

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)
)

REPLY 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

July 6, 2016

Table of Contents

Page

I. INTRODUCTION AND SUMMARY.....	1
II. THE RECORD OVERWHELMINGLY DEMONSTRATES THAT THE COMMISSION’S PROPOSALS WOULD BE AFFIRMATIVELY HARMFUL TO CONSUMERS AND UNDERMINE IMPORTANT PUBLIC POLICY GOALS, WITHOUT ANY BENEFIT OR JUSTIFICATION.....	7
A. Commenters Broadly Demonstrate the Numerous Consumer and Other Harms that Would Result from the Commission’s Proposals.....	8
1. Consumers will be confused by a regime that treats the <i>same</i> data used for the <i>same</i> purposes differently based solely on the entity that holds it.	9
2. Consumers will be less-informed and less able to take advantage of innovative services and discounted offerings that they have consistently received marketing for and benefited from for many years.	12
3. The proposed data breach rules will subject consumers to over-notification and warning fatigue.....	15
4. The proposed rules will prevent consumers from receiving lower prices or other offers of value in exchange for the use of their data.....	18
5. The proposed rules will harm innovation, broadband investment, and competition.	21
6. The proposed rules will harm network security and hamper ISPs’ ability to efficiently work with trusted third parties.	24
B. Purported Benefits and Justifications Cited by Supporters Do Not Stand Up to Marketplace Facts or Record Evidence.....	28
1. Overbroad opt-in consent does not benefit consumers.	28
2. The Commission’s proposed privacy rules for ISPs will not improve broadband adoption.	32
C. ISPs Do Not Have Unique or Comprehensive Access to Consumer Data on the Internet.....	34
1. ISPs are not unique in their ability to collect or use consumer data.....	34
2. The Commission’s proposals will not materially advance consumer privacy.....	39
III. THE RECORD OVERWHELMINGLY DEMONSTRATES THAT THE COMMISSION’S PROPOSALS ARE UNLAWFUL.....	40
A. The Commission’s Proposals Would Violate the First Amendment.....	40
B. Any Authority the Commission May Have in Section 222 to Regulate ISP Data Usage and Sharing Practices Is Carefully Circumscribed.....	44

Table of Contents
(continued)

Page

1. The Commission may not expand the scope of its framework to encompass <i>non</i> -CPNI like IP addresses and device identifiers.	45
2. Section 222 excludes <i>both</i> aggregate and de-identified information.	47
3. Section 222 does not govern information that ISPs obtain from third parties.....	49
C. Other Provisions of the Communications Act Do Not Support the Proposed Rules.....	50
D. The Commission Cannot Prohibit or Limit the Use of Mandatory Arbitration Clauses.	53
E. The Commission Should Not and Cannot Extend Its Rules to Cover ISPs’ Affiliates.....	55
F. Adopting the Proposed Rules Would Be a Textbook Example of Arbitrary and Capricious Rulemaking.....	60
IV. THERE IS WIDESPREAD CONSENSUS IN THE RECORD THAT THE COMMISSION SHOULD CLOSELY ALIGN ITSELF WITH THE TECHNOLOGY-NEUTRAL POLICIES AND PRINCIPLES ESPOUSED BY THE ADMINISTRATION AND THE FTC.....	61
A. The Administration and FTC Approach Have Successfully Protected Consumers While Facilitating Innovation, Competition, and Investment.	61
B. The Consensus Privacy Framework Is the Best Path Forward to Achieve the Commission’s Goals.....	64
V. CONCLUSION	67

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)	
)	

REPLY COMMENTS OF COMCAST CORPORATION

Comcast Corporation (“Comcast”) hereby replies to comments submitted in response to the above-captioned Notice of Proposed Rulemaking (“NPRM”). Comments from industry, advertising, academia, public interest and civil rights organizations, edge providers, small businesses, current and former government officials, and sister federal agencies demonstrate that the onerous, prescriptive, and inflexible regime proposed by the Commission is incompatible with sound public policy; likely to harm consumers, innovation, and competition; outside the scope of the Commission’s authority; arbitrary and capricious; and unconstitutional. Notably, comments filed by the Federal Trade Commission (“FTC”) call the FCC’s proposed approach “not optimal” and proffer many recommendations for changes, including limiting the opt-in consent requirement to the use of sensitive data.

By contrast, there is widespread agreement that adopting an approach that aligns closely with the one espoused and embraced by the Obama Administration and the FTC for many years – and reinforced in the FTC’s comments in this proceeding – would accomplish the FCC’s goals, while still allowing entities on the Internet to compete, innovate, and invest in ways that benefit consumers and the public interest. The Consensus Privacy Framework, supported by Comcast and others, accomplishes this.

I. INTRODUCTION AND SUMMARY

“FTC staff is mindful that the FCC’s proposed rules, if implemented, would impose a number of specific requirements on the provision of BIAS services that would *not* generally apply to other services that collect and use significant amounts of consumer data. This outcome *is not optimal.*”¹ In two brief sentences, the FTC cuts straight to the heart of the issue presented by the FCC’s NPRM.² After decades of having a cohesive, technology-neutral privacy regime on the Internet that has worked well to protect consumers – one with which Internet service providers (“ISPs”) dutifully complied as well as or better than any other group of entities on the Internet – the FCC has proposed to move forward with rules that would completely upend settled expectations; leave consumers confused, less-informed, and deprived of longstanding discounted offerings; stifle competition, investment, and innovation; and hamstring data security efforts – all without any material improvement to consumer privacy.

The FTC’s comments are particularly telling, raising over 25 concerns with, and recommending substantial changes to, key aspects of the FCC’s proposals, including the scope of data covered, the approach to consumer consent particularly with respect to first-party marketing, the de-identification standard, data security requirements, and data breach notification obligations. In particular and very importantly, the FTC concludes that the FCC’s default opt-in “approach does not reflect the different expectations and concerns that consumers have for sensitive and non-sensitive data,”³ and that “[o]pt-out is sufficient for use and sharing of non-

¹ FTC Comments at 8 (emphasis added). For the sake of brevity, all references in this pleading to “Comments” are to submissions in Docket No. 16-106 in response to the NPRM. Any references to comments filed in other proceedings include specific citations to the proceeding in which the comment was filed.

² *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*”).

³ FTC Comments at 22.

sensitive data.”⁴ In light of the clear record evidence, the Commission should substantially amend its proposal to more closely align with the Administration and FTC approach to privacy.

Numerous commenters, including the FTC and current and former FTC officials, agree with Comcast that the Commission’s current proposal would be detrimental to consumers and the public interest. In particular:

- *Consumers would be harmed.* The record includes many concrete examples of how consumers would be worse off under the Commission’s proposals. ISPs, public interest groups, academics, technology companies, advertisers, and others highlight how the Commission’s proposals would (1) lead to consumer confusion and frustration because the same data used for the same exact purposes would be subject to dramatically different privacy regimes based solely on the identity of the data collector; (2) make it much less likely that consumers will be informed about discounts and other offerings that would substantially benefit them; and (3) inundate consumers with meaningless breach notifications that would lull them into ignoring real threats. Likewise, the proposal to prohibit ISPs from offering discounts or other value to customers in exchange for their consent to use their data for advertising or other purposes is both paternalistic and decidedly anti-consumer. This business model is widely used throughout the Internet, and it works well because consumers are capable of making decisions so long as they are fully informed. Critics also ignore the potential benefits – to broadband adoption, to competition, and to innovation – of these models.
- *Innovation would be stifled.* Numerous commenters explain how the Commission’s proposed rules would be so expansive and inflexible as to ossify business models and prevent ISPs from using even basic, non-sensitive data – including data that is not customer proprietary network information (“CPNI”) – to innovate, as other companies in the Internet ecosystem routinely do under the more reasonable and time-tested FTC privacy framework that will continue to apply to them.
- *Broadband investment would be dampened.* For many years now, the Commission has expressly recognized that a company’s ability to offer bundled services has been central to the economics of investing in and deploying next-generation broadband networks. The record confirms that the Commission’s proposals in the proceeding, however, would be an enormous step backwards, making it significantly harder for ISPs to market the kinds of bundles and discounts that significantly benefit individual consumers and facilitate additional broadband investment and deployment.
- *Competition would be harmed.* The record confirms the Commission’s proposals would harm competition, most directly by imposing a sweeping and unprecedented opt-in consent regime solely on ISPs that would limit ISPs’ ability to compete in the highly

⁴ *Id.* at 35.

concentrated online advertising marketplace – 70 percent of which is controlled by *non-ISP*s and in which ISPs do not have a significant presence today (not a single ISP is among the top-10 players in this space). But the competitive harms would extend far beyond ISPs. For example, the record is replete with comments by small energy companies, healthcare providers, advertisers, and others highlighting how the proposals would hamstring small businesses that need to be able to leverage the scale and scope of the ISP platform to reach consumers and compete against larger incumbents in their respective industries. The anti-competitive ripple effects of the Commission’s proposals are extensive and profound.

- *Network security would be harmed.* Academics, researchers, technology companies, former government officials, the FTC, and others highlight the problems that would result because the Commission’s proposal would impose inflexible and rigid security requirements, as well as effectively bar ISPs from sharing information with trusted third-parties who help ensure the security, reliability, and integrity of the service.

In contrast to the concrete and tangible evidence of consumer harms that would result from the adoption of the Commission’s proposals, the putative benefits of the proposals are flimsy, do not withstand even cursory scrutiny, and are completely at odds with real-world facts and sound public policy.

- *Overbroad application of opt-in consent does not benefit consumers.* One of the fundamental misconceptions being perpetuated in this proceeding is the mistaken notion that expanding opt-in consent to more data and more uses will benefit consumers. The FTC, along with current and former FTC officials, all explain that not tying the level of choice to the sensitivity of the data actually goes against consumer expectations and would harm consumers. Moreover, consumers are perfectly capable of opting out of uses and sharing that they find objectionable, as they have done successfully for many years under the FTC’s privacy framework – and more likely than not the rule will harm consumers, who will be *less* informed about valuable products, innovative services, and lower-priced bundles. Claims that a default opt-in consent requirement will not have a significant effect ignore the substantial record evidence submitted by Comcast and others demonstrating the very low percentages of consumers that choose to participate regardless of the potential benefits.
- *Onerous privacy rules for ISPs will not improve broadband adoption.* Some commenters continue to push the theory that privacy rules for ISPs will somehow improve broadband adoption. This theory only makes sense if one ignores (1) substantial evidence from surveys by the Commission, Pew, NTIA, and others showing that privacy concerns are *not* a barrier to broadband adoption; (2) the fact that surveys raising privacy as a consumer concern speak in general terms about privacy on the Internet, not privacy concerns *specific to ISPs* (indeed, record evidence that Comcast and others submitted show that consumers trust ISPs *more* than non-ISPs); and (3) the real-world facts of how

consumers use the Internet and the tremendous success of the Internet under the Administration/FTC privacy regime.

- *ISPs are not unique, and the Commission's proposals will not advance consumer privacy.* The record affirms Professor Peter Swire's well-documented conclusions and Comcast's position that ISPs have neither a unique nor comprehensive view of consumer data. Numerous commenters, from ISPs and advertisers to public interest organizations, current and former government officials, academics, technologists, and others confirm that the openness of the Internet means that network operators do not have a monopoly on unique consumer information they arguably had in the legacy voice context. And unrebutted record evidence reinforces the fact that the amount of information to which ISPs have access is dwindling and is far less than many other participants in the Internet ecosystem. Accordingly, the Commission's proposed rules will not materially advance consumer privacy because the same data that the Commission proposes to regulate uniquely and overly-aggressively here will continue to be available to non-ISPs to use under the FTC privacy framework.

There is also no way to justify the proposed expansive and inflexible regime as a matter of law. The record includes substantial and thoughtful analyses demonstrating that the

Commission's proposal contravenes both the Communications Act and the U.S. Constitution:

- *The Commission's proposals would violate the First Amendment.* As Comcast and numerous other commenters – including noted constitutional scholar Laurence Tribe – explain, the Commission's proposals would violate ISPs' First Amendment commercial speech rights. Specifically, commenters show that the Commission's proposal would fail the *Central Hudson* intermediate scrutiny analysis (not to mention the content-based restriction analysis that was applied in similar circumstances in *Sorrell*). And the only two supporters of the Commission's rules to even acknowledge the constitutional issues fail to offer any arguments that would challenge, let alone refute, this conclusion.
- *Section 222 is not intended to cover ISPs.* As an initial matter, as Comcast and many other parties demonstrate, Congress never intended Section 222 to reach, let alone stifle the activities of, ISPs. The Commission's statement in the 1998 Universal Service Report to Congress that ISPs "generally do not provide telecommunications" and thus are not telecommunications providers required to contribute to the universal service fund reflected the widely-accepted view at the time – a view that was also reflected in language Congress chose for Section 222. That language highlights that Congress's intent and sole focus was to cover and restrict the privacy practices of *telephony providers*, which had access to unique, sensitive *voice*-related data – called CPNI – that Congress was interested in regulating and restricting. If Congress truly intended Section 222 to govern the privacy practices of ISPs, it would have used more expansive language to define the scope of information covered by Section 222 – but it clearly did not.
- *Section 222 focuses on CPNI.* Even assuming Section 222 does cover ISPs, the provision confines the Commission's authority in at least two important ways. First, the categories

of information to which it applies are carefully delimited. Specifically, Section 222 only covers a narrow set of carefully defined CPNI, not personally identifiable information (“PII”) generally or some undefined and unlimited category of “proprietary information.” And it certainly does not include IP addresses or de-identified information, as the courts have made clear. Second, it sets forth clearly what the Commission can – and, by extension, cannot – do. So, for example, the Commission cannot find in Section 222 authority to limit or otherwise prohibit arbitration clauses, or prohibit ISPs from developing different business models that may involve offering reduced prices in exchange for the ability to use or share a customer’s data.

- *Section 222 occupies the field of telecom carrier privacy regulation.* The record affirms that the regulations proposed by the Commission cannot be saved by Sections 201 or 705 of the Communications Act, or Section 706 of the Telecommunications Act of 1996. The Commission cannot avoid the clear canon of statutory construction that the specific governs the general, or the Commission’s clear precedent holding that, in enacting Section 222, Congress intended to occupy the field of privacy regulation for telecommunications carriers and therefore to preclude the use of other provisions to further expand the FCC’s jurisdiction over these issues. The Commission thus cannot circumvent the confines that Congress carefully and purposefully established in Section 222 by invoking any of these other provisions to adopt rules that are not otherwise permissible under Section 222. And were the Commission to nonetheless cite these or other provisions in an effort to justify more restrictive regulations against ISPs, doing so would also undermine its claim that it has no jurisdiction to regulate the privacy practices of edge providers or other non-ISPs, as some of these other provisions are not limited to telecommunications services.

Despite all the problems identified on the record with the Commission’s proposal, there is a clear path forward for the Commission to accomplish its goal of protecting consumer privacy without harming consumers, competition, or innovation. The technology-neutral privacy principles consistently espoused and embraced by the Obama Administration and the FTC receive nearly universal acclamation on the record. Members of Congress, the FTC, current and former FTC and Administration officials, ISPs, public interest groups, advertisers, academics, technology companies, small businesses, and others praise this approach and urge the Commission to more closely align itself with it. The Consensus Privacy Framework jointly proposed by Comcast and others across the Internet ecosystem continues to be the only approach put forward on the record that builds off the successful Administration/FTC approach to privacy

and gives the FCC the tools it needs to protect consumers' privacy and security on the Internet while allowing innovation, competition, and investment to continue to flourish.

* * *

In sum, the record built in response to the Commission's NPRM provides strong evidence that the Commission's initial proposal is unnecessarily inflexible and should not be adopted.

Instead, the Commission should:

- *Adopt the Consensus Privacy Framework.* The record confirms that the FCC should closely align its approach with the well-established and highly successful Administration and FTC privacy principles, and the only proposal on the record to do that is the Consensus Privacy Framework. Adopting this Framework would protect consumers while promoting continued competition, innovation, and investment in the vibrant Internet ecosystem.
- *Limit the Scope of Any Rules to CPNI.* Any rules the Commission may adopt must be limited to the use and disclosure of CPNI collected by the ISP. Numerous commenters explained how adopting rules that apply to categories of information other than CPNI, trying to broaden the scope of CPNI to include information like IP addresses, device identifiers, and port information, or expanding the rules to cover information acquired from third-parties or collected by non-ISP affiliates would be contrary to precedent and inconsistent with the plain language and intent of the statute.
- *Limit Opt-In Consent to Sensitive Data.* As the FTC confirms in its comments, there is no benefit to be had from a broad opt-in mandate, but there would be substantial harms to consumers, competition, and innovation. 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. As the FTC and many other commenters convincingly argue, 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.* The record is devoid of any rational policy or legal basis on which the Commission could justify imposing an opt-in consent requirement on the use or disclosure of CPNI (or any other data) that does not identify an individual ("de-identified information"). Also, as the FTC's comments make clear, (1) any de-identification standard must build in an appropriate level of flexibility to enable companies to *reasonably* de-identify the data, and (2) information should be able to qualify as de-identified *regardless* of whether it is aggregated.
- *Clarify Use of Vendors/Service Providers.* The record highlights the ways in which ISPs – like all other companies in the Internet ecosystem – need to be able to share CPNI (and other data) with their agents/vendors to accomplish many tasks. The Commission should

be clear that any rules it adopts do not prevent ISPs from providing CPNI to an agent/vendor based on implied consent, provided the ISP has an agreement with the agent/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 agent/vendor's own purposes.

