Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

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

REPLY COMMENTS OF CTIA

Thomas C. Power
Senior Vice President and General Counsel

Debbie Matties
Vice President, Privacy

Scott K. Bergmann
Vice President, Regulatory Affairs

CTIA
1400 Sixteenth Street, NW
Suite 600
Washington, DC 20036
(202) 785-0081

July 6, 2016

TABLE OF CONTENTS

INTRODUCTION AND SUMMARY 1

I. THE COMMISSION SHOULD ADOPT MANY OF THE FTC'S SUGGESTIONS. 7

A. Regulating ISPs Under a Different Privacy Framework is "Not Optimal." 7

B. The Commission Should Make the Sensitivity of Data the Touchstone for Its Privacy Rules. 8

C. The Commission Should Exclude From "Customer Proprietary Information" Any Data That Are Not "Reasonably Linkable" to a Consumer. 9

D. The Commission Should Distinguish Expressly Between Harmful and Non-Harmful Uses and Disclosures of Data. 10

E. The Commission Should Eliminate the Strict Liability Data Security Standard. 10

F. The Commission Must Redraft the Data Breach Rules. 11

G. The Gap Between the Proposed Rules and the FTC's Recommendations Compel a Further Notice of Proposed Rulemaking. 12

II. THE COMMISSION DOES NOT HAVE LEGAL AUTHORITY UNDER THE COMMUNICATIONS ACT TO ADOPT THE PROPOSED RULES. 13

A. Section 222 Does Not Permit the Commission to Protect Information Beyond CPNI, Limit the Sharing of Information With Affiliates, or Impose Data Minimization Requirements. 15

1. Public Knowledge's Comparisons to Other Provisions Do Not Support Its Claims that Section 222(a) Provides a Grant of General Authority. 17

2. The 2007 *Pretexting Order* Does Not Hold That CPNI Includes PII. 19

B. Section 222(c) Neither Restricts the Use of De-identified Data Nor Mandates Opt-In Consent. 20

1. Section 222(c) Cannot Be Interpreted to Restrict Uses and Disclosures of De-identified Data. 20

2. Section 222(c) Cannot Be Interpreted to Always Require Opt-In Consent. 24

C. Commenters' Misunderstandings of Section 222(d) Underscore That the NPRM's Interpretation of Section 222 Is Untenable. 25

D. Commenters That Claim That Sections 201 and 202 Support the Proposed Rules or Other Privacy Rules Are Wrong 26

1. Section 222 Supersedes Sections 201 and 202 with Respect to the Protection of Privacy 26

2. There Is an Inadequate Record to Justify the Proposed Rules or the Contemplated Restrictions or Prohibitions in Any Event. 29

E. Virtually No Commenters Advocated Reliance on Section 705 or 706, Because Those Provisions Do Not Support the Proposed Rules or Other Privacy Rules. 30

F. The Arguments of Other Commenters Do Not Justify the Commission's Proposal to Prohibit the Use of Arbitration. 32

1. The Commission Lacks Authority to Prohibit or Regulate Arbitration. 32

2. Arbitration Provides Wireless Consumers a Better Opportunity to Resolve Disputes Than Lawyer-Driven Class Actions 34

a. Arbitration is Beneficial for Consumers. 34

b. The Commission Should Not Prohibit Arbitration In Favor of Lawyer-Driven Class Actions 41

III. COMMENTERS THAT SUPPORT THE NPRM EITHER ENTIRELY IGNORED OR DRASTICALLY UNDERSTATED THE PROPOSED RULES' FIRST AMENDMENT PROBLEMS 43

A. The Proposed Rules Impose Prohibited Speaker-Based and Content-Based Restrictions on Speech and Fail to Satisfy Strict Scrutiny Under *Sorrell*. 44

B. Public Knowledge's Attempt to Preserve the Proposed Rules Under *NCTA v. FCC* Is Based on an Erroneous Analysis That Fails on Its Own Terms in Any Event. 45

1. The Proposed Rules Fail as Applied to Any Use Case That Does Not Involve Disclosure or Dissemination to a Third Party. 46

2. Given Gaps in the Record, the Proposed Rules Also Fail as Applied to Use Cases That Involve Disclosure to Third Parties. 48

