & CEO
National Cable & Telecommunications Association



Walter B. McCormick, Jr.
President & CEO
USTelecom

cc: The Honorable Mignon Clyburn
The Honorable Jessica Rosenworcel
The Honorable Ajit Pai
The Honorable Michael O'Rielly

Privacy Framework

Discussion Paper

All entities in the Internet ecosystem should be subject to a consistent privacy framework with respect to consumer information. Consumer information should be protected based upon the sensitivity of the information to the consumer and how the information is used—not the type of business keeping it, how that business obtains it, or what regulatory agency has authority over it. Consumers should have consistent and predictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it. Consumers also will benefit from a consistent privacy framework that promotes the emergence of new business models and innovative uses of data that foster increased consumer choice and service customization.

The FCC should adopt an approach to privacy and data security for CPNI that is flexible, harmonized with the well-established and successful FTC framework, and backed up by strong but fair enforcement for unfair or deceptive acts or practices (UDAP) that materially harm consumers.[1] This well-tested consumer protection approach is consistent with the FCC's privacy recommendations in the 2010 National Broadband Plan, the FTC's and White House's 2012 Privacy Reports, and the White House's 2015 Consumer Privacy Bill of Rights, as well as with Chairman Wheeler's recent testimony before Congress acknowledging the importance of coordination with the FTC and harmonization with its privacy framework.

That approach will benefit consumers by safeguarding privacy interests as it has for years and will ensure that the same privacy and security framework applies to all entities in the Internet ecosystem. By leveraging a tested privacy model, the FCC will avoid inconsistent requirements that could otherwise hamper innovation and reduce competition. Most important, it will minimize consumer confusion as well as other harms associated with disparate privacy regulation across the ecosystem. Indeed, this approach will align with consumers' expectations that their data would be subject to consistent privacy rules regardless of whether it is used by their Internet Service Provider (ISP), application developers, operating systems, or edge providers.

When adopting a framework, the FCC should keep the following guidelines in mind:

- Consistent and Coordinated Regulatory Regimes. The FCC's rules and principles for regulating and enforcing privacy and security should be as similar as possible to the FTC approach, which will continue to govern other Internet ecosystem players' use and disclosure of the same or similar data. The consistent application of standards across sectors would fulfill the following key tenets in the White House Privacy Report: (1) avoid "inconsistent standards for related technologies" that could dampen innovation; (2)

[1] This framework is intended for discussion purposes, and we are not conceding that the FCC has authority to adopt privacy and security rules for Broadband Internet Access Services or over data related to consumers' use of Broadband Internet Access Services. To the extent it is determined that the FCC has such statutory authority, this document is intended to set forth principles for FCC consideration and possible adoption that are harmonized and consistent with the FTC and other government entities' approach to privacy and security for the same or similar data. Even if courts determine that the FCC's reclassification of Broadband Internet Access Services is a lawful exercise of authority, any rules must not exceed the text and legislative history of Section 222 of the Act.

foster a "level playing field for companies;" and, most importantly, (3) create "a consistent set of expectations for consumers." To achieve this end, the FCC's policies, rules, and enforcement practices should conform to the longstanding limiting principles articulated in the FTC's Unfairness and Deception Policy Statements. In addition, the FCC and FTC can achieve their recent MOU's stated goal of avoiding "duplicative, redundant or inconsistent oversight" by developing a new process to ensure that their substantive privacy policies and basis for enforcement are consistent going forward.