- *Permit Use of Lower Pricing and Other Benefits in Exchange for Consent to Use CPNI.* Numerous commenters explain the ways in which using innovative business models and pricing strategies would affirmatively benefit consumers. As a wide range of commenters, including FTC Commissioner Maureen Ohlhausen, persuasively argue, the Commission should allow ISPs to offer their customers lower prices or other benefits in exchange for customer permission to use or disclose data for marketing purposes, so long as the terms of such offers are clear.
- *Adopt Sensible Data Breach Rules.* A number of commenters, including the FTC, highlight the problems with the FCC's proposed approach to data breach notifications. Consistent with the data breach rules applicable in almost every other setting, any breach notification rule the Commission adopts should (1) apply only to breaches of sensitive personal information; (2) incorporate reasonable exceptions that are commonplace in other breach rules (such as for use of encryption, likelihood of consumer harm, inadvertent disclosures, etc.); and (3) allow at least 30-60 days after discovery of the breach to send the notification as recommended by the FTC and others.
- *Refrain from Restrictions on Arbitration Clauses.* The record confirms that there is no sound legal or policy basis to restrict the use of arbitration clauses. Congress clearly authorized such clauses in the Federal Arbitration Act, and the Supreme Court and many other courts have consistently upheld them. Commenters explain that 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.* There is no support on the record for expanding the broadband CPNI rules to cover cable services. Congress purposefully created separate privacy statutes for cable services and telecommunications services, and the Commission is not at liberty to ignore the clear language of the Act.

II. THE RECORD OVERWHELMINGLY DEMONSTRATES THAT THE COMMISSION'S PROPOSALS WOULD BE AFFIRMATIVELY HARMFUL TO CONSUMERS AND UNDERMINE IMPORTANT PUBLIC POLICY GOALS, WITHOUT ANY BENEFIT OR JUSTIFICATION.

Despite the widespread support for aligning closely with the Administration and FTC approach to privacy, and the statements of praise in the NPRM itself for the Administration and FTC approach, "nearly every proposal in the NPRM is inconsistent and potentially in conflict

with the FTC’s current effective approach to protecting and enforcing consumer privacy.”⁵ As a result, “the Commission’s proposed rules would affirmatively harm consumers and undermine other important policy objectives.”⁶ The harms would be manifold and, as discussed below, were specifically and concretely identified by commenters in ways that the Commission cannot ignore. In contrast, the purported benefits of and asserted justifications for the Commission’s proposal set forth by supporters thereof are flimsy, unsubstantiated, and generally unable to stand up to marketplace facts or record evidence. The net result of this analysis is that the Commission’s proposal will not materially advance consumer privacy, will harm the public interest in numerous ways, and should not be adopted.

A. Commenters Broadly Demonstrate the Numerous Consumer and Other Harms that Would Result from the Commission’s Proposals.

If adopted, the Commission’s proposal would affirmatively harm consumers and undermine important public policy priorities. Specifically, numerous commenters highlight how the proposed rules will (1) confuse consumers by having different privacy regimes apply to the same data used for the same purposes solely based on the type of entity that collects that data; (2) deprive consumers of necessary information about innovative products and services, and bundled discounts from which they have benefited for many years; (3) desensitize consumers to real data security breaches that could harm them because they will likely develop warning fatigue from the over-notification of harmless “breaches” the proposal would require; (4) prevent consumers from receiving lower prices or other benefits in exchange for their consent to use their data; (5)

⁵ Mobile Future Comments at 2; *see also* Consumers’ Research Comments at 13 (explaining that the FCC’s proposal is contrary to the Administration’s guidance “to avoid ‘inconsistent standards for related technologies’”).

⁶ Comcast Comments at 42.

stifle competition, dampen broadband investment, and hamper network security efforts; and (6) harm network security and hamper ISPs' ability to efficiently work with trusted third parties.

1. Consumers will be confused by a regime that treats the *same* data used for the *same* purposes differently based solely on the entity that holds it.

Consumers have spoken with a clear voice – they want a single, cohesive privacy regime on the Internet:

By an overwhelming margin, 94% v. 5%, [I]nternet users agree that “All companies collecting data online should follow the same consumer privacy rules so that consumers can be assured that their personal data is protected regardless of the company that collects or uses it,” including 82% of Internet users who say they “strongly” agree with that statement.⁷

The only real response proffered by supporters of the Commission's rules – that the Commission does not have authority over non-ISPs – is irrelevant. That the Commission may not have authority to regulate the entire Internet is not a reason to overregulate one part of the Internet. Former FTC Chair Jon Leibowitz recommends that, “[b]ecause the FCC is not in a position to dictate privacy rules for the entire Internet ecosystem, it should strive to harmonize its proposed rules with the FTC approach and other U.S. privacy laws, and carefully consider the consequences of failing to do so.”⁸

There can be little doubt as to why consumers would prefer a single privacy regime across the entire Internet: “Consumers do not expect their basic privacy protections to vary based on the identity of the entity they are interacting with at any particular time.”⁹ The FTC explains that its privacy regime is based on the sensitivity of the data, rather than the type of

⁷ Progressive Policy Institute Comments at 1; *see also* Verizon Comments at 6 (“Given the myriad entities that have access to consumer data as it travels across the Internet, consumers have a strong interest in having a *uniform* privacy regime apply to each company with access to their data.”) (emphasis in original).

⁸ Jon Leibowitz Comments at 7.

⁹ National Cable & Telecommunications Association (“NCTA”) Comments at 5.

entity that holds it: “[T]he more sensitive the data, the more consumers expect it to be protected and the less they expect it to be used and shared without their consent.”¹⁰ MMTC concludes that “consistency is critical to the effectiveness of the Commission’s efforts to serve its transparency goal, and consumers should not be expected to parse the distinctions the Commission proposes to make.”¹¹

Many commenters echo Comcast’s concern that consumers will become confused and frustrated when their information is used for purposes they thought they declined in one context or when they fail to receive information about services they are interested in without having to take additional steps in another. For example, as Future of Privacy Forum notes:

With the average person visiting ninety-six or more separate domains per month, and an exponential increase in third party data sharing, it is unreasonable to expect consumers to differentiate between the privacy practices of different platforms and publishers in the Internet ecosystem.¹²

Likewise, AT&T explains that consumers would be surprised that “AT&T must obtain opt-in consent” to use certain customer information, while “Google need follow no such requirement in arranging for the Android operating system to transmit all of the same information (and more) back to Google’s centralized servers for the same types of uses.”¹³ This highlights one of the key

¹⁰ FTC Comments at 21.

¹¹ MMTC Comments at 6.

¹² Future of Privacy Forum Comments at 28; *see also* International Center for Law & Economics (“ICLE”) Comments at 18 (“Consumers are unlikely to know that different regulatory regimes apply to ISPs and edge providers. . . . [And] may then blame ISPs for things like targeted advertising due to edge services collecting information on them.”).

¹³ AT&T Comments at 57; *see also* T-Mobile Comments at 8-9 (“Thus, rather than meeting consumers’ expectations, the proposal would cause substantial consumer confusion.”); Competitive Carriers Association Comments at 4 (“Different frameworks applicable to similar providers will result in substantial consumer confusion where consumers often don’t distinguish between the two.”); ICLE Comments at 16 (explaining that the NPRM will “create consumer confusion regarding privacy owing to the disparate treatment of edge providers and ISPs”).

problems with having dual privacy regimes – as identified by the FTC – and is a critical harm that is inherent to the Commission’s proposed approach.

On the other hand, none of the commenters that support the Commission’s proposal address the point that inconsistent privacy regimes for ISPs and non-ISPs will cause consumer frustration and confusion. If anything, some of these proponents highlight that the new rules will cause additional confusion. For example, Consumer Watchdog recognizes that consumers feel confused, discouraged, and impatient when trying to make decisions about sharing their personal information with companies, and that this situation would only be exacerbated by dual privacy regimes in the online ecosystem.¹⁴ As Electronic Privacy Information Center (“EPIC”) highlights, “it is obvious that the more substantial privacy threats for consumers are not the ISPs,” and failing to treat all parties on the Internet the same will only serve to confuse consumers.¹⁵

Moreover, commenters confirm Comcast’s initial conclusion that requiring notice and consent at *multiple points* throughout a customer’s online experience would exacerbate the consumer confusion problems already inherent in the Commission’s proposal.¹⁶ Generally, the FTC and the Administration have supported an approach that uses a “just-in-time” notice and choice mechanism at the time of sign up, and then relies on additional disclosures only when

¹⁴ Consumer Watchdog Comments at 3.

¹⁵ EPIC Comments at 16.

¹⁶ See T-Mobile Comments at 39 (explaining that the proposed transparency obligations, including multiple “just-in-time” notices, would “cause ‘notice fatigue’ and consumer confusion” and would reduce “consumers’ awareness of relevant privacy practices”); USTelecom Comments at 12 (explaining that “just-in-time” notice and choice would be extremely burdensome for consumers and would lead to notice fatigue); Deepfield Networks Comments at 4-5 (explaining that a complex “just-in-time” opt-out or opt-in regime could severely slow network services and traffic flow and disrupt service); INCOMPAS Comments at 9-10 (explaining that potentially frequent notice and choice would contribute to “notice fatigue” and reduce the effectiveness of notices).

companies materially change the way they use data.¹⁷ The FTC’s comments reaffirm this approach, noting that by “informing consumers at an appropriate *moment in time*, a disclosure is likely to be of greater relevance to them.”¹⁸ Moreover the FTC comments suggest that for ISPs the most relevant moment to present consumers with a just-in-time notice and choice is “upon sign up” because that is when their consumers are most likely to be considering material terms.¹⁹ The Commission should adopt the FTC’s recommendation and refrain from adopting any requirement that ISPs notify and receive consent from consumers at multiple “just-in-time” points.

2. Consumers will be less-informed and less able to take advantage of innovative services and discounted offerings that they have consistently received marketing for and benefited from for many years.

Consumers benefit from having information about competitive alternatives, lower-priced offerings and discounts, and innovative products and services.²⁰ But the record includes

¹⁷ See *Protecting Consumer Privacy in an Era of Rapid Change*, FTC Report, Federal Trade Commission, at 48-50 (Mar. 2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> (“2012 FTC Privacy Report”); *Mobile Privacy Disclosures: Building Trust Through Transparency*, FTC Staff Report, Federal Trade Commission, at ii (February 2013), <https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf>; *Internet of Things: Privacy & Security in a Connected World*, FTC Staff Report, Federal Trade Commission, at vi (Jan. 2015), <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>; 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 11 (Feb. 2012), www.whitehouse.gov/sites/default/files/privacy-final.pdf (“2012 White House Consumer Privacy Bill of Rights Report”); Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015, at 7 <https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf>.

¹⁸ FTC Comments at 24 (emphasis added).

¹⁹ FTC Comments at 24-25.

²⁰ See, e.g., Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, White House Report, at 40-41 (May 2014), https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (“2014 White House Big Data Report”) (explaining that online advertising in particular has been a “vital driver of the growth of the Internet” and that “[c]onsumer are reaping the benefits of a robust digital ecosystem that offers a broad array of free content, products, and services. . . . As a result, consumers are getting better, more useful ads from – and access to – a wider range of businesses, in a marketplace that is ultimately more competitive and innovative.”); see also Direct

numerous examples of ways in which consumers will be deprived of information about these offerings that they have routinely received and benefited from for many years. Consumers need to know about these competitive alternatives to take advantage of them. And arguments from parties like Center for Democracy & Technology (“CDT”) that the proposed rules will not restrict marketing are completely at odds with the marketplace, record evidence about how consumers respond to opt-in, and basic economics.²¹

Commenters like Earth Networks (d/b/a “WeatherBug”) explain how difficult it would be to reach consumers if it could not leverage the ISP platform because of the significant limitations imposed by the Commission’s proposed rules. For example, WeatherBug describes how an opt-in restriction would thwart its efforts to reach consumers with information about beneficial energy efficiency products, and urges the Commission to ensure that its privacy regime does “not unfairly prevent or discourage individual customers from learning about the options available to privately benefit from participation in such offerings, or to contribute to the broader benefits they promise for society.”²² Similarly, the International Center for Law & Economics (“ICLE”) cautions that the Commission’s proposed approach “essentially destroys the ability of providers to market potential add-on or complementary services which, in combination, may provide efficiencies that justify lowering costs to the consumer.”²³ This is consistent with the cautionary advice provided by the FTC, which notes that adoption of the FCC’s proposed rules “could

Marketing Association (“DMA”) Comments at 4 (“The innovative and responsible use of data for advertising and marketing has been the economic backbone to the unprecedented benefit to consumers resulting from the Internet.”).

²¹ Specifically, CDT claims that the Commission’s approach “would still afford [ISPs] and their affiliates considerable latitude to use customer PI to market their other commonly-offered services to customers.” CDT Comments at 27; *see also* Mozilla Comments at 5 (arguing that ISPs should be able to use customer data in new revenue streams but that the FCC’s proposed framework is nonetheless appropriate).

²² Earth Networks Comments at 6.

²³ ICLE Comments at 18.

hamper beneficial uses of data that consumers may prefer.”²⁴ In other words, consumers would miss out on these great opportunities because they would never learn about them.

Similarly, numerous commenters explain that the Commission’s proposed rules would make it more difficult for ISPs to offer lower-priced bundles of services, including services that do not fall within the traditional “triple play” bundle of voice, video, and broadband. For example, the Consumer Technology Association (“CTA”) explains that the proposed rules will create uncertainty over whether ISPs may bundle their non-communications-related and communications-related services together and that “this uncertainty [will] hurt ISPs’ ability to market new services and offerings, [and] will impede potential partnerships between ISPs and other Internet ecosystem players to bundle and market products and services that could offer value to consumers.”²⁵ T-Mobile explains that the communications-related services distinction “simply is not consistent with consumers’ expectations – fostered by the existing CPNI rules – that a company providing one set of services will be able to offer discounted bundles involving other offerings.”²⁶ Importantly, the Commission’s proposed interpretation of the communications-related service category would have the effect of significantly expanding the applicability of the opt-in requirement, to the point where the Commission’s proposal is

²⁴ FTC Comments at 22.

²⁵ CTA Comments at 8-9; *see also* CTIA Comments at 127 (“Indeed, restricting companies from expanding to offer new lines or from achieving efficiencies through innovative bundling of products and services would run counter to the principles that underlie the American economy.”).

²⁶ T-Mobile Comments at 9.

indistinguishable from the broad opt-in requirement that was adopted in the 1998 CPNI Order²⁷ and subsequently overturned by the Tenth Circuit in *U.S. West*.²⁸

3. The proposed data breach rules will subject consumers to over-notification and warning fatigue.

The record contains widespread agreement that the Commission’s proposed data breach notification regime will do more harm than good. There are three specific problems with which many commenters agree: it covers too much information, it does not use a harm threshold or include exceptions for inadvertent but harmless disclosures, and the notification deadline is unreasonably short.

As to scope, the State Privacy & Security Coalition concludes that “the NPRM proposal is broader than existing information security and breach notice requirements in that it would apply to a large range of information that is not sensitive, including even data that is publicly available or that travels widely around the Internet when users communicate.”²⁹ The FTC recognizes that the broad scope of the FCC’s approach could lead to even more data being gathered about consumers:

[B]ecause the definition includes unauthorized access to any customer proprietary information, companies that only collect data such as device identifiers or information held in cookies may be required to collect other consumer information such as email addresses in order to provide consumers with breach notification. For example, this could effectively prohibit BIAS providers, from maintaining only anonymous browsing

²⁷ *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 (1998) (“1998 CPNI Order”).

²⁸ See *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999).

²⁹ State Privacy & Security Coalition Comments at 2; see also DMA Comments at 16 (“The Commission’s expansive definition of PII could trigger breach notification obligations for types of data that have not been captured under state and other federal regulatory regimes that have evaluated the types of information that warrant breach notification.”); Marketing Research Association Comments at 5 (“State and federal law ordinarily focuses on data which, when breached, could be subject to criminal abuse, like social security numbers and financial account information.”).

information, and instead, require them to link browsing with account information, so that they could notify customers of a breach involving any kind of persistent identifier.³⁰

To address this issue, the FTC urges the FCC to “apply [the breach notification requirement] to a narrower subset of personal information than customer proprietary information and not include device identifiers, cookies, or other persistent identifiers standing alone.”³¹ Comcast agrees with this recommendation.

As to the question of reasonable exceptions or a harm threshold, the FTC again highlights the problem with a simple rhetorical question: “If, for example, a company’s employee were to inadvertently access a document, but not read it, should a consumer receive a notice?”³² The concern is that lack of a harm threshold or reasonable exceptions would lead to over-notification of consumers.³³ Consumers that receive breach notifications for incidents where there is no likelihood of harm are more likely than not to succumb to warning fatigue – a perfectly natural response to hearing many warnings about potential harms that do not come to fruition.³⁴ Again, the FTC recommends a reasonable solution: “[Include] an exception to the notification

³⁰ FTC Comments at 31; *see also* Leibowitz Comments at 10-11 (explaining that the proposed data security provisions “should be more narrowly tailored to customer information that carries a risk of harm to the customer in the event of a breach, and in no case should apply to simple IP addresses, MAC addresses, or individually de-identified or aggregate data”).

³¹ FTC Comments at 32.