IV. THERE IS AN INSUFFICIENT RECORD FOR ADOPTION OF THE PROPOSED RULES. 51

A. ISPs Do Not Possess Unique Capabilities with Respect to the Collection or Use of Consumer Information and Are Constrained by a Robustly Competitive Market. 52

B. Even If ISPs Had Unique Access to Customer Information and Were Quasi-Monopolists, There Still Would Be Inadequate Evidence That They Pose a Unique Privacy Risk. 56

1. There Is an Unstated and Flawed Assumption in Many Comments That Routine Uses and Disclosures of Information, Without More, Constitute Privacy Harm. 57

2. ISPs Lack Incentives, and Often the Technical Infrastructure, to Engage in the "Parade of Horribles" in the NPRM and Supportive Comments. 58

C. There Is No Record Evidence That Customers View ISPs as a Unique Privacy Risk or Otherwise Expect or Prefer Asymmetric Regulation of ISPs. 61

D. The Record Strongly Supports That Any Rules the Commission Adopts Should Reflect Two Fundamental Principles: Data Sensitivity and Flexibility to Adapt Data Practices. 62

V. THE RECORD DOES NOT SUPPORT THE COMMISSION'S OVERLY PRESCRIPTIVE PROPOSED RULES REGARDING NOTICE AND CHOICE. 65

A. The Commission Should Adopt Flexible Notice Rules. 65

B. The Proposed Choice Rules Are Flawed in Design and Should Be Abandoned. 67

C. The Commission Should Reject Public Knowledge's Assertion That Rules Must Treat All Information as Sensitive as a Prophylactic Measure 70

D. The Commission Should Reject Calls for Even More Routine Use of Opt-In Protections and Just-in-Time Notice for Uncontroversial Uses and Disclosures. 72

E. The Commission Should Not Retain Its Proposed Distinction Between Communications-Related and Other Services, But If It Does, It Should Define "Communications-Related" Broadly. 74

F. Despite Some Commenters' Claims, Opt-Out Is a Meaningful Form of Consent That Best Balances Privacy Interests and Costs. 76

G. ISPs' Offers of Service with Financial Inducements or Other Privacy-Related Incentives Are Not Unique and Are in the Public Interest. 78

VI. PROPOSED DATA SECURITY RULES ARE NOT IN THE PUBLIC INTEREST. 80

A. The Record Confirms that the Data Security Proposals Are Deeply Flawed. 80

1. The Commission Proposal Abandons Federal Policy Promoting a Collaborative, Flexible, and Voluntary Approach to Cybersecurity. 80

2. The Record Does Not Reveal a Problem that Justifies Imposing Rigid Security Solutions on ISPs. 82

3. These Data Security Proposals Will Have Negative Consequences. 83

B. The Commission Must Change Its Approach. 85

1. The FTC Agrees the Commission Should Eschew Strict Liability. 85

2. It Is Apparent that the Commission Should Not Treat All Data as Equal. 86

3. Nothing in the Record Justifies the Commission's Unrealistic Approach to Mitigation and Risk Management. 87

4. The Record Is Clear—the Commission Must Avoid Granular Regulation. 88

5. Commenters Confirmed that the Commission Should Not Hold ISPs Accountable for Third-Party Action. 91

6. The Commission Must Not Limit Cybersecurity Information Sharing in Any Way 92

VII. THE COMMISSION SHOULD MODIFY THE PROPOSED DATA BREACH NOTIFICATION RULES 93

A. The Record Supports Tailoring the NPRM's Data Breach Notification Requirements. 94

B. Calls to Broaden the Proposed Notification Obligations Should Be Rejected 97

CONCLUSION 99

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

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

REPLY COMMENTS OF CTIA

CTIA[1] hereby submits its reply comments on the Notice of Proposed Rulemaking ("NPRM") in the above-captioned proceeding.[2]

INTRODUCTION AND SUMMARY

CTIA members are committed to protecting the online privacy and data security of their customers. CTIA likewise appreciates the Commission's interest in establishing rules in these areas, and, along with its members, is participating in this rulemaking process in the hopes of finding consensus around balanced rules that would meaningfully protect customers without jeopardizing the continuing and dynamic growth of the online ecosystem and related markets. Indeed, CTIA members recognize that protecting the privacy and security of customers' data is good business practice, and support the adoption of a technology-neutral regulatory regime, supported by backstop, *ex post* enforcement actions, that preserves flexibility for Internet service providers ("ISPs") to experiment and innovate in not only uses of customer information for