- Flexibility. The FCC's approach should provide a flexible framework within which telecommunications service providers can implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments in this space. Specifically, this framework should identify the privacy or security *goals*, and afford providers flexibility in achieving those goals, rather than dictate the particular *methods* by which providers are expected to achieve those goals. Adopting a flexible approach also will help ensure consistent federal and state requirements governing customer information.
- Application. Consistent with the Communications Act and to eliminate unnecessary duplication of authority with other agencies, the FCC's framework should only apply when 1) telecommunications service providers are providing telecommunications services and 2) the CPNI is made available by the customer to the telecommunications service provider solely by virtue of the carrier-customer relationship. The framework cannot lawfully apply to:
    - Providers' non-telecommunications services and products
    - Providers' non-telecommunications service provider affiliates
    - Information that is not made available to the carrier by the customer solely by virtue of the carrier-customer relationship
- Individually Identifiable. The FCC should carve out from the scope of its new framework any data that is de-identified, aggregated, or does not otherwise identify a known individual. The insights derived from the use of de-identified data can offer great benefits to consumers and society and such use avoids the sensitivities that may be associated with identified data.
- Unfair or Deceptive Conduct. As noted above, the FCC's policies, rules, and enforcement practices should conform to the FTC's longstanding limiting principles articulated in its Policy Statements on Unfairness (1980) and Deception (1983). This approach is consistent with the FCC's commitment to conduct a cost-benefit analysis of its regulatory framework in accordance with President Obama's Executive Orders 13563 and 13579, which require agencies to "adopt a regulation only upon a reasoned determination its benefits justify its costs" and "tailor its regulations to impose the least burden on society."
    - Unfair Conduct. A provider acts unfairly if its act or practice (1) causes or is likely to cause substantial injury to consumers (2) which is not reasonably avoidable by consumers themselves, and (3) is not outweighed by countervailing benefits to consumers or to competition.
    - Deceptive Conduct. A provider acts deceptively if (1) it makes a statement or omission, or engages in a practice, that is likely to mislead a customer, (2) viewed from the perspective of a consumer acting reasonably under the circumstances, and (3) the deceptive statement, omission, or practice is material—meaning that

the misrepresentation or practice is likely to affect the consumer's conduct or decision with regard to a product or service.

- Additional Guidance. In coordination with other privacy regulators, the FCC could, like the FTC and various states like California, provide additional guidance on how it interprets its framework through workshops or reports. The FCC also could encourage and support the development and implementation of industry guidelines.
- Update and Harmonize Existing CPNI Rules. The existing CPNI rules should be revisited in their entirety and modernized to use the same flexible framework for all services subject to Section 222, including traditional voice services. In no event should the prescriptive outdated CPNI rules designed for legacy voice services apply to broadband services. Instead, a common set of flexible policies that allow providers to keep up with their customers' expectations and evolving technology should apply to both types of services.

With these guidelines in mind, if the courts determine that the FCC has authority to regulate broadband privacy, the FCC could adopt the following principles, which encompass and are consistent with the privacy and security framework that applies to the rest of the industry. Each of these principles and the goals noted above should provide flexibility for providers to implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments:

- Transparency. A telecommunications service provider should provide notice, which is neither deceptive nor unfair, describing the CPNI that it collects, how it will use the CPNI, and whether and for what purposes it may share CPNI with third parties.
- Respect for Context and Consumer Choice. A telecommunications service provider may use or disclose CPNI as is consistent with the context in which the customer provides, or the provider obtains, the information, provided that the provider's actions are not unfair or deceptive. For example, the use or disclosure of CPNI for the following commonly accepted data practices would not warrant a choice mechanism, either because customer consent can be inferred or because public policy considerations make choice unnecessary: product and service fulfillment, fraud prevention, compliance with law, responses to government requests, network management, first-party marketing, and affiliate sharing where the affiliate relationship is reasonably clear to consumers. Consistent with the flexible choice mechanisms available to all other entities in the Internet ecosystem, telecommunications service providers should give consumers easy-to-understand choices for non-contextual uses and disclosures of their CPNI, where the failure to provide choice would be deceptive or unfair. The provider should consider the sensitivity of the data and the context in which it was collected when determining the appropriate choice mechanism.
- Data Security. A telecommunications service provider should establish, implement, and maintain a CPNI data security program that is neither unfair nor deceptive and includes reasonable physical, technical, and administrative security safeguards to protect CPNI from unauthorized access, use, and disclosure. Providers' CPNI data security programs should provide reasonable protections in light of the nature and scope of the activities of the company, the sensitivity of the data, and the size and complexity of the relevant data operations of the company.

- Data Breach Notifications. Telecommunications service providers should notify customers whose CPNI has been breached when failure to notify would be unfair or deceptive. Given that breach investigations frequently are ongoing at the time providers offer notice to customers, a notice that turns out to be incomplete or inaccurate is not deceptive, as long as the provider corrects any material inaccuracies within a reasonable period of time of discovering them. Telecommunications providers have flexibility to determine how and when to provide such notice.

The FCC can ensure compliance with the above principles by pursuing reasonable enforcement actions against telecommunications service providers that have clearly violated these principles.