³² *Id.* at 31.

³³ *See, e.g.*, CTIA Comments at 176 (“The Commission should require notification only if a breach causes harm or is likely to cause harm. Notifying customers of a data breach when no harm has occurred will not protect consumers. On the contrary, it will cause confusion and, through over-notification, will lead consumers to disregard notices even when harm has occurred.”); CenturyLink Comments at 42 (“A harm element is particularly important given the exhaustive scope of information to which the proposed rules, if adopted, would apply.”); State Privacy and Security Coalition Comments at 13 (“[A] core principle of information security law and best practices is to distinguish between circumstances in which there is a risk of harm from unauthorized acquisition of data and circumstances where there is not.”).

³⁴ *See* CenturyLink Comments at 39-41; Marketing Research Association Comments at 5.

requirement for certain inadvertent, good-faith actions by company employees that would otherwise meet the definition of ‘breach.’”³⁵

Commenters like New America’s Open Technology Institute (“OTI”) seem to believe that consumers will read each new notification and give it proper consideration before deciding for themselves whether there is a likelihood of harm.³⁶ This idyllic portrait of a consumer taking control of her own digital life is completely at odds with real-world experience about how consumers react to receiving numerous notifications. As CTIA explains, “consumers are not served by expansive, untimely, and repetitious privacy notices” and “providing customers with frequent notices results in customer annoyance and may even deter customers from visiting certain websites.”³⁷ OTI’s ignorance – willful or otherwise – of consumer behavior in these situations discredits its comments on this issue.

Finally, as numerous commenters note, the proposed deadline for providing breach notifications is unreasonably short and likely to contribute to the over-notification problem.³⁸ The FTC agrees, explaining that the short time period proposed by the FCC would “not allow companies sufficient time to conduct an investigation. This could have a detrimental effect on

³⁵ FTC Comments at 32.

³⁶ OTI Comments at 24, 33-34, 39.

³⁷ CTIA Comments at 99-100; American Cable Association Comments at 9 (“[B]ased on numerous interviews with ACA members, it appears the most common complaint from customers about privacy and data security is that the existing rules – which require consumers to receive, read, and respond to multiple notices and approval forms based on each service – are too confusing and burdensome . . .”).

³⁸ *See, e.g.*, Technology Policy Institute (“TPI”) Comments at 28 (“A 10-day notification period for any breach regardless of severity seems to risk creating the ‘notification fatigue’ that concerns the FCC.”); CenturyLink Comments at 43 (explaining that “premature notification can result in the provision of inaccurate and incomplete information regarding the scope of the breach and any potential harm to consumers.”); CTIA Comments at 179-82 (explaining that the timelines for notification “will result in less effective breach responses, customer confusion, and unnecessary costs”); State Privacy and Security Coalition Comments at 13-15 (explaining that short 7- and 10-day breach notice deadlines will lead to over-notification and incomplete and inaccurate notice).

consumers, who could get erroneous information about breaches.”³⁹ Consistent with Comcast and numerous others on the record, the FTC “suggests that companies be required to provide breach notice without unreasonable delay, but not later than an outer limit of between 30 and 60 days.”⁴⁰

4. The proposed rules will prevent consumers from receiving lower prices or other offers of value in exchange for the use of their data.

The primary argument made by those who would prohibit ISPs from offering lower-priced or more expansive services in exchange for use of consumer data is that it would turn privacy into a luxury for only the well-to-do.⁴¹ This concern for minority communities, the underprivileged, vulnerable individuals, etc. would be more commendable if it were not completely at odds with how the Internet works or willfully ignorant of the benefits that could accrue to consumers from the use of such practices. Indeed, as MMTC states, “[c]onsumers –

³⁹ FTC Comments at 32-33; *see also* T-Mobile Comments at 53 (“Breach responses and investigations take time and tremendous resources.”); ITI Comments at 12 (“Recognizing the sophistication of today’s hackers and the challenging nature of a post-data breach forensic investigation, a breach notification regime must provide realistic, flexible, and workable time requirements.”); Leibowitz Comments at 12 (explaining that there “may also be practical limitations as to how quickly an investigation can be completed, individuals can be identified, and required notifications can be prepared and sent”).

⁴⁰ FTC Comments at 33; *see also* Association of National Advertisers Comments at 30 (“[A]ny time period less than a 30-day time frame is clearly unreasonable, though in complicated breach scenarios, even that time period might be insufficient.”); Hughes Network System Comments at 7 (“[A] more equitable solution would be to stipulate that broadband service providers must report a breach within 30 days from the discovery of that breach, with leave to extend the reporting period by 30 day increments if the broadband service provider can demonstrate that more time is needed to determine the scope of the breach, to conduct risk assessments, and to restore reasonable integrity to the network.”).

⁴¹ Free Press Comments at 19 (“Financial inducement schemes could render privacy (a right guaranteed to customers by statute) a luxury for the rich.”); Consumer Watchdog Comments at 6 (“Pay-for-privacy schemes are most likely to have a negative impact on minority communities, low-income neighborhoods and the elderly. If widely adopted, they would create a two-tiered system, in which only the wealthy will be able to protect their privacy.”); Privacy Rights Clearinghouse Comments at 6 (“PRC is fundamentally opposed to and concerned about the potential effects of pay-for-privacy scenarios on all consumers and particularly vulnerable populations. Under no circumstances should any consumer, especially those who are members of vulnerable communities, have to choose between their rights to privacy and foregoing broadband service.”).

especially low-income consumers – could *benefit* from discounts or other ‘financial inducements’ offered by ISPs.”⁴²

The business model which these parties excoriate is the same business model used throughout almost all of the rest of the Internet.

- Search engines allow consumers to search for free because the search engine collects information about the searches and sells that information to advertisers.⁴³
- Some webmail providers offer email services for free in exchange for the ability to scan consumer emails for information and sell that information – and the access they have to consumers – to advertisers.⁴⁴
- Social media sites offer a free platform for consumers to connect with friends and family in exchange for gathering information about users and selling that information to advertisers.⁴⁵

Consumers can choose to use services that do not use their data in the same way as the free services – for example, paying for Yahoo! Mail allows the consumer to use it without seeing any advertisements.⁴⁶ But there is nothing about any of this that creates a two-tiered privacy system on the Internet.

It is highly ironic that, in the same proceeding where supporters of the Commission’s proposed rules take the position that individuals should have more control over how their data gets used, some parties argue that consumers should not have *this* choice. Public Knowledge

⁴² MMTC Comments at 8 (emphasis added).

⁴³ 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 51-57 (Feb. 29, 2016), <http://peterswire.net/wp-content/uploads/Online-Privacy-and-ISPs.pdf> (“Swire Paper”).

⁴⁴ *Id.* at 59-64.

⁴⁵ *Id.* at 43-49.

⁴⁶ YAHOO! HELP, *Sign up for Yahoo Ad Free Mail*, <https://help.yahoo.com/kb/sln15967.html> (last visited July 5, 2016). Importantly, the market supports several different business models for email services so that consumers who do not want a particular offer will have other choices – as they would for ISPs.

exemplifies this, stating first that “[i]f the consumer wants to sell or trade away her information in a value exchange for targeted goods and services, she should have that right,”⁴⁷ before pronouncing itself “deeply concerned” with allowing consumers to make this particular choice.⁴⁸ In other words, these parties appear to approve of allowing a consumer to “trade away her information” for free, but do not wish to give consumers the opportunity to do so in exchange for a lower price or some other financial benefit.

A wide range of commenters highlight the problems with banning these discounted offerings, both in terms of a loss of consumer welfare and in terms of hampering ISPs’ ability to address the broadband adoption gap:

- “A ban on discounts for ad-supported BIAS *prohibits a consumer from trading some of her data for a price discount*, even if the consumer is fully informed.”⁴⁹
- “Banning arrangements in which consumers opt to pay for equivalent services rather than provide personal information amounts to an onerous form of price control that reduces consumer welfare. A ban would enshrine in regulation the mistaken assumption that consumers are not competent to decide what form of payment – whether in personal information or money – that they are willing to make for services.”⁵⁰
- “Such inducements serve to significantly drive online usage and, in some cases, ISPs also use inducements and marketing to help financially challenged consumers by offering bundled services and extended payments.”⁵¹
- “Would-be broadband subscribers cite high cost as more important than privacy concerns for the reason why they have not adopted broadband. Given that fact, such a ban may prohibit ad-supported broadband services and thereby eliminate a way to increase broadband adoption.”⁵²

⁴⁷ Public Knowledge et al. Comments at 27.

⁴⁸ *Id.* at 32.

⁴⁹ Ohlhausen Comments at 3 (emphasis added).

⁵⁰ Free State Foundation Comments at 9.

⁵¹ MMTC Comments at 8.

⁵² Ohlhausen Comments at 3 (internal citations omitted).

The potential benefits to broadband adoption are particularly apparent. The Commission’s recently-adopted revisions to the Lifeline program acknowledge the role that price plays in the decision to adopt,⁵³ and parties like Free Press and Public Knowledge who, in this proceeding, would prevent ISPs from offering lower-priced services, have used other proceedings and venues to complain that high prices are keeping lower-income households from adopting broadband.⁵⁴ Instead of facilitating broadband adoption, however, a ban on such offerings would make it harder for ISPs to offer lower-priced options. In other words, consumers would lose.

5. The proposed rules will harm innovation, broadband investment, and competition.

In addition to directly harming consumers, the Commission’s proposals would be detrimental to important public policy objectives. As ICLE recognizes, “the rules contemplate disparate regulatory treatment that would likely harm competition and innovation without evident corresponding benefit to consumers.”⁵⁵ Supporters of the Commission’s proposal have no answer for this, and some, such as Public Knowledge, even seem to believe that it is a benefit of the Commission’s proposal. This is a concession that the Commission’s proposals flip the

⁵³ *Lifeline and Link Up Reform and Modernization, Telecommunications Carriers Eligible for Universal Service Support, Connect America Fund, Second Further Notice of Proposed Rulemaking, Order on Reconsideration, Second Report and Order, and Memorandum Opinion and Order*, 30 FCC Rcd. 7818, ¶ 7 (2015).

⁵⁴ *Compare, e.g.*, Free Press Comments at 19-20 with Letter from Free Press et al. to Chairman Tom Wheeler, FCC, MB Docket No. 15-149, at 2 (filed Mar. 21, 2016) (opposing the merger of Charter, Time Warner Cable, and Bright House) (“As a recent Pew Research Center report found, broadband adoption rates are dropping, particularly for low-income households and communities of color. *The main reason for this decline is high prices that force people in marginalized communities to choose between paying for broadband and other necessities.*” (emphasis added)).

⁵⁵ ICLE Comments at 2; *see also* NCTA Comments at 57 (“The proposed rules also will harm consumer welfare by engendering reductions in investment, innovation and competition due to the significant disparities in privacy and data use burdens for ISPs compared to everyone else in the ecosystem.”); CTIA Comments at 3 (“The proposed rules will harm competition in the digital advertising market, by placing ISPs, who are new entrants to this market, at a competitive disadvantage.”).

traditional goals of regulation on their head by regulating to prevent new competition, rather than to encourage it.

The U.S. Chamber of Commerce highlights the fundamental problem with the Commission's proposals when it notes that the proposed rule "creates regulatory imbalance" between ISPs and non-ISPs, in which non-ISPs will continue to be able to innovate and compete "under the light-touch regulatory framework of the FTC" while ISPs will be subject to highly restrictive, inflexible, and prescriptive regulations.⁵⁶ In contrast, the Administration and FTC approach to privacy is explicitly technology-neutral, even when it comes to ISPs:

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

The disparate treatment of ISPs that would result from the Commission's proposal is likely to distort competition, and, in the process, stifle innovation and investment in broadband.⁵⁸

The record includes numerous commenters who confirm that the Commission's proposal will harm competition in the online advertising space, as well as other markets where start-ups and other small companies need to be able to leverage ISP footprints to compete against entrenched incumbents to offer innovative services to consumers. National Cable & Telecommunication Association ("NCTA") explains, "[t]ying the hands of ISPs will eliminate one of the most plausible sources of competition for large digital advertisers, and thereby inhibit

⁵⁶ U.S. Chamber of Commerce Comments at 5; *see also* NCTA Comments at 1-2 (explaining that the "Commission has proposed an asymmetric privacy framework that unlawfully and unfairly singles out ISPs for burdensome treatment" and that this regulatory imbalance will stifle innovation); LocationSmart Comments at 4 ("[A]dding greater confusion through disparate regulatory requirements will stifle innovation, slow adoption of new services and limit consumers' access to and enjoyment of those services.").

⁵⁷ *2012 FTC Privacy Report* at 56 (emphasis added).

⁵⁸ *See* Information Accountability Foundation Comments at 4 (explaining that the proposed rules would result "in lost innovation and higher costs on individuals, business, and society as a whole").

the emergence of competition that could lower costs for consumers.”⁵⁹ USTelecom notes that “the reality is that BIAS providers are small players in the advertising market and that their expansion in that market would increase competition and innovation.”⁶⁰ Professor Tribe points out that, “[b]y essentially blocking ISP entry into the online advertising market by singling out new entrants in the online advertising market for heightened standards that do not apply to the established market leaders, the FCC’s proposal is anti-competitive, anti-consumer, and anti-First Amendment.”⁶¹

The record also confirms that the proposed rules will dampen investment in broadband networks.⁶² CenturyLink explains that the Commission’s proposals “would inhibit providers’ ability to offer services in the way their customers demand, and to find new ways to generate revenue, which in turn would reduce investment incentives.”⁶³ Former FTC Commissioner Joshua Wright includes an even more dire warning: “Because the NPRM eliminates important avenues for ISPs to earn revenues and increases ISPs’ costs of communicating with their customers, broadband prices will invariably rise.”⁶⁴ The National Association of Manufacturers similarly comments that the Commission’s proposal “will take away critical resources that would

⁵⁹ NCTA Comments at 58-59 (internal citations omitted).

⁶⁰ USTelecom Comments at 15.

⁶¹ Laurence H. Tribe & Jonathan S. Massey, *The Federal Communications Commission’s Proposed Broadband Privacy Rules Would Violate the First Amendment*, at 4 (May 27, 2016), attached to Letter from CTIA, NCTA, & USTelecom Association, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 (filed May 27, 2016) (“Tribe Comments”). Additionally, as noted above, the record includes examples of how small companies like WeatherBug that rely on partnerships with ISPs to get their products into the hands of consumers will have a harder time reaching customers. See *supra* § II.A.2.

⁶² Comcast Comments at 44-46.

⁶³ CenturyLink Comments at 4.

⁶⁴ Joshua D. Wright, *An Economic Analysis of the FCC’s Proposed Regulation of Broadband Privacy*, at 20 (May 27, 2016), attached to Letter from Jonathan Banks, SVP, Law & Policy, United States Telecom Association, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 (filed May 27, 2016) (“Wright Analysis”).

otherwise be applied to further investment in our nation’s broadband infrastructure on which manufacturers depend to fuel their innovation pipeline.”⁶⁵

Public Knowledge seems to argue that tying ISPs’ hands is actually a good thing, saying that “no ISP enjoys an unfettered right to abuse its market position in one line of business (broadband provision) to gain a competitive advantage in a separate line of business (predictive advertising).”⁶⁶ But the notion that an ISP abiding by the FTC’s framework for data collection and use is somehow an “abuse” of its market position strains credulity.⁶⁷ And the idea that it is contrary to consumer interests for an ISP to provide a competitive alternative in a different marketplace – particularly one as concentrated as the marketplace for online advertising⁶⁸ – is unhinged from basic economic theory and the widely accepted reality that competition in any marketplace inures to the ultimate benefit of consumers.⁶⁹

6. The proposed rules will harm network security and hamper ISPs’ ability to efficiently work with trusted third parties.

Finally, the record highlights how network security efforts will be significantly hampered if the Commission moves forward with its proposals. Supporters of the Commission’s proposals appear to suggest that even the limited flexibility offered in the proposed rules goes too far.⁷⁰

⁶⁵ National Association of Manufacturers Comments at 1.

⁶⁶ Public Knowledge et al. Comments at 3.

⁶⁷ As Comcast and others show in the initial comments, ISPs have been good stewards of their customers information, as proven by the very few enforcement actions that the FTC has taken against ISPs. *See, e.g.*, Comcast Comments at 6, 37-40; NCTA Comments at 50-52.

⁶⁸ Comcast Comments at 53-55; Advanced Communications Law & Policy Institute Comments at 16-17.

⁶⁹ *See generally* Council of Economic Advisors Issue Brief, *Benefits of Competition and Indicators of Market Power*, (Apr. 2016), https://www.whitehouse.gov/sites/default/files/page/files/20160414_cea_competition_issue_brief.pdf.

⁷⁰ *See, e.g.*, Center for Digital Democracy (“CDD”) Comments at 17-18 (“Opt-in for all services provides a fair foundation ensuring that consumers make the decision on what information can be used.”); OTI Comments at 39 (“The FCC should consider requiring opt-in for all data use, disclosure, and access practices other than those undertaken to provide service.”); EPIC Comments at 8 (“Internet-based services must obtain voluntary, specific, and

For example, Access Now expressly objects to and opposes “the use or disclosure of CPNI for cybersecurity purposes without specific protections for user privacy and security.”⁷¹ But numerous commenters with significant expertise and experience in network and cyber security – including the FTC,⁷² academics,⁷³ industry,⁷⁴ and others – explain how the Commission’s proposals would both contravene well-established U.S. cybersecurity policy and would make it harder for ISPs and other experts to work together to ensure the security, reliability, and integrity of the services being provided.

The Administration’s – and, until recently, the Commission’s – policy on cybersecurity has been focused on giving those entities on the “front lines” the tools, information, and flexibility necessary to implement appropriate security measures.⁷⁵ As USTelecom explains, these efforts represented “a bold move in cybersecurity that has produced a seismic shift in the way government and industry approach cybersecurity risk.”⁷⁶ And this approach is widely accepted as sound: “[S]pecifying many of the detailed requirements in the regulations will make it difficult for the BIAS providers to innovate or evolve their privacy protections, because such changes could necessitate petitions for rulemaking or waiver requests, neither of which get

informed opt-in consent from consumers for all collection, use, and disclosure of consumer data beyond what is necessary to accomplish the specific purpose for which that data was disclosed.”); Free Press Comments at 13 (“The Commission should modify its proposal accordingly and require opt-in approval for sharing or use outside the direct provision of broadband service – even within affiliated services.”).

⁷¹ Access Now Comments at 7.

⁷² FTC Comments at 27-30.

⁷³ See, e.g., William Lehr et al. Comments at 8-9.

⁷⁴ See e.g., AT&T Comments at 72-74; T-Mobile Comments at 47-49.

⁷⁵ See Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 19, 2013); Framework for Improving Critical Infrastructure Cybersecurity February 2014, at <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>; CSRIC IV WG4 Final Report, at https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

⁷⁶ USTelecom Comments at 21.

resolved expeditiously.”⁷⁷ Unfortunately, as the Interactive Advertising Bureau notes, “[t]he proposed data security requirements are *not consistent* with existing guidance from other governmental entities or with proposed legislation currently under consideration in Congress.”⁷⁸ Other commenters explain that the rules will cause ISPs to inefficiently allocate resources in this space, thus depleting valuable assets that could be used to address evolving security threats.⁷⁹ And the Internet Association concludes, “there is simply no need for the FCC to reinvent the privacy and security wheel for such services.”⁸⁰

Flexibility is a key component of the nation’s cybersecurity strategy, but the FCC’s proposals offer an inflexible set of security rules. In particular, the FTC highlights in its comments that the proposed rule text would actually create a strict liability standard for ISPs to ensure security.⁸¹ Moreover, former FTC Chairman Jon Leibowitz notes that the “prescriptive and static nature” of the FCC’s proposed security requirements is “at direct odds with the Administration’s Cybersecurity Framework, as implemented by NIST, which has been voluntarily adopted by a wide swath of the industry and reflects flexible and reasonable standards that accommodate changing threats.”⁸² Unsurprisingly, the FTC ultimately urges the FCC to adopt a more reasonable and flexible approach, consistent with Administration policy.⁸³

⁷⁷ ADTRAN Comments at 3-4.

⁷⁸ Interactive Advertising Bureau Comments at i (emphasis added); *see also* DMA Comments at 20; ITI Comments at 15-16; AT&T Comments at 79-80; USTelecom Comments at 21-25; MMTC Comments at 4-6.

⁷⁹ *See, e.g.*, AT&T Comments at 75 (“As an initial matter, extending the data security rules to cover this wide range of information would greatly exacerbate the costs imposed by the NPRM’s ‘data security framework.’”).

⁸⁰ Internet Association Comments at 7.

⁸¹ FTC Comments at 27-28.

⁸² Leibowitz Comments at 10-11.

⁸³ FTC Comments at 27-28.

Another critical component to our national cybersecurity strategy is information sharing.⁸⁴ Consistent with that, the record shows that ISPs work with trusted third parties to develop solutions to address ever-present abuses and security threats on the Internet.⁸⁵ But the Commission’s proposal threatens to undermine that work. For example, M³AAWG describes how IP addresses and other data elements like MAC IDs and domain information “are central to our work, even though they do not inherently or automatically identify any specific person” and cautions the Commission that its work “could be significantly curtailed, if not out-and-out banned” if the NPRM’s proposals applying overbroad and onerous opt-in consent requirements to the use of basic – and even public – information like IP addresses are adopted.⁸⁶ Multiple academics, engineers, and other researchers impress upon the Commission the high stakes involved in ensuring that information can be disclosed for cybersecurity purposes.⁸⁷ And a collective of experts in the field succinctly express the trade-off the Commission may be forcing: “Depriving researchers of this data, in favor of a ‘consent to protect’ interpretation of the Notice, will destroy the science of cyber public health in its early days.”⁸⁸ In its attempt to protect

⁸⁴ *See, e.g.*, Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. N, Title I (2015) (establishing procedures for sharing cyber threat information); Promoting Private Sector Cybersecurity Information Sharing, Exec. Order No. 13691, 80 Fed. Reg. 9349 (Feb. 20, 2015).

⁸⁵ Nick Feamster Comments at 1-2, 7 (explaining that the FCC’s proposal needs to add an exception for “vendors and protocol developers, who rely on access to real network test traffic to debug software and protocol implementations”).

⁸⁶ M³AAWG Comments at 2-4, 6; *see also* Return Path Comments at 3-4 (urging the FCC to drop its proposal to treat “IP addresses, domain names, and other generic transactional metadata” as CPNI and illustrating the harms to network security and abuse harms that can result if the use of such information is restricted).

⁸⁷ *See, e.g.*, Lehr et al. Comments at 2; Feamster Comments at 2-3; Manos Antonakakis et al. Comments at 4-6; *see also* Nominum Comments at 4 (“As an essential part of every IP network, DNS data offers valuable operational insights that benefit consumers and is an efficient and effective way for security researchers to identify cyber threats. It would be extremely difficult, costly, and/or highly intrusive to obtain similar data any other way.”).

⁸⁸ Antonakakis et al. Comments at 3-4; *see also* Nominum at 4 (urging the Commission to “ensure that its rules support use of DNS data to operate, secure, extend, and improve BIAS provider networks without customer consent”).

consumer privacy, the Commission must ensure that it does not remove the ability of ISPs and others to protect consumers from ever-evolving cyber-threats.

B. Purported Benefits and Justifications Cited by Supporters Do Not Stand Up to Marketplace Facts or Record Evidence.

In contrast to the concrete and tangible harms that would be visited on consumers, competition, innovation, investment, and network security if the Commission’s proposals were adopted, the purported benefits put forward by the supporters of the proposed rules are vague, illusory, and, ultimately, completely unable to withstand scrutiny in light of real-world facts and record evidence.

1. Overbroad opt-in consent does not benefit consumers.

One of the fundamental misconceptions being perpetuated in this proceeding is the baseless assertion that expanding opt-in consent to more data and more uses will benefit consumers. OTI is one of the primary purveyors of this fanciful theory: “Opt-in consent is the most important mechanism for ensuring customers give consent to a provider’s data practices.”⁸⁹ OTI also argues, without evidence, that an opt-in approach would be consistent with consumer expectations.⁹⁰ Some commenters assert further that opt-in is important because it shifts the burden from the consumer to the provider.⁹¹ But nowhere do these commenters – or any other

⁸⁹ OTI Comments at 36.

⁹⁰ *Id.* at 26.

⁹¹ EPIC Comments at 14-15 (“An opt-in standard would place the responsibility on the companies that ultimately benefit from the disclosure of private consumer information.”); *see also* Consumer Watchdog Comments at 6 (“Opt-out consent is insufficient. In fact, it is not really consent. Opting-out places the burden on consumers to take extra steps to avoid something that likely was not adequately explained to them.”). And Public Knowledge takes it one step further, arguing that the Commission should not allow opt-out even for communications-related services because of some conjured-up fear that ISPs will argue that all their services fall into the communications-related services category. Public Knowledge et al. Comments at 28-29 (explaining that incorporating the “total services” approach from the legacy CPNI rules would make the opt-out bucket too broad because of how “incumbent carriers have attempted to classify all types of services as ‘broadband,’ including services that the average consumer would not expect to be classified as broadband”). Public Knowledge’s objection is particularly absurd and unfounded. The communications-related services category as defined by the Commission’s proposal would only include Commission-regulated services. *See NPRM* ¶ 71; AT&T Comments at 41 (“Inexplicably, however, the NPRM

supporters of opt-in – show how such a broad opt-in regime actually benefits consumers or squares with marketplace facts in which implied and opt-out consent have applied to ISPs and all other entities for many years with much success and no significant consumer harm. Nor do they explain how consumers would benefit from a regulatory framework in which opt-in applies only to ISPs’ use of data to do things like provide relevant advertising and other customized offerings, while use by other online entities with access to the *very same customer data* used for *the very same purposes* is subject to opt-out consent.

The record shows that, far from benefiting consumers, shifting the burden to ISPs simply *increases costs for consumers* – both in terms of the opportunities for innovative services and lower-priced bundles that will be missed, and in terms of the amount of effort that consumers will need to make to even learn about those opportunities in the first place.⁹² As FTC Commissioner Ohlhausen notes, “[i]f a regulation imposes defaults that do not match consumer preferences, it imposes costs on consumers without improving consumer outcomes. The burdens imposed by a broad opt-in requirement may also have negative effects on innovation and growth.”⁹³ And the notion that a sweeping opt-in approach is consistent with consumer

proposes not only to retain the limiting category of ‘communications-related services’ but to narrow it further—and thus enlarge the scope even of first-party advertising that is subject to the opt-in requirements.”). As Comcast and others explain, this approach would significantly narrow the scope of this category of service, to the point where “ISPs might be subject to opt-in consent requirements whenever they wish to use their customers’ names and email addresses simply to market their own branded home-alarm system, their own branded mobile applications, a newly introduced smartphone offered in conjunction with their wireless plans, and perhaps even their branded over-the-top VoIP or video-streaming services.” AT&T Comments at 41-42; *see also* Comcast Comments at 47 n.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.”). Moreover, after years of fighting to expand the scope of the Commission’s regulatory authority, one would think that Public Knowledge would welcome the notion that this would create an incentive for service providers to bring their services within the scope of the Commission’s regulatory purview.

⁹² *See, e.g.*, Wright Analysis at 20-26.

⁹³ Ohlhausen Comments at 3.

expectation is completely unfounded. As the FTC remarks, the FCC’s default opt-in “approach does not reflect the different expectations and concerns that consumers have for sensitive and non-sensitive data.”⁹⁴

As a number of commenters note, both the Administration and the FTC already have analyzed what kind of consent regime is best to meet the dual goals of protecting consumers and facilitating innovation and competition.⁹⁵ In both cases, the conclusion was overwhelmingly in favor of a broad opt-out and implied consent regime, with only minimal opt-in for the use of particularly sensitive information. For example, the 2012 White House Consumer Privacy Bill of Rights Report said that:

[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.⁹⁶

Likewise, the FTC in its *2012 Privacy Report* 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,⁹⁷

⁹⁴ FTC Comments at 22; *see also* Letter from Christopher N. Olsen, Counsel to Ghostery, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 16 (filed Apr. 29, 2016) (“An Opt-In solution is not the best way to provide informed consent and level the playing field in a competitive online advertising marketplace.”); Verizon Comments at 66 (explaining that the FCC proposal will “harm consumers by creating a one-size-fits-none approach that will impose strict requirements on non-sensitive data that has a very low risk of attack, ultimately requiring providers to divert limited resources away from more aggressively protecting more sensitive systems data”).

⁹⁵ *See, e.g.*, MMTC Comments at 4-5 (explaining that the Administration’s approach has been successful and the FCC should continue to harmonize its oversight with that approach); Howard Beales Comments at 2; Nominum Comments at 8 (“We also encourage the Commission to provide flexibility for innovative ways of providing consumers privacy notices and embrace and include new methods, including in-browser messaging.”).

⁹⁶ *2012 White House Consumer Privacy Bill of Rights Report* at 17.

⁹⁷ *2012 FTC Privacy Report* at 48.

and cited, as an example of acceptable use of implied consent, a situation where an entity shares information with an affiliate with a clear affiliate relationship for marketing purposes:

The 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.⁹⁸

For the Commission to move forward with a broad opt-in regime, it would have to repudiate these findings, which it cannot do on the record before it. Rather, it should heed the FTC's recommendation that "[o]pt-out is sufficient for use and sharing of non-sensitive data."⁹⁹

This approach is just as valid for ISPs as it is for others in the Internet ecosystem. Public Knowledge seems to take the position that ISPs would have to review all the content of a user's Internet traffic to determine what is sensitive and what is not, and, therefore, the distinction would not work in the ISP context.¹⁰⁰ This is little more than a red herring. The information that the Commission proposes to cover is much broader than the content of user communications. For example, IP addresses or device identifiers cannot, on their own, identify an individual, let alone be considered sensitive information,¹⁰¹ but such information would be captured by the Commission's proposed rule. Moreover, Public Knowledge has no answer for the fact that ISPs and others in the Internet ecosystem have been able to comply with this distinction between

⁹⁸ 2012 FTC Privacy Report at 39.

⁹⁹ FTC Comments at 35.

¹⁰⁰ Public Knowledge et al. Comments at 24-26.

¹⁰¹ See, e.g., *Pruitt v. Comcast Cable Holdings, LLC*, 100 F. App'x 713, 716 (10th Cir. 2004) (finding that information stored within set-top boxes is not, by itself, personally identifiable information, because "without more," it is "nothing but a series of numbers"); *Eichenberger v. ESPN, Inc.*, No. C14-463 TSZ, 2015 WL 7252985 *3 (W.D. Wash. May 7, 2015) ("Courts that have considered the meaning of the term 'personally identifiable information' in other contexts have held that this term requires information that identifies a specific individual rather than an anonymous identification number or ID.").

sensitive and non-sensitive data under the FTC’s privacy regime for years without having to catalogue and categorize each and every piece of user content in an Internet packet as sensitive or non-sensitive.¹⁰²

2. The Commission’s proposed privacy rules for ISPs will not improve broadband adoption.

Another common, yet baseless, refrain from supporters of the Commission’s rules is that the proposed rules will somehow improve broadband adoption. OTI claims that “[p]ermissionless use of BIAS customers’ personal information . . . negatively impacts broadband adoption and use,”¹⁰³ and that “research has broadly and consistently demonstrated that privacy concerns constitute a barrier to broadband adoption and use.”¹⁰⁴ This is a false connection that is completely unsupported by any rational interpretation of the evidence.

In fact, the evidence on the record demonstrates the opposite: “[T]here is little connection between privacy concerns and adoption.”¹⁰⁵ All research on the drivers of non-adoption, including research by the NTIA using the Census Bureau’s Current Population Survey, has consistently found that privacy concerns is one of the least important barriers to broadband adoption. In the most current NTIA research, privacy or security concerns were cited as the main reason for non-adoption by a mere 1.4% of non-adopters, whereas lack of need or lack of interest was cited as the main reason by 55.2% of non-adopters, and expense (which includes both ISP

¹⁰² See Comcast Comments at 6, 37-38; NCTA Comments at 50-51 (noting the relatively few actions brought against ISPs by the FTC, that consumers trust ISPs more than edge providers in regards to privacy and security, and that ISPs have a strong incentive to maintain trust by respecting the privacy of their subscribers).

¹⁰³ OTI Comments at 9.

¹⁰⁴ *Id.* at 10.

¹⁰⁵ TPI Comments at 19; *see also* James C. Cooper Comments at 5 (“A recent survey of the literature on the economics of privacy finds that the adoption of privacy enhancing technologies has lagged substantially behind the use of information sharing technologies. These data see to belie the notion that more stringent privacy regulation is required to instill the trust necessary to foster broadband use.”).

and non-ISP costs) was cited as the main reason by 23.5% of non-adopters.¹⁰⁶ “The July 2015 Computer and Internet Use Supplement to the Current Population Survey finds that less than one-half of one percent of nonadopters note privacy concerns as the key reason they do not use the [I]nternet.”¹⁰⁷ And “in a 2015 Pew survey, less than one percent of respondents who do not own smartphones cite privacy concerns as a reason.”¹⁰⁸

To the extent there is any connection between broadband adoption and privacy, the research that OTI and others cite for this connection suggest the privacy concerns are not ISP-specific. OTI’s reference to the National Broadband Plan is telling, because the language regarding privacy concerns that OTI cites is part of a list of “several issues that are important *for the development of applications and content*.”¹⁰⁹ In other words, “even if privacy concerns *did* chill broadband adoption, they would do so not only – or even primarily – because of any ISP data uses; they would more likely do so because of the much more free-wheeling collection, use, and sometimes outright sale of consumer data by many others in the ecosystem.”¹¹⁰

Finally, this connection simply does not stand up to the real world facts about how consumers behave on the Internet and the tremendous success of an Internet economy built on the use of customer information for marketing and advertising. “[D]espite their privacy concerns, people increasingly engage in online activities that might involve sensitive

¹⁰⁶ NTIA, Digital Nation Data Explorer (Mar. 21, 2016), <https://www.ntia.doc.gov/otherpublication/2016/digital-nation-data-explorer>.

¹⁰⁷ TPI Comments at 20.

¹⁰⁸ *Id.*

¹⁰⁹ FCC, Connecting America: The National Broadband Plan 17 (2010), <https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf> (emphasis added).

¹¹⁰ AT&T Comments at 112 (emphasis in original); *see also* CTIA Comments at 65-69.

information, like financial transactions and shopping.”¹¹¹ As CTIA notes, “the dominance that Google and Facebook enjoy in their respective markets, and in the broadband ecosystem more generally, belies any notion that consumers’ concerns about privacy have inhibited the use of online services that collect, use, and share massive amounts of consumers’ personal data.”¹¹² And much of this success – by both ISPs and non-ISPs alike – has been enjoyed under the FTC’s robust but flexible privacy framework.¹¹³

C. ISPs Do Not Have Unique or Comprehensive Access to Consumer Data on the Internet.

One of the key justifications for burdensome privacy regulation cited by commenters that support the Commission’s proposals is that ISPs have a unique and comprehensive view into what consumers are doing on the Internet and, therefore, merit uniquely prescriptive and invasive privacy rules. But even a brief review of the record shows that notion to be a complete house of cards based on antiquated notions of how the network functions and how consumers use the Internet. The reality is that because of the open nature of the Internet and the widespread use of this information, the Commission’s proposal will not materially advance consumer privacy.

1. ISPs are not unique in their ability to collect or use consumer data.

ISPs are *not* unique in their ability to collect consumer information or with respect to the competitive forces that drive the marketplace.¹¹⁴ Renowned privacy expert Peter Swire recently

¹¹¹ Scott J. Wallsten, *No, the NTIA’s Survey Data Do Not Show a “Tipping Point” in Behavior Due to Privacy Concerns*, TPI Blog (May 15, 2016), <https://techpolicyinstitute.org/2016/05/15/no-the-ntias-survey-data-do-notshow-a-tipping-point-in-behavior-due-to-privacy-concerns/>.

¹¹² CTIA Comments at 67; *see also* MediaFreedom Comments at 2 (“Some of the most valuable and dominant companies on the planet – such as Google and Facebook – derive the overwhelming lion’s share of their billion in yearly revenues and profit from [the data generated by consumers on Internet] traffic.”).

¹¹³ CTIA Comments at 68; *see also* MMTC Comments at 2.

¹¹⁴ NCTA Comments at 46-47 (“Other broadband entities, including search engines, browsers, operating systems and content providers, may have even more comprehensive access to broadband consumer network usage data, by virtue of the fact that they interact with users across multiple broadband platforms and providers.”).

released a study finding that, “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.”¹¹⁵ And numerous commenters supported and reinforced Professor Swire’s conclusions.¹¹⁶ As even some supporters of the Commission’s proposal have recognized, the widespread ability of non-ISPs to collect as much or more of the data to which ISPs have access demonstrates that adopting privacy rules unique to ISPs will not materially advance the protection of consumer privacy.¹¹⁷

Those who support the FCC’s proposal offer unsubstantiated abstractions about ISP incentives to monetize customer information that are wholly devoid of real-world evidence.¹¹⁸ The only facts on the record demonstrate that ISPs have a strong track record of taking the privacy and security of their customers very seriously, have every incentive to do so, and rarely have taken steps that conflict with the FTC’s robust enforcement requirements.¹¹⁹

¹¹⁵ *Swire Paper* at 3-4.

¹¹⁶ *See, e.g.*, Cooper Comments at 5-6 (explaining that assumptions that ISPs have unique access to consumer data are unfounded because people increasingly connect to multiple ISPs throughout the day using mobile devices); CTIA Comments at 7 (“Indeed, contrary to the Commission’s assumptions, ISPs’ access to online consumers’ personal information in this ecosystem is neither comprehensive nor unique.”); T-Mobile Comments at 5 (explaining that the *Swire Paper* demonstrates that consumers “use multiple ISPs and devices and the increasing prevalence of encryption and proxy services have eroded whatever expansive access ISPs might once have had to their users’ traffic”); Verizon Comments at 17-21 (explaining that ISPs do not have unique and comprehensive access to consumer information); Communications Workers for America Comments at 3 (explaining that the NPRM’s premise that ISPs are uniquely able to collect sensitive and personal information is wrong).

¹¹⁷ EPIC, in particular, has criticized the proposal’s “narrow focus on ISPs.” *See Memorandum, FCC Communications Privacy Rulemaking*, EPIC, 1 (Mar. 18, 2016), available at <https://epic.org/privacy/consumer/EPIC-Draft-FCC-Privacy-Rules.pdf>.

¹¹⁸ Public Knowledge et al. Comments at 3-4, 12-17.

¹¹⁹ *See, e.g.*, Comcast Comments at 38-40; American Cable Association Comments at 8 (“ACA members have developed robust and effective privacy and data security procedures to protect the confidentiality of their customers’ proprietary information.”); NCTA Comments at 50-52 (noting the relatively few actions brought against ISPs by the FTC, that consumers trust ISPs more than edge providers in regards to privacy and security, and that ISPs have a strong incentive to maintain trust by respecting the privacy of their subscribers).

ISPs are also not in a unique competitive position. Regardless of what one may think about the state of ISP competition in any particular geographic market at any particular point in time, the facts are that the same competitive forces that drive the ISP marketplace are just as prevalent – and, in some cases, more so – in the marketplace for other online services. This means that switching a search engine, email provider, social media site, or operating system is no less difficult than switching an ISP – *and as demonstrated on the record, in many cases, it is more difficult.*¹²⁰ And even if the competitive situations were different, as Professor Christopher Yoo explains, that would not matter:

[I]n effect [this argument] suggest[s] that small companies facing high levels of competition have no incentive to abuse private information or that somehow disclosures and abuses of private information are somehow less problematic if done by a smaller firm. Any such conclusions are belied by the fact that small companies often look to more widespread use of private information to gain a competitive advantage against their larger rivals, and harm to consumers associated with disclosures or abuses of private information does not turn in any way on the size of the company involved.¹²¹

The record also demonstrates, consistent with Professor Swire’s conclusions, that ISPs can access and collect no more consumer data than many non-ISPs, and in many cases, have access to less consumer data.¹²² For example, AT&T explains that “countless entities that are not regulated telecommunications carriers have access to essentially all the same information as ISPs,” but that non-ISP actors have far more visibility into the online behavior of consumers – offering a series of illustrations that demonstrate that the “‘visibility gap’ between ISPs and other

¹²⁰ See, e.g., Comcast Comments at 40-42 (showing that consumers face high switching costs when moving between non-ISPs and are thus not likely to switch between services); AT&T Comments at 47 (demonstrating that it is far more difficult to switch operating systems, social networks, and email providers than ISPs because switching between these non-ISP providers requires consumers to give up valuable apps and services, social connections, and non-portable email addresses, which are either quite difficult or impossible to transfer between services).

¹²¹ Christopher Yoo Comments at 5.

¹²² 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.”).

actors is rapidly widening.”¹²³ Mobile Future similarly notes that “[e]specially in the mobile context, other players dominate cross-device and cross-context tracking.”¹²⁴ Future of Privacy Forum explains that if the Commission “seeks to create rules that will be relevant and influential across the Internet ecosystem, . . . it must first understand that ecosystem,” and proceeds to explain the intricacies of non-ISP tracking and data collection practices.¹²⁵

Fundamentally, as the FTC’s *2012 Privacy Report* concludes, “ISPs are just one type of large platform provider.”¹²⁶ Tellingly, the NPRM inexplicably omits any reference to the parts of that FTC report and the statements of FTC staff at the conclusion of the large platform provider workshop that ISPs are *not* unique or deserving of any special rules and asserts that privacy policies should be technology-neutral.¹²⁷ Several commenters repeat the Commission’s mistake, creating an echo chamber of misleading assertions both about what the FTC said in its report and about the data collection capabilities of ISPs.¹²⁸

¹²³ AT&T Comments at 12 (illustrating the relative abilities of online entities to collect user information when a consumer “(i) accesses news websites on his or her home computer; (ii) runs a Google search on that computer; (iii) watches Netflix on his smartphone while riding a bus; and (iv) checks Facebook on that smartphone while sitting in a coffee shop”).

¹²⁴ Mobile Future Comments at 4-5.

¹²⁵ Future of Privacy Forum Comments at 9-26.

¹²⁶ *2012 FTC Privacy Report* at 56.

¹²⁷ *See* Comcast Comments at 26-27 & n.59.

¹²⁸ *See, e.g.*, CDT Comments at 17-18 (“BIAS providers are uniquely positioned to have access to large amounts of very detailed customer PI.”); CDD Comments at 10-11 (“Through the capture of consumer behavior across their devices, including the mobile phone, and combined with their customer database, BIAS companies are in a unique position to create personalized communications based on a person’s real actions.”); Consumer Watchdog Comments at 4-5 (“Nonetheless, BIAS providers occupy a unique spot in the Internet ecosystem. They have access to virtually all of a subscriber’s Internet traffic. Even if the data is encrypted, a great deal is revealed purely from basic header information such as IP addresses, ports, and timing.”); National Consumers League Comments at 8-9 (“BIAS providers pose a ‘unique and heightened risk to privacy for their subscribers’ because BIAS providers collect vast amounts of customer information and there is a relative lack of competition among BIAS providers.”).

To be sure, a few commenters, including Upturn and Public Knowledge, actually attempt to rebut Professor Swire’s findings, but their analyses amount to little more than attempts at misdirection, and do nothing to undermine the validity of the basic facts as reported by Professor Swire.¹²⁹ For example, in response to the argument that encryption has significantly limited what information ISPs can see regarding their customers’ behavior on the Internet, Public Knowledge and Upturn both make much of the notion that even when traffic is encrypted the ISP can see the domain name of the site that the customer is visiting. But Professor Swire acknowledges that ISPs can see domain names of the websites their customers visit. His point is not that ISPs cannot see anything – even though he does note that this *is* the case when a customer is using a VPN¹³⁰ – but that the amount of information an ISP can see today is significantly reduced vis-à-vis what ISPs could see in the past and what other platform providers can still see today.¹³¹ On that last point, Upturn tries to minimize this trend by arguing that some sensitive traffic is still not encrypted.¹³² Again, the notion that some traffic remains unencrypted is not inconsistent with Professor Swire’s findings. But the trend that Professor Swire identifies is clear – “[a]n estimated 70 percent of traffic will be encrypted by the end of 2016”¹³³ – and *nobody* on the record attempts to refute that.

¹²⁹ See Upturn Comments at 1-2; Public Knowledge et al. Comments at 11.

¹³⁰ *Swire Paper* at 3, 7, 26-35.

¹³¹ See, e.g., *Swire Paper* at 35, 69 (“[A]n ISP can see, at most, the host domain a user visits, but not the detailed URL of the sub-page visited.”).

¹³² Upturn Comments at 3.

¹³³ *Swire Paper* at 3.

2. The Commission's proposals will not materially advance consumer privacy.

Because the information the Commission seeks to regulate is widely available to many on the Internet – to ISPs and non-ISPs alike – the Commission's proposals would not materially advance consumer privacy. In recognition of this fact, many commenters expressed the need for an approach that covers all companies operating in the online space in order to provide consumers with meaningful, comprehensive privacy protections. For example, EPIC explains:

Indeed, many of the largest email, search, and social media companies rival the scope and data collection activities of the ISPs. It is significant also that the FTC permitted Google to consolidate the data of Internet users across multiple Internet services over the strong objections of privacy advocates, technology experts, members of Congress, and the states Attorneys Generals [*sic*]. A failure to protect the privacy of consumers from these Internet-based services is a failure to provide meaningful communications privacy protections. The FCC describes ISPs as the most significant component of online communications that poses the greatest threat to consumer privacy. This description is inconsistent with the reality of the online communications ecosystem. Internet users routinely shift from one ISP to another, as they move between home, office, mobile, and open WiFi services. However, all pathways lead to essentially one Internet search company and one social network company. Privacy rules for ISPs are important and necessary, but it is obvious that the more substantial privacy threats for consumers are not the ISPs.¹³⁴

Similarly, Future of Privacy Forum recognizes that the FCC's framing of the relative data collection abilities of ISPs and edge providers “reflects a fundamental misunderstanding of the current online ecosystem.”¹³⁵ Future of Privacy Forum admonishes that, as constructed, “[t]he FCC's proposed rules, by deviating markedly from industry norms, will not be relevant to the rest of the Internet advertising and data exchange ecosystem” and “the rules will be considered irrelevant even for edge providers carrying out identical advertising activities to those captured

¹³⁴ EPIC Comments at 16.

¹³⁵ Future of Privacy Forum Comments at 9.

by the Rule. As a result, consumers will see no change in their online experience or in the extent to which [the] data about their online activities are collected and used.”¹³⁶

*

*

*

This analysis reinforces the conclusion Comcast and others express in the initial round of comments: That when the various harms the Commission’s proposal is likely to cause are measured against the putative benefits of the proposed rules, the result is unmistakably clear – the harms demonstrated in the record far outweigh any possible consumer benefits, and there is no sound public policy basis for such inflexible, expansive, and invasive rules.

III. THE RECORD OVERWHELMINGLY DEMONSTRATES THAT THE COMMISSION’S PROPOSALS ARE UNLAWFUL.

Even assuming there were a sound public policy basis for the Commission’s proposals, there is no legal basis for adopting them. The record confirms that imposing such an expansive regime on ISPs would be a violation of ISPs’ First Amendment commercial speech rights, outside the scope of the Communications Act, and a textbook example of arbitrary and capricious rulemaking in violation of the Administrative Procedure Act.

A. The Commission’s Proposals Would Violate the First Amendment.

The record demonstrates that the Commission’s proposal would violate the First Amendment under *Central Hudson*,¹³⁷ *Sorrell*,¹³⁸ and other applicable Supreme Court decisions. Multiple commenters identify many reasons why the proposed rules would be unconstitutional.¹³⁹ In contrast, very few commenters even try to argue that the proposed rules

¹³⁶ *Id.* at 29-30.

¹³⁷ *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n of N.Y.*, 447 U.S. 557 (1980).

¹³⁸ *Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011).

¹³⁹ See Tribe Comments at 2-8, 9-10, 39-40; American Advertising Federation et al. at 8; Association of National Advertisers Comments at 31-35; AT&T Comments at 91-100; CenturyLink Comments at 12-13; Consumers’

would be constitutional, much less explain how they could survive judicial scrutiny.¹⁴⁰

Specifically, only two commenters filing in support of the proposal discuss the First Amendment implications of the proposed rules in any depth: Public Knowledge and Access Now. Neither offers any credible constitutional defense for the rules.

Public Knowledge asserts that the Commission’s onerous opt-in proposal “easily meets *Central Hudson’s* constitutional speech test” based on the D.C. Circuit’s holding in *NCTA v. FCC*.¹⁴¹ But Public Knowledge ignores the critical differences between the challenged order in *NCTA* and the current proposed rules. Among other things, the *NCTA* court’s consideration was limited to a requirement that voice carriers obtain opt-in consent to share CPNI with unaffiliated third party marketers.¹⁴² Here, the Commission proposes an expansive opt-in regime governing a much broader swath of customer information and a much broader set of uses by ISPs or their controlled agents/vendors to market their own products and to help others market their products. The new rules would also impose content- and speaker-based distinctions that the Supreme Court categorically rejected in *Sorrell*.¹⁴³

Public Knowledge further suggests that differences in the amount of record evidence may help explain why the Tenth Circuit rejected similar blanket opt-in requirements in *U.S. West v. FCC*, whereas the D.C. Circuit found such a regime to be constitutionally permissible in

Research Comments at 10-11; CTIA Comments at 73-94; DMA Comments at 18; NCTA Comments at 32-33; T-Mobile Comments at 42-43; USTelecom Comments at 31-32; Verizon Comments at 29-34, 36-40, 50-53; Washington Legal Foundation Comments at 10-16.

¹⁴⁰ See Access Now Comments at 9-10; Public Knowledge et al. Comments at 35-39.

¹⁴¹ See Public Knowledge et al. Comments at 36.

¹⁴² Comcast Comments at 90 n.245.

¹⁴³ See Comcast Comments at 95-96. Professor Tribe also explains that the FCC’s proposal is unconstitutional because it “runs afoul of fundamental First Amendment limits on the FCC’s authority to regulate customer information, as recognized in *Sorrell v. IMS Health, Inc.*, 564 U.S. 552 (2011)” Tribe Comments at 3.

NCTA.¹⁴⁴ But that revisionist argument is entirely unsubstantiated and, rather than supporting the Commission’s position here, only undermines it. As Comcast and other commenters show, the current rulemaking record lacks *any* evidence that consumers want, much less need, the burdensome privacy rules proposed by the Commission, or that the Commission’s proposal would actually lead to any material improvement for consumer privacy.¹⁴⁵

In apparent recognition of this evidentiary problem, Access Now argues in its comments that “the Verizon unique ID header [UIDH] program” is evidence of “concrete harm” sufficient to show that the Commission “has a substantial interest [in] protecting the fundamental right to privacy in the face of this type of widespread and invasive tracking.”¹⁴⁶ However, the UIDH program involved a single firm and a dispute over the adequacy of the disclosures and choices it offered to its customers. To the extent the Commission decides it needs to address that behavior, it has demonstrated that it can already do so via a consent decree that imposes far fewer burdens on speech than the proposed rules.¹⁴⁷ This isolated incident is woefully insufficient to satisfy the Commission’s burden of demonstrating that its more onerous proposed rules will materially advance an important governmental interest in a narrowly tailored manner, as the applicable Supreme Court precedent requires.¹⁴⁸

¹⁴⁴ Public Knowledge et al. Comments at 37-38.

¹⁴⁵ See, e.g., Comcast Comments at 25-42; NCTA Comments at 56-57; AT&T Comments at 42-49.

¹⁴⁶ Access Now Comments at 9-10.

¹⁴⁷ See *Cellco Partnership, d/b/a Verizon Wireless*, Order and Consent Decree, 31 FCC Rcd. 1843 (2016). Verizon’s consent decree with the Commission requires it to obtain opt-in consent before sharing the UIDH of a customer with a third party to deliver targeted advertising; all other uses and sharing of a customer’s UIDH are subject to opt-out consent. *Id.* ¶ 18. This requirement is *less* restrictive than the Commission’s proposed rules, which would require opt-in consent for both first-party and third-party uses and disclosures.

¹⁴⁸ Tribe Comments at 4, 16-17, 18-29, 38-40.

Against these weak assertions by Public Knowledge and Access Now, the views of numerous other commenters, including Professor Tribe, are overwhelmingly consistent with Comcast's conclusion that the Commission's proposed opt-in regime would not pass scrutiny under either the *Central Hudson* test or the Supreme Court's more recent holding in *Sorrell*.¹⁴⁹ As Professor Tribe explains, the Commission's proposal "suffer[s] from tailoring flaws and content-[and speaker-]based distinctions that were not present in *NCTA*," and as a result:

The proposed rules cannot meet the *Central Hudson* test, much less the requirements of full First Amendment scrutiny [as applied in *Sorrell*]. Contrary to the NPRM's insistence, technological and market developments since the *U.S. West* decision in 1999 make the proposed rules even *more constitutionally problematic* than the CPNI regulations invalidated by the Tenth Circuit. The proposed rules would impose a *much larger* burden on speech and are far *less* tailored to any substantial government interest.¹⁵⁰

Public Knowledge and Access Now similarly disregard the critical differences between the Commission's proposed rules and the regime enforced by the FTC, the nation's foremost expert in consumer privacy, to regulate the use of even more extensive customer information by non-ISPs. As Comcast and other commenters show, the FTC's approach is more narrowly tailored, technologically neutral, and context-sensitive.¹⁵¹ It imposes far fewer burdens on speech and has been successfully enforced by the FTC for over a decade. The record forecloses any justification for the more inflexible, speech-suppressing rules proposed by the Commission. As Professor Tribe observes, "the FTC experience demonstrates that there is nothing unique about ISPs' data collection, use, or sharing practices that would justify the FCC's proposed

¹⁴⁹ See Comcast Comments at 89-100.

¹⁵⁰ Tribe Comments at 7, 16 (emphasis in original).

¹⁵¹ See, e.g., Comcast Comments at 16-20; Association of National Advertisers Comments at 16-20; Leibowitz Comments at 4-5; Communications Workers of America Comments at 3-4; FTC Comments at 15-16, 27.

Draconian privacy rules.”¹⁵² The “availability of the FTC’s regulatory scheme as an obvious alternative that is less speech-suppressing *dooms* the FCC’s proposed rules under the third prong of the *Central Hudson* test.”¹⁵³

B. Any Authority the Commission May Have in Section 222 to Regulate ISP Data Usage and Sharing Practices Is Carefully Circumscribed.

Even assuming Section 222 could be read to cover ISPs, which it does not,¹⁵⁴ it represents the maximum privacy authority that the Commission has with respect to telecommunications providers. Most of the proposal’s supporters merely assert that the Commission has the authority to adopt its proposal, but fail to explain how the language of Section 222 can be squared with the expansive regime proposed by the Commission or consider the ramifications of invoking section 706, which potentially extends the Commission’s jurisdiction throughout the entire Internet ecosystem.¹⁵⁵ As a result, these assertions are meritless and inconsistent with the plain language of the statute.

¹⁵² Tribe Comments at 34.

¹⁵³ *Id.* at 25 (emphasis added).

¹⁵⁴ A number of commenters confirm Comcast’s initial assessment that Section 222 does not cover ISPs. *See, e.g.*, CTIA Comments at 16 (“Both the plain language of Section 222 and the legislative history make clear that Congress drafted this section to protect certain information that carriers obtain solely by providing *voice* services to customers in a concentrated, closed market.”) (emphasis in original); NCTA Comments at 8-9 (“The plain text of Section 222 contains language specific to the provision of telephony services that simply cannot map to broadband at all, thereby underscoring the absence of Congressional intent to apply those provisions to the Internet generally or to broadband Internet access service specifically.”); American Advertising Federation, et al. Comments at 5-6; DMA Comments at 13. Moreover, there is nothing in the D.C. Circuit’s recent decision regarding the Open Internet rules that changes this argument.

¹⁵⁵ *See, e.g.*, OTI Comments at 11-12 (arguing vaguely that the Commission can rely on “several additional sources of statutory authority” to support and enforce its proposal); EPIC Comments at 28-30 (proposing that the FCC adopt a privacy regime completely divorced from the requirements of Section 222 without describing how such a regime might be accomplished); Consumer Watchdog Comments at 2.

1. The Commission may not expand the scope of its framework to encompass *non*-CPNI like IP addresses and device identifiers.

The record is clear that the proposed scope of the information that would be covered by the Commission’s authority exceeds the bounds of Section 222. As explained by Comcast, NCTA, CTIA, and many others, neither CPNI nor the newly invented category of “customer proprietary information” is broad enough to encompass all the information that the Commission proposes to cover within its rules.¹⁵⁶

Many of the proposal’s supporters urge the Commission to apply the rules to both CPNI and PII, or in some cases to expand the list of covered PII to include additional information, but they do not explain how the Commission can legally accomplish this.¹⁵⁷ Others merely assert that Section 222(a) gives the Commission authority to cover PII in its privacy framework, arguing that Section 222(a) is an independent grant of authority and the Commission can broadly interpret the scope of “proprietary information.”¹⁵⁸

¹⁵⁶ See, e.g., Comcast Comments at 74 (“[T]he 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.”); CTIA Comments at 11 (“[T]he language of the statute and well-established principles of statutory construction make clear that Section 222 protects only a limited category of customer information of telephone *voice service* customers.”) (emphasis in original); NCTA Comments at 12 (“It would be anomalous to decide that, in enacting Section 222, Congress intended to comprehensively protect a voice service customer’s CPNI by imposing privacy obligations on the full scope of entities that may be able to access such data, while also – via the same statutory language – providing piecemeal protection for broadband customer data by imposing privacy requirements on only a small slice of entities that have access to such data.”).

¹⁵⁷ See, e.g., Access Now Comments at 4-5 (supporting the proposed customer proprietary information and PII definition and urging the Commission to expand its non-exhaustive list of PII covered to include more types of metadata); Public Knowledge et al. Comments at 27-28 (arguing that, in its 2007 CPNI Order, the Commission interpreted CPNI to encompass PII in a broad sense and must address its rationale for doing otherwise in this context but not otherwise explaining how PII can be included legally within the Commission’s privacy rules); Access Humboldt et al. Comments at 3 (asserting that Section 222 gives the Commission authority “to protect the confidentiality of customers’ private information”); CDD Comments at 15-16 (same).

¹⁵⁸ See, e.g., CDT Comments at 11-12; OTI Comments at 18-20; Free Press Comments at 9-10.

However, numerous commenters show that the Commission cannot create a new category of “customer proprietary information” to expand Section 222 to PII. For example, the Electronic Transactions Association agrees with Comcast and others that “Section 222(a) merely articulates the duty all telecommunications carriers have to protect CPNI and the proprietary information of other carriers (and equipment manufacturers) as more fully detailed in Sections 222(b) and (c), and that it does not create a category of customer proprietary information separate and apart from CPNI.”¹⁵⁹ CTIA and AT&T further explain that the Commission cannot expand Section 222 to encompass PII because “proprietary information” is not the equivalent of PII.¹⁶⁰ Rather, proprietary information “is information that a person or entity owns to the exclusion of others.”¹⁶¹ In an open network like the Internet, however, this concept is completely anachronistic.¹⁶² These comments overwhelmingly show that Section 222 cannot be extended to cover non-CPNI PII.

Similarly, a number of commenters explain that IP addresses and other device identifiers are not encompassed within Section 222. Comcast’s initial comments demonstrate that a customer’s IP address cannot be CPNI, in part because it is not information that is “made

¹⁵⁹ Electronic Transactions Association Comments at 9; *see also* Comcast Comments at 71-75 (arguing same based on the statutory text, framework, and legislative history); AT&T Comments at 103-08 (“Section 222(a) grants the Commission no legal authority to ‘protect customer information that is not CPNI.’”); CTIA Comments at 25-35 (explaining that “[t]he text and structure of Section 222, as well as its legislative history, make clear that CPNI is the *only* customer data that Section 222 protects”).

¹⁶⁰ CTIA Comments at 32 (“Congress drafted Section 222 to cover ‘proprietary information,’ not ‘personal information’ or ‘personally identifiable information’ (‘PII’), the latter of which are the kinds of information that privacy laws typically protect.”); AT&T Comments at 101-02 (explaining that “there is thus nothing confidential, and thus nothing ‘proprietary,’ about information accessible not only to ISPs, but more broadly to other entities throughout the Internet ecosystem”).

¹⁶¹ CTIA Comments at 32-35; AT&T Comments at 100-03. CTIA also disproves the argument made by Public Knowledge that the FCC has previously interpreted CPNI to include PII in its 2007 CPNI Order by showing that, in context, the FCC’s discussion in that order is really limited to CPNI. CTIA Comments at 30-31.

¹⁶² Comcast Comments at 86-87 & n.234.

available to the carrier by the customer,” as required by the CPNI definition.¹⁶³ Moreover, because the customer does not own the IP addresses, it is impossible to say that consumers have a “proprietary” interest in them. Other commenters agree that neither IP addresses nor device identifiers are CPNI.¹⁶⁴ Those who support the Commission’s proposals have no answer for the analysis put forward by Comcast and others demonstrating that IP addresses are not CPNI.¹⁶⁵ Thus, the Commission cannot and should not include IP addresses (or similar device IDs) within its privacy framework under any category.

2. Section 222 excludes *both* aggregate and de-identified information.

There is widespread agreement on the record that Section 222 excludes both aggregate customer information and information that is not “individually identifiable” CPNI, and that the Commission’s proposal to exclude only information that is *both* de-identified and aggregated is both unlawful and unnecessary, particularly in light of the Commission’s proposed “linked or linkable” standard.¹⁶⁶ Commenters broadly recognize that Section 222 does not cover either de-identified *or* aggregate information.¹⁶⁷ For example, CTIA notes that the statute “unambiguously

¹⁶³ *Id.* at 77-81.

¹⁶⁴ Internet Commerce Coalition Comments at 14; *see also* NCTA Comments at 21 (arguing same and pointing out that the Commission itself recognized in the NPRM that IP addresses are “‘roughly analogous’ to a telephone number”); Cincinnati Bell Comments at 6 (“[S]ource and destination IP addresses . . . should not be considered CPNI because this information is necessarily sent onto the open Internet in order to make the service work.”).

¹⁶⁵ *See, e.g.*, OTI Comments at 20-21.

¹⁶⁶ Comcast Comments at 84-86; *see also* AT&T Comments at 61-72; CenturyLink Comments at 17-18 (“[I]nformation that is anonymized and/or reasonably de-identified cannot and should not be covered by the rules, regardless of whether it is in aggregate form.”); Sprint Comments at 6-8; NCTA Comments at 19-21 (“Indeed, there is nothing in Section 222 to suggest that de-identified information which is not ‘aggregate’ somehow remains ‘individually identifiable.’”); State Privacy and Security Coalition Comments at 5; ITIF Comments at 18-19.

¹⁶⁷ *See, e.g.*, Comcast Comments at 85 (explaining that under Section 222 “carriers are free to use, disclose, or provide access to CPNI that is not ‘individually identifiable’ without obtaining customer approval”); AT&T Comments at 61-62 (explaining that Section 222 categorically exempts de-identified data from CPNI regulation).

excludes de-identified data.”¹⁶⁸ And former FTC Chairman Jon Leibowitz similarly explains that de-identified data “does not present a risk to consumer privacy or security.”¹⁶⁹

Future of Privacy Forum confirms that the Commission should allow for use of de-identified information regardless of whether it is also aggregated:

We urge the FCC to specifically recognize that *non-aggregate* data can be de-identified in a manner that makes it not reasonably linkable to a specific individual. The FCC’s suggestion that data must be aggregated to be de-identified ignores the range of de-identification tools that are available to make it difficult or impossible to re-identify data as pertaining to a specific individual.¹⁷⁰

Other commenters strongly urge the FCC to exclude aggregate and de-identified information from its framework (including information that is de-identified with respect to a single individual even if it is not aggregated with other information), because of the value such information provides for network and service management and the identification and mitigation of security concerns.¹⁷¹ Comcast agrees with these commenters and also with AT&T that “information about a *device* can raise privacy concerns only to the extent that it can in turn be linked to a *person*.”¹⁷²

¹⁶⁸ CTIA Comments at 35.

¹⁶⁹ Leibowitz Comments at 6.

¹⁷⁰ Future of Privacy Forum Comments at 6 (emphasis in original); *see also* IMS Health Comments at 6 (“All other data privacy frameworks that exist in the United States (and in most places globally) permit de-identification of individual data, where appropriate steps are taken to remove identifiers and protect the data.”).

¹⁷¹ *See, e.g.*, Lehr et al. Comments at 8-9 (urging the Commission to make de-identified and aggregate information available to academics and researchers “to sustain the safe operation of the end-to-end Internet”); T-Mobile Comments at 34-36 (“[D]e-identified data (whether aggregated or not) provides a variety of significant public interest benefits,” including monitoring and containing the spread of infectious diseases, improving traffic patterns and transportation infrastructure; and aiding in disaster recovery efforts); Email Sender & Provider Coalition Comments at 7-8 (recommending the FCC permit sharing of aggregate data to aid email service providers in assessing the functionality of their services).

¹⁷² AT&T Comments at 69 (emphasis in original).

Finally, commenters highlight the problems with the Commission’s proposed “linked or linkable” definition of individually identifiable information.¹⁷³ The FTC helpfully suggests “that the definition of PII only include information that is ‘*reasonably*’ linkable to an individual.”¹⁷⁴ Comcast supports this recommendation, which is required by the plain statutory language indicating that only “individually identifiable” CPNI is covered by Section 222.¹⁷⁵

3. Section 222 does not govern information that ISPs obtain from third parties.

In addition, several commenters highlight the problems associated with the Commission’s suggestion that it limit ISPs’ use of information obtained from third parties.¹⁷⁶ Expanding the scope of the rules so broadly as to require an opt-in for *any* use of data, regardless of how it is collected or obtained, is untenable and contrary to the statute. In particular, as Comcast notes, “[t]he 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 the carrier customer relationship’ or outside the ISP’s ‘provision of a telecommunications service.’”¹⁷⁷

Many other commenters agree that Section 222 does not apply to data the ISP acquires from third parties.¹⁷⁸ Limiting ISPs’ access to or use of information they obtain from third

¹⁷³ Comcast Comments at 84-86.

¹⁷⁴ FTC Staff Comments at 9 (emphasis added); *see also* Leibowitz Comments at 6 & n.23 (“[T]he FTC was clear that companies should be provided with flexibility in determining how to ensure de-identified data stays protected.”).

¹⁷⁵ *See* 47 U.S.C. § 222(c)(1).

¹⁷⁶ *See NPRM* ¶ 138.

¹⁷⁷ Comcast Comments at 76-77; *see also* CenturyLink Comments at 15-16 (“For example, the *Notice* proposes to include . . . information that is publicly available, whether through a data broker or otherwise, including the customer’s name. The suggestion that information of this type is in all cases proprietary to the customer is indisputably wrong. Rather, often it is easily obtained by multiple parties, and cannot be deemed CPNI.”).

¹⁷⁸ *See* Comcast Comments at 75-77 (explaining that the CPNI “does not include any data that the carrier may obtain *outside* of this relationship, such as from a third party”) (emphasis in original); NCTA Comments at 83-84 (“[T]he proposal to subject publicly available data obtained from third parties to the proposed default opt-in permissions

parties, while other companies – like edge providers – are able to purchase and use that same information, will not lead to any benefit for consumer privacy.¹⁷⁹ But it certainly *will* exacerbate the competition-distorting effects of what the Commission has already proposed by further hamstringing ISPs’ ability to compete with non-ISPs in the online advertising marketplace.¹⁸⁰

C. Other Provisions of the Communications Act Do Not Support the Proposed Rules.

Section 222 represents the *maximum* privacy authority the Commission has under the Communications Act with respect to telecommunications providers. The record includes numerous analyses that reinforce the argument that the Commission must respect the strictures inherent in the plain language and framework of Section 222, and it cannot adopt rules that alter the balance established by Congress in adopting this provision.¹⁸¹ On the other hand, commenters like OTI seem to take the view that these provisions give the Commission authority to go above and beyond what Congress has instructed. These unsupported assertions do not withstand scrutiny.

regime should be rejected, because it would be far more stringent than what others in the ecosystem are subject to under the FTC Framework.”); USTelecom Comments at 30 (“Even if subsection (a) could be read to somehow protect customer information that is not CPNI, its provisions could not be read to authorize the proposed restraints on BIAS providers’ valid use of information that is publicly available.”).

¹⁷⁹ AT&T Comments at 43 n.97 (“An ISP might also obtain information about its customers from third parties (*e.g.*, data brokers) and combine it with its own customer data to increase the relevance of its first- and third-party advertising. There is no discernible basis for restricting an ISP’s ability to use third-party information in that manner: that information is already freely available on the market, and the ISP’s use of it does not result in any sharing of ISP-derived information with third parties.”).

¹⁸⁰ *See supra* § II.A.5 (discussing how the Commission’s proposal will harm competition).

¹⁸¹ *See, e.g.*, CTIA Comments at 59-73 (stating that “Section 222 is a unique creature of the Telecommunications Act of 1996; attempts to bootstrap the Proposed Rules to other provisions would suggest that the Commission is engaged in a results-oriented approach in this rulemaking, and, in any event, the other potential statutory candidates all suffer from fatal shortcomings” and explaining why the Commission cannot look to Sections 201, 202, 705, 706, or Title III for authority). Indeed, as Free Press acknowledges, “Sections 201 and 202’s prescriptions are by congressional design both more expansive and less specific than the privacy rules mandated by Section 222.” Free Press Comments at 15.

For example, OTI takes the position that Section 201 could serve the Commission in the same way that Section 5 of the FTC Act serves the FTC.¹⁸² OTI argues that the Commission could use Section 201 to inquire “whether a BIAS provider’s practice causes substantial injury, has no or insufficient countervailing benefits, and is not reasonably avoidable by consumers,” and that the Commission could use Section 201 to “find that BIAS providers’ use of customers’ private information for purposes other than to provide service constitutes not only a Section 222 violation when done without prior affirmative consent, but also a Section 201 violation.”¹⁸³ In other words, if a particular use violates the Commission’s rules under Section 222, it is a violation of both the rules *and* Section 201. But if the rules do not violate the rules under Section 222, the Commission would have a second bite at the apple under Section 201 if, for whatever reason, it happens not to like the particular data usage practice at issue.

Commenters highlight numerous problems with this reading of the statute. First, it renders Section 222 utterly superfluous, and that the Commission cannot do.¹⁸⁴ Second, consistent with the generally accepted canons of statutory interpretation, as well as with clear Commission precedent,¹⁸⁵ the Commission cannot look to other more general provisions to go further than what Congress authorized in the specific provision it adopted.¹⁸⁶ “Congress

¹⁸² OTI Comments at 12.

¹⁸³ *Id.*

¹⁸⁴ The Commission must not interpret one provision of the statute in a way that turns another provision of the statute into mere surplusage. Comcast Comments at 67-71.

¹⁸⁵ *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 ¶ 153 (1999) (“1999 CPNI Recon. Order”) (“[T]he specific consumer privacy and consumer choice protections established in section 222 supersede the general protections identified in sections 201(b) and 202(a).”).

¹⁸⁶ The D.C. Circuit has held that Section 706 also 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 *D. Ginsberg & Sons v. Popkin*, 285 U.S. 204, 208 (1932)); *see also* American Cable Association Comments at 20 (“[T]he Verizon Court also noted that

established the parameters of consumer privacy protections in Section 222, and the Commission cannot expand those protections through the more general mandate in Section 201(b).”¹⁸⁷ These same principles preclude the Commission from relying on Sections 705 or 706 as the basis for adopting privacy rules that are inconsistent with or broader than the framework set forth in Section 222.

In addition, commenters highlight how the plain text of these other provisions, particularly Sections 705 and 706, do not support the Commission’s assertion of authority. For example, T-Mobile explains that “Section 705 addresses issues surrounding piracy and the unlawful interception of content. It cannot provide authority for the dramatically expansive privacy rules proposed in the NPRM, which concern issues other than the content of the communications at issue.”¹⁸⁸ And NCTA highlights how the Commission has failed to consider the interplay between Section 705 and the Wiretap Act, and how the latter runs counter to the Commission’s proposed rules.¹⁸⁹ As to Section 706, NCTA notes that “it would be difficult for the Commission to argue that its proposed privacy rules would *eliminate* barriers to broadband investment,” and that, to the contrary, “there is already evidence that the Commission’s proposal to single out ISPs for more stringent rules would dampen broadband investment.”¹⁹⁰

Section 706(a) had ‘at least two limiting principles’: (1) the section must be read in conjunction with other provisions of the Communications Act to ensure that any regulatory action under Section 706(a) fell within the Commission’s subject matter jurisdiction, and (2) regulations must be “designed to achieve a particular purpose: to ‘encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans.’” (citing *Verizon*, 740 F.3d at 639-40)).

¹⁸⁷ T-Mobile Comments at 22; CTIA Comments at 61 (“Indeed, in enacting Section 222, Congress defined the appropriate scope of consumer privacy protections under the Act, and the Commission cannot expand that protection through a more general section of the Act.”).

¹⁸⁸ T-Mobile Comments at 22.

¹⁸⁹ NCTA Comments at 26-29.

¹⁹⁰ *Id.* at 29 (emphasis in original); see also T-Mobile Comments at 23 (“The Commission cannot rely on Section 706 because, as shown in these comments and others, the proposed rules are not tailored to promote the acceleration

Instead of looking to other statutory provisions for support, the Commission must – as per the direction of Congress – stay within the confines of Section 222 with respect to governing the privacy practices of telecommunications providers.

D. The Commission Cannot Prohibit or Limit the Use of Mandatory Arbitration Clauses.

As a number of commenters make clear, the Commission does not have authority under the Communications Act to prohibit or otherwise limit arbitration clauses, and it should not do so in any event because, as Congress and the Supreme Court have recognized, these clauses benefit both consumers and providers in a number of ways. Several parties support a limitation or outright prohibition on mandatory arbitration clauses, arguing, among other things, that the Commission does have the authority to restrict forced arbitration in broadband privacy claims¹⁹¹ and that limiting arbitration clauses will benefit consumers.¹⁹² But neither of these arguments is persuasive.

First, Section 222 does not authorize the Commission to nullify or otherwise limit the applicability of arbitration clauses. The argument that Section 222 can invalidate an arbitration clause rests on the notion that such a prohibition is necessary to implement the statutory

of broadband deployment and are, in fact, likely to have the opposite effect, as the proposed regime is likely to hamper BIAS providers' ability to compete and to confuse and frustrate consumers.”).

¹⁹¹ See American Association for Justice Comments at 6 (explaining that the FCC has legal authority under Sections 222 and 201 of the Communications Act and that the Federal Arbitration Act (“FAA”) is inapplicable); *see also* Consumer Federation of California Comments at 11-12; EPIC Comments at 27; Privacy Rights Clearinghouse Comments at 7.

¹⁹² See OTI Comments at 46 (explaining that forced arbitration should be prohibited because it “would be incongruous to give consumers so much control over their data, only to have disputes about the misuse of that data end up in forced arbitration, which so heavily favors the companies who hire the arbitrators”); *see also* American Association for Justice Comments at 5 (explaining that a proposal from the Consumer Financial Protection Bureau (CFPB) said that “limiting forced arbitration clauses containing class action bans has a powerful deterrent effect, resulting in companies changing practices in ways that benefit consumers as a whole”); Comments of Smithwick & Belendiuk at 7-10.

obligations in Section 222.¹⁹³ But Congress in Section 222 already prescribed a detailed regime to give effect to its intent, and prohibiting arbitration clauses is nowhere to be found. As Comcast argues in its initial comments, “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.”¹⁹⁴

Second, the Commission cannot use other provisions of the Act to enact such a prohibition or limitation. As described above, the Commission is prohibited from using broader sources of authority to disrupt the statutory balance Congress established in Section 222.¹⁹⁵ Moreover, none of those other sources of authority include the explicit “contrary congressional command” that the Supreme Court has said is necessary to override the Federal Arbitration Act (“FAA”).¹⁹⁶ Importantly, federal courts have upheld arbitration clauses in customer contracts for services covered by Sections 206, 207, and 208 of the Act, thus indicating that nothing in those provisions contravenes the express intent of Congress in the FAA to encourage the use of arbitration as a mechanism for dispute resolution.¹⁹⁷

Finally, even if the Commission did have such authority, preventing or limiting ISPs from using arbitration clauses in their customer contracts would be bad public policy because

¹⁹³ See, e.g., American Association for Justice Comments at 6 (stating that Section 222 “provides a duty for providers of communications services to protect both the privacy and security of information about their customers, [and] also provides the FCC with the authority to adopt rules that are necessary to implement this obligation”).

¹⁹⁴ Comcast Comments at 103; see also Verizon Comments at 70-80; AT&T Comments at 114-15; CTIA Comments at 50-59; Hughes Network Systems Comments at 8-9.

¹⁹⁵ See *supra* § III.C.

¹⁹⁶ *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).

¹⁹⁷ See, e.g., *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333, 346-47 (2011) (upholding an arbitration clause in a customer agreement for CMRS); *MCI Telecomms. Corp. v. Happy the Glass Man, Inc.*, 974 F. Supp. 1016, 1020-21 (E.D. Ky. 1997) (upholding an arbitration clause in a tariff for long-distance service).

such a decision would remove a useful, consumer-friendly tool for dispute resolution, ultimately resulting in harm to consumers.¹⁹⁸ Arbitration clauses are widely used throughout the Internet ecosystem, including by companies like Google and Netflix.¹⁹⁹ The idea that arbitration is bad for consumers and therefore should be limited rests on inaccurate assumptions about how arbitration works. The fact is that arbitration is much faster than taking a dispute to court or even an administrative agency.²⁰⁰ As Comcast discusses at length in our initial comments, arbitration can be a useful tool to resolve disputes because it allows for an efficient, less costly procedure that gives individuals a statistically better chance of recovery than class action litigation.²⁰¹ As Verizon explains, “[m]ultiple studies have found that consumers obtain relief in arbitration at rates higher than they do in court.”²⁰²

E. The Commission Should Not and Cannot Extend Its Rules to Cover ISPs’ Affiliates.

The record also highlights a number of issues with the way that the Commission may treat affiliates under the proposed rules. Specifically, various commenters explain that the

¹⁹⁸ Comcast Comments at 102-06; Verizon Comments at 70-80; AT&T Comments at 114-15; CTIA Comments at 50-59; Hughes Network Systems Comments at 8-9.

¹⁹⁹ See Google Fiber Residential Terms of Services (last updated June, 9, 2016), <https://fiber.google.com/legal/terms/residential/> (“Google Fiber and you agree to arbitrate all disputes and claims that arise from or relate to these Terms or the Services, except for claims arising from bodily injury. This agreement to arbitrate is intended to be broadly interpreted[.]”); Netflix Terms of Use (last updated May 5, 2016), <https://help.netflix.com/legal/termsfuse?locale=en&docType=termsfuse> (“If you are a resident of the United States (including its possessions and territories), you agree to the Arbitration Agreement and class action waiver described in Section 15 to resolve any disputes with Netflix (except for matters that may be taken to small claims court).”).

²⁰⁰ See Comcast Comments at 104 (explaining the consumer benefits to arbitration).

²⁰¹ *Id.* at 105-06.

²⁰² Verizon Comments at 75-76 (analyzing multiple studies and finding that “raw win rates, comparative win rates, comparative recoveries, and comparative recoveries relative to amounts claimed . . . do not support the claim that consumers and employees achieve inferior results in arbitration compared to litigation”); David Sherwyn et al., *Assessing the Case for Employment Arbitration: A New Path for Empirical Research*, 57 *Stan. L. Rev.* 1557, 1567 (2005) (“What seems clear from the results of these studies is that the assertions of many arbitration critics were either overstated or simply wrong.”).

Commission has no good policy reason or legal authority to require ISPs to obtain opt-in consent before sharing CPNI or customer proprietary information with their affiliates, or to extend the proposed rules to cover data collected by ISP affiliates.²⁰³ While some commenters, like OTI, Center for Digital Democracy (“CDD”), and Free Press, would have the Commission require opt-in consent for such affiliate sharing,²⁰⁴ they ignore the fact that doing so would be contrary to Commission precedent, the FTC’s time-tested approach, and common sense. CDD seems to argue that all ISP affiliate data collection practices should also be directly subject to the Commission’s proposed rules,²⁰⁵ but this would be even more problematic as a matter both of policy and law.

Regarding the first issue – sharing of CPNI or customer proprietary information with affiliates – in its *2012 Privacy Report*, the FTC noted that a “consumer choice mechanism is necessary *unless the affiliate relationship is clear to consumers.*”²⁰⁶ In other words, sharing non-sensitive information with affiliates – and affiliates’ use of that information for marketing – is permissible pursuant to *implied consent* under the FTC’s privacy framework *unless* the affiliate relationship is not clear to the consumer, in which case *opt-out* consent applies. The FTC explains in its comments in this proceeding that “[c]ommon branding is one way of making the

²⁰³ See, e.g., Verizon Comments at 24 (“Customers already reasonably assume that they have given their implied consent to receive offers from their own provider or from an affiliate of that provider to market any of those companies’ services – not just services to which the customer already subscribes.”); Competitive Carriers Association Comments at 25 (rejecting “the Commission’s proposal requiring BIAS providers to solicit and receive opt-in customer approval before sharing customer PI with all other affiliates and third parties” when not providing communications-related services).

²⁰⁴ OTI Comments at 23; CDD Comments at 18; Free Press Comments at 13 (“The Commission should modify its proposal accordingly and require opt-in approval for sharing or use outside the direct provision of broadband service – even within affiliated services.”).

²⁰⁵ CDD Comments at 18 (“Affiliates must also obtain opt-in for any services. Otherwise the arrangement illustrated by Verizon’s control of AOL and Millennial Media will undermine a consumer’s reasonable expectation for privacy.”).

²⁰⁶ *2012 FTC Privacy Report* at 42 (emphasis added).

affiliate relationship clear to consumers,”²⁰⁷ and that non-commonly branded affiliates may “be treated in the same manner as third-party sharing,” i.e., *using at most an opt-out mechanism for non-sensitive information*.²⁰⁸ This well-established approach – to share within a corporate family for marketing purposes – allows for efficiencies in the market and, accordingly, benefits consumers and companies alike, and has received significant support on the record in this proceeding.²⁰⁹ In contrast, the Commission’s proposed approach – particularly if taken to the extreme being advocated by OTI and Free Press – would undermine these efficiencies and, as a result, harm consumers. Thus, the Commission should follow the FTC’s privacy framework and allow ISPs to share customer data with their affiliates based on implicit consent if the affiliate relationship is clear to consumers, as in the case with common branding; in all other cases, opt-out consent should be permitted (unless sensitive data is involved, in which case opt-in consent would apply).

This is not to suggest that CPNI shared with affiliates would lose its protections – far from it. As Verizon explains in its comments:

[A]s long as broadband providers (1) provide clear and transparent notices about how customer information may be used; (2) ensure that their affiliates use customer information in accordance with the choices the customer has made; (3) ensure that the affiliates secure the information appropriately; and (4) provide any required notices in the

²⁰⁷ FTC Comments at 24.

²⁰⁸ *Id.*; see also *2012 FTC Privacy Report* at 42. As the FTC’s comments make clear, “the FTC’s longstanding approach . . . calls for the level of choice to be tied to the sensitivity of [the] data.” FTC Comments at 23.

²⁰⁹ See, e.g., T-Mobile Comments at 32 (“In addition, consistent with the FTC’s framework, providers should be free to use non-sensitive customer information for other innocuous and consumer-friendly purposes, **including affiliate sharing**, as long as the affiliate relationship is reasonable clear to consumers.” (emphasis added)); Verizon Comments at 14 (“Customers have come to expect companies with whom they already do business **and their affiliates** to offer them new products and services. Therefore, consent to use less sensitive customer information (such as an email address, the type of service plan to which the customer subscribers [*sic*], or the accessories they may have purchased) should be inferred for such first-party marketing.” (emphasis added)); American Advertising Federation et al. Comments at 8 (“The proposed opt-out standard for **sharing data with affiliates** for marketing communications-related services is unduly burdensome. It is a common practice, which consumers understand, for companies to market to their existing customers and to share within the same corporate family for this purpose, especially where the marketed service is related to the existing customer relationship.” (emphasis added)).

unlikely event of a breach, providers should be permitted to share their customers' information with their affiliates on an implied-consent basis.²¹⁰

The approach laid out by Verizon for sharing CPNI with affiliates is eminently reasonable and consistent with Commission precedent.²¹¹ Specifically, the Commission in its 2002 CPNI Order concluded that adopting an opt-in approach for sharing with affiliates was unnecessary because the likelihood of harm “is significantly reduced in the intra-company context by the carrier’s need for a continuing relationship with the customer.”²¹² In other words, when sharing CPNI with affiliates, ISPs have both the incentive and the ability to ensure that the data is protected and treated consistent with the customer’s choices. An opt-in requirement is unnecessary for sharing non-sensitive information, and implied consent or, at most, opt-out is more than sufficient to protect any interest the Commission may have in regulating the use of CPNI.

With respect to the second issue – extending the rules to cover information collected by non-ISP affiliates – the Commission’s authority here is clearly limited both by its subject matter jurisdiction under the Communications Act and by the scope of Section 222. With respect to the former, Comcast and other commenters note in their initial comments that extending the Commission’s rules to cover the collection and use of customer information by non-telecommunications carriers – including affiliates of telecommunications carriers – “would be

²¹⁰ Verizon Comments at 27.

²¹¹ See, e.g., *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; 2000 Biennial Regulatory Review – Review 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, ¶¶ 37-38 (2002).

²¹² *Id.* ¶ 37. This precedent also highlights why the Commission’s professed concerns about “corporate restructurings” are completely overblown. See *NPRM* ¶ 124. The straightforward approach proposed by Verizon and used by the Commission in the past addresses any such concerns in a way that is consistent with (i) the statute, (ii) the FTC’s time-tested approach, (iii) consumer expectations, and (iv) common sense.

patently unlawful.”²¹³ As the Commission insists, it lacks the authority to regulate “edge providers.”²¹⁴ Chairman Wheeler reiterated this position during the May 11, 2016 Senate Judiciary Committee hearing.²¹⁵ If the Commission’s conclusion is that the Communications Act, and Section 222 in particular, does not reach providers of non-telecommunications services, that conclusion must also hold true for providers of non-telecommunications services that happen to be affiliates of telecommunications carriers.

Moreover, Section 222, to the extent it applies to ISPs at all, only covers information collected by an ISP in the provision of the broadband Internet access service. Specifically, the statutory definition of CPNI is limited to information that a company collects *in the course of providing a telecommunications service*.²¹⁶ Thus, if an ISP’s affiliates are engaged in separate lines of business and collect information through their own, non-telecommunications-related

²¹³ Comcast Comments at 83; DMA Comments at 14 (“[T]he Commission does not have statutory authority to regulate entities that are not under Title II. We agree that any expansion to include, for instance, edge providers, would reach beyond those entities over which the Commission has jurisdiction.”); Computer & Communications Industry Association Comments at 2 (“The FCC is correct to limit its authority in the Broadband Privacy NPRM to exclude providers of edge services.”).

²¹⁴ See *Protecting and Promoting the Open Internet, Report and Order on Remand, Declaratory Ruling, and Order*, 30 FCC Rcd. 5601, Order ¶¶ 190-92 (2015) (limiting the scope of entities to which the Open Internet rules apply); see also 47 U.S.C. § 152(a) (limiting the Commission’s authority to “interstate and foreign communication by wire or radio”); *United States v. Southwestern Cable Co.*, 392 U.S. 157, 167, 178 (1968) (explaining that the scope of the Commission’s authority is limited to regulating “interstate and foreign communication by wire or radio” and things “reasonably ancillary to the effective performance of the Commission’s various responsibilities”).

²¹⁵ 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) (statement of Tom Wheeler, Chairman, FCC), <http://www.c-span.org/video/?409389-1/fcc-commissioners-testify-proposed-internet-privacy-rules> (starting at 00:23:08) (“We do not regulate those with whom the network terminates – in the vernacular of today – the edge providers. And this by the way includes network affiliates acting as edge providers. And we have never asserted jurisdiction over edge providers and do not assert it now.”).

²¹⁶ 47 U.S.C. § 222(c)(1). The Commission’s proposed definition of consumer proprietary information is consistent with the limited scope of the definition of CPNI. See NPRM ¶¶ 56-59 (proposing to define customer proprietary information “to include private information that customers have an interest in protecting from public disclosure, and consider such information to fall into two categories: (1) customer proprietary network information (CPNI); and (2) personally identifiable information (PII) the *BIAS provider acquires in connection with its provision of BIAS*” (emphasis added)).

lines of business, that information is neither CPNI nor consumer proprietary information, even if the customer from whom it is collected happens to also be a customer of the ISP business.²¹⁷ In such cases, affiliates and the information they collect cannot be subject to any of the rules the Commission may adopt; rather, such affiliates' privacy practices would instead continue to be covered by the FTC's privacy framework.

F. Adopting the Proposed Rules Would Be a Textbook Example of Arbitrary and Capricious Rulemaking.

Numerous commenters echo Comcast's initial assessment that adopting the proposed rules would be arbitrary and capricious because doing so would require the Commission to ignore important factors and misread the evidence.²¹⁸ In particular, adopting the proposed rules would require the Commission to ignore the clear costs, and embellish the unsupported benefits, of its proposal. That it cannot do without violating the Administrative Procedure Act.

There is simply no evidence that the Commission's proposal will enhance consumer privacy. The justifications and benefits supporters of the proposed rules cite are at best illusory and unable to stand up to real-world facts or record evidence.²¹⁹ On the other hand, the record includes numerous concrete examples of significant harms that would fall on consumers and frustration of important public policy objectives if the Commission were to follow through with

²¹⁷ *1999 CPNI Recon. Order* (“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.”).

²¹⁸ *See, e.g.*, T-Mobile Comments at 43-44, 46, 56; CTIA Comments at 15 (“[T]he classification of broadband service as a telecommunications service is contrary to the text, structure, and history of the Communications Act; is arbitrary and capricious; and is otherwise unlawful”); Consumers' Research Comments at 17 (explaining that the proposal would be arbitrary and capricious given the FCC's mistaken and misapplied justifications for its proposed rules); NCTA Comments at 30-31 (explaining how the FCC proposal is arbitrary and capricious under the Administrative Procedure Act because it fails to consider an important aspect of the problem and offers an explanation for its decision that runs counter to the evidence before the agency).

²¹⁹ *See supra* § II.B.

its proposal.²²⁰ Moving forward with its proposal would require the Commission to ignore this substantial and significant record evidence, and in so doing the Commission would commit a textbook example of arbitrary and capricious rulemaking.

IV. THERE IS WIDESPREAD CONSENSUS IN THE RECORD THAT THE COMMISSION SHOULD CLOSELY ALIGN ITSELF WITH THE TECHNOLOGY-NEUTRAL POLICIES AND PRINCIPLES ESPOUSED BY THE ADMINISTRATION AND THE FTC.

The record widely and strongly confirms Comcast’s position that the Administration and FTC approach to online privacy has been tremendously successful at protecting consumers while promoting innovation, investment, and competition, and that the “optimal” approach for the FCC would be to closely align itself with that approach. To that end, the Consensus Privacy Framework continues to be the only proposal on the record that provides for robust protection of consumers while also encouraging innovation, investment, and competition that will inure to the benefit of all consumers.

A. The Administration and FTC Approach Have Successfully Protected Consumers While Facilitating Innovation, Competition, and Investment.

Numerous commenters highlight the robust nature of the FTC’s privacy enforcement regime and the success of that approach in protecting consumers and fostering an environment where innovation, investment, and competition can thrive. The FTC explains that it “has brought over 500 cases protecting the privacy and security of consumer information” in a wide variety of circumstances, and that these “actions – in both the physical and digital worlds – send an important message to companies about the need to protect consumers’ privacy and data security.”²²¹ The Information Technology Industry Council notes that “the Internet has thrived –

²²⁰ See *supra* § II.A.

²²¹ FTC Comments at 4-5. Chairwoman Ramirez echoed this sentiment in a recent Senate hearing when she said “I think the Federal Trade Commission has done a very effective job in addressing consumer privacy and ensuring that consumer information is appropriately safeguarded.” *Examining the Proposed FCC Privacy Rules: Hearing Before*

and privacy has been protected – under the [FTC’s] approach to privacy.”²²² Likewise, Future of Privacy Forum observes that “the FTC has the broad regulatory authority to ensure that companies engage in fair and non-deceptive practices,” and that “[r]ecent enforcement actions demonstrate that the FTC’s jurisdiction is an effective model for online privacy.”²²³ And Professor Howard Beales remarks that one of the successes of the FTC and Administration approach thus far has been that “it applies a uniform regulatory approach to different technologies and different business models,” and that, as a result, “[i]t has largely avoided creating artificial barriers to either competition or innovation.”²²⁴

The success of the privacy model espoused by the Administration and enforced by the FTC leads many commenters to conclude that the FCC should closely align its rules with that approach. For example, ViaSat urges the Commission to “adopt a framework akin to the longstanding approach employed by the FTC, grounded on prohibiting ‘unfair or deceptive’ practices” and explains that “the FTC’s case-by-case approach . . . has been successful in protecting consumer privacy while affording businesses the ability to adapt and innovate as the

the Subcomm. on Privacy, Technology and the Law of the Senate Comm. on the Judiciary, 115th Cong. (May 11, 2016) (Statement of Edith Ramirez, Chairman, FTC), <http://www.c-span.org/video/?409389-1/fcc-commissioners-testify-proposed-internet-privacy-rules> (starting at 01:10:30).

²²² ITI Comments at 4; *see also* AT&T Comments at 30-35; Software & Information Industry Association Comments at 4; USTelecom Comments at iii; Beales Comments at 2.

²²³ Future of Privacy Forum Comments at 26; *see also* ITIF Comments at 10-12; Electronic Transactions Association Comments at 3-4; Beales Comments at 2; Verizon Comments at 6.

²²⁴ Beales Comments at 2. On the other hand, critics of the FTC’s approach highlight issues that either would be exacerbated by the FCC’s proposals, or that will not be fixed by the FCC’s proposals. For example, CDT laments that “American consumers face a patchwork of privacy standards that leave some personal information unprotected in surprising ways, and a general purpose consumer protection law enforced by the Federal Trade Commission (FTC) that maps imperfectly onto privacy rights.” CDT Comments at 6. But as explained above and by numerous other commenters, the FCC’s proposal will merely make the patchwork worse. *See, e.g.*, Advanced Communications Law & Policy Institute Comments at 14; Consumers’ Research Comments at 13; CTA Comments at 1.

market for online services evolves.”²²⁵ CALinnovates recommends that “the FCC should adopt a set of privacy rules mirroring the time-tested approach that guides the [FTC’s] enforcement actions.”²²⁶ And former FTC Chair Leibowitz explains that making the FCC’s rules “consistent with the FTC’s privacy framework would ensure that privacy enforcement remains technology-neutral, based on the type of data being collected and how it is used, rather than turning on the type of entity collecting the data.”²²⁷

Congressional leaders also encourage the FCC to align itself closely with the privacy policies espoused by the Administration and enforced by the FTC. For example, Senator Jeff Flake (R-AZ), in a letter to Chairman Wheeler, argues that the FCC’s approach would violate the First Amendment and that “[t]he FTC’s opt-out framework satisfies any substantial interest the government might have in protecting privacy,”²²⁸ and urges the FCC to “adopt the light-touch, opt-out approach to data privacy employed by the FTC.”²²⁹ Likewise, Representatives Upton (R-MI), Walden (R-OR), and Burgess (R-TX) write, “rather than a prescriptive rulemaking, we

²²⁵ ViaSat Comments at 4-5; ICLE Comments at 4-5 (encouraging the Commission to replicate the current “federal privacy regime”).

²²⁶ CALinnovates Comments at 2; *see also* Cincinnati Bell Telephone Co. Comments at 5 (“[T]he Commission’s PII regime should mirror the existing FTC definitions, breach parameters and response requirements, and guidance for protecting sensitive data.”); IMS Health Comments at 11 (“We encourage the FCC to implement an overall approach to de-identification that mirrors the key elements of the existing legal frameworks.”).

²²⁷ Leibowitz Comments at 2; *see also* CTIA Comments at 186 (urging the Commission to adopt an approach similar to the FTC’s approach); ITIF Comments at 11 (“This is a widely agreed-upon point: privacy rules in particular, and rules governing technology-enabled practices and business models generally, should be technology-neutral and evenly applicable across different entities.”); Richard Bennett Comments at 1 (suggesting a “more productive approach that would . . . [h]armonize rulemaking on private information visible to both ISPs and other Internet services under the common, technology-neutral framework devised by the FTC”).

²²⁸ Senator Flake Comments at 7.

²²⁹ *Id.* at 8.

believe that the FCC should create a more consistent privacy experience for consumers by mirroring the FTC’s successful enforcement-based regime.”²³⁰

Perhaps most importantly, pursuing an approach for ISPs that closely hews to the Administration and FTC approach is consistent with consumer expectations. The Progressive Policy Institute (“PPI”) commissioned a poll – the *only* such data regarding consumer expectations on the record in this proceeding – “to assess consumer opinion about how their online information is protected.”²³¹ The results of PPI’s poll “demonstrate that consumers want consistent protections for their online information from all players in the internet ecosystem,” by the extremely wide margin of 94% to 5%.²³² In light of these results, PPI urges the FCC to “consider rules that are consistent with the principles embodied in the Obama Administration’s Consumer Privacy Bill of Rights and the Federal Trade Commission’s well-established and effective privacy framework.”²³³

B. The Consensus Privacy Framework Is the Best Path Forward to Achieve the Commission’s Goals.

The Consensus Privacy Framework put forward by a diverse group of industry associations acknowledges and addresses these consumer expectations by implementing the successful Administration and FTC approach in the context of ISPs and the FCC’s authority under Section 222. This proposal received extensive support in the record. T-Mobile, for example, urges the FCC to “pursue a consensus framework, such as that set forth by the American Cable Association, Competitive Carriers Association, CTIA, National Cable &

²³⁰ Letter to Chairman Wheeler from Representatives Fred Upton, Greg Walden, and Michael Burgess at 3 (June 1, 2016).

²³¹ Progressive Policy Institute Comments at 1.

²³² *Id.*

²³³ *Id.*

Telecommunications Association, and USTelecom, which is grounded on longstanding FTC principles.”²³⁴ The American Cable Association observes that the Consensus Privacy Framework will satisfy the Commission’s policy goals because it “focuses on four privacy principles: (1) transparency; (2) respect for context and consumer choice; (3) data security; and (4) data breach notification.”²³⁵

Adopting the Consensus Privacy Framework will address some of the key concerns raised by Comcast and others in this proceeding:

- *Promote Competition and Innovation.* The Consensus Privacy Framework will ensure a level playing field between edge providers and BIAS providers, promoting an innovative and competitive broadband ecosystem while still allowing the Commission to safeguard the privacy interests of consumers.²³⁶
- *Limit Scope to CPNI.* The scope of information regulated by the Consensus Privacy Framework would be consistent with the Commission’s approach in the legacy voice context, and with the plain language and intent of the statute.²³⁷
- *Limit Opt-In Consent to Sensitive Data.* Opt-in consent would 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).²³⁸
- *Implement a Reasonable De-Identification Standard.* ISPs should be free to use, disclose, and provide access to de-identified information that is reasonably de-linked from any identified individual, even if it is not aggregated, without obtaining prior customer approval.²³⁹

²³⁴ T-Mobile Comments at 15.

²³⁵ American Cable Association Comments at 40; *see also* WISPA Comments at 9-10.

²³⁶ American Cable Association Comments at 42; *see also* Competitive Carriers Association Comments at 7.

²³⁷ *See supra* § III.B.

²³⁸ *See, e.g.*, Ohlhausen Comments at 2; FTC Comments at 22; NCTA Comments at 58; Mobile Future Comments at 3-4; Cincinnati Bell Telephone Co. Comments at 10-11; ITI Comments at 16; Verizon Comments at 66.

²³⁹ *See supra* § III.B.2; *see also* AT&T Comments at 61-72; CenturyLink Comments at 17-18; Sprint Comments at 6-8; NCTA Comments at 19-20; State Privacy and Security Coalition Comments at 5; Future of Privacy Forum Comments at 6; ITIF Comments at 18-19.

- *Clarify Use of Agent/Vendors/Service Providers.* These relationships should be permitted so long as the ISP has an agreement with the entity requiring it to safeguard the CPNI and to use it solely on behalf of and as directed by the ISP, and not for the entity's own purposes.²⁴⁰
- *Permit Use of Lower Pricing and Other Benefits in Exchange for Consent to Use CPNI.* The record confirms that such offerings are consistent with the statute and with common marketplace practices, and would significantly benefit consumers.²⁴¹
- *Adopt Sensible Data Breach Rules.* Any data breach notification rule the Commission adopts 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 30-60 days after discovery of the breach to send the notification.²⁴²
- *Refrain from Restrictions on Arbitration Clauses.* The record is clear that these provisions benefit both consumers and providers by offering them a less expensive and more convenient means of settling disputes, and that any attempt to restrict them in this proceeding would contravene the Federal Arbitration Act and well-established Supreme Court and other judicial precedent.²⁴³
- *Refrain from Applying the Broadband CPNI Rules to Cable Services.* The Consensus Privacy Framework only applies to ISP services; there is no reason or any legal basis to apply any rules adopted in this proceeding to cable services under Section 631 of the Act,²⁴⁴ and no commenter presented any arguments that would suggest otherwise.

²⁴⁰ See, e.g., T-Mobile Comments at 32-33; Feamster Comments at 4, 7.

²⁴¹ See, e.g., Consumers' Research Comments at 8-10 (explaining that the FCC should allow consumers to choose to offer information about themselves in exchange for something of value); Mobile Future Comments at 7 ("Restricting consumers' ability to voluntarily share information in exchange for benefits, such as financial inducements, would directly contradict one of the Commission's own stated goals in this proceeding: that consumers should have a choice in how their private information is used.").

²⁴² See, e.g., FTC Comments at 32; Consumers' Research Comments at 20-25; CenturyLink Comments at 30-44.

²⁴³ See *supra* § III.D. Comcast Comments at 102-06; Verizon Comments at 70-80; AT&T Comments at 114-15; CTIA Comments at 50-59; Hughes Network Systems at 7-8.

²⁴⁴ Comcast Comments at 106-110; NCTA Comments at 35-38; American Cable Association Comments at 18-19.

V. CONCLUSION

The overwhelming record provides strong evidence that the Commission's initial proposal is unnecessarily onerous and inflexible, and should not be adopted. Instead, the Commission should adopt the Consensus Privacy Framework and otherwise revise its proposed rules consistent with the comments herein and with Comcast's original comments.

Respectfully submitted,

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

Counsel for Comcast Corporation

/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.
Senior Vice President & Deputy General
Counsel, Chief Privacy Officer,
Comcast Cable Communications

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

July 6, 2016