[1] CTIA® (www.ctia.org) represents the U.S. wireless communications industry. With members from wireless carriers and their suppliers to providers and manufacturers of wireless data services and products, the association brings together a dynamic group of companies that enable consumers to lead a 21st century connected life. CTIA members benefit from its vigorous advocacy at all levels of government for policies that foster the continued innovation, investment and economic impact of America's competitive and world-leading mobile ecosystem. The association also coordinates the industry's voluntary best practices and initiatives and convenes the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] *In re Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, 31 FCC Rcd 2500 (2016) ("NPRM"); *see also* Comments of CTIA, WC Docket No. 16-106 (filed May 26, 2016) ("CTIA Opening Comments").

efficient and pro-competitive marketing purposes, but also network management practices, data security responses, and a host of other activities that are in the public interest. From the outset of this proceeding, CTIA and its members have proposed just such a regime, which the NPRM references and is modeled on the Federal Trade Commission's ("FTC's") notice-and-choice framework and unfair and deceptive acts and practices authority,[3] supported by a multistakeholder process led by the Department of Commerce's National Telecommunications and Information Association ("NTIA").[4]

Many commenters in this proceeding made similar recommendations in their opening comments, urging the Commission to adopt rules that mirror the FTC's flexible framework. As these commenters argued, such an approach would provide strong privacy protections while simultaneously ensuring that the Internet remains a dynamic and open environment for the development of innovative new services, offerings, and business models—an outcome that will benefit ISPs, edge providers, and, most importantly, customers.[5]

[3] *See* NPRM ¶¶ 280-282. On March 1, 2016, several trade associations, including CTIA, sent a letter to Commission Chairman Wheeler proposing a privacy framework for the Commission to adopt in this rulemaking proceeding. A copy was attached to CTIA's Opening Comments as Exhibit A.

[4] CTIA Opening Comments at 4. As CTIA noted in its Opening Comments, the Obama Administration established the NTIA-led multistakeholder process in its 2012 privacy report. In that report, the Obama Administration also recommended harmonizing laws governing communications providers by giving the FTC sole authority to enforce the Consumer Privacy Bill of Rights against them. Executive Office of the President of the United States, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[5] *See, e.g.*, Beales Comments at 2 ("The FTC's approach to privacy regulation has worked well. Importantly, it applies a uniform regulatory approach to different technologies and different business models. It has largely avoided creating artificial barriers to either competition or innovation."); Internet Association Comments at 4-5 (arguing that the "FTC's existing data privacy and security enforcement framework provides strong consumer protections" and that the FTC is the "national thought leader and strong enforcement authority" that "has helped define privacy standards for consumers and commercial entities alike"); Mobile Future Comments at 3-7 (discussing NPRM's deviations from FTC's privacy regime and emphasizing FTC's preservation of flexibility to providers); Consumers' Research Comments at 2 ("Rather than adopt prescriptive, ex-ante regulation, the FCC should consider the [FTC's] more flexible approach, which considers consumer harm and cost-benefit analysis."); Wright Comments at 6 ("Rather than imposing a rigid regulatory framework, the FTC focuses on the sensitivity of the data at issue and the potential harm to consumers deriving from disclosure or misuse of that data. In this way, the FTC looks to consumer welfare as its lodestar. FTC enforcements have served to effectively safeguard consumer privacy across

It is especially noteworthy that the FTC itself filed comments which describe the rules proposed in the NPRM (the "Proposed Rules") as "not optimal" and propose a set of specific recommendations as to how the Commission could set aside and modify the Proposed Rules in favor of rules that are more consistent with the FTC's effective approach to privacy protection.[6] In Section I below, CTIA addresses the FTC's recommendations. While the FTC's proposals do not resolve CTIA's statutory or constitutional objections—nor indeed all of CTIA's policy concerns—many of these recommendations would go some distance toward the creation of a consensus, uniform, technology-neutral regime. CTIA therefore urges the Commission to use the FTC's recommendations as a starting point, as discussed below and throughout these reply comments.

It is likewise significant that the Progressive Policy Institute ("PPI") conducted methodologically sound polling that strongly supports the consensus proposal.[7] Specifically, PPI's survey reveals, unsurprisingly, that consumers overwhelmingly expect consistent regulation across the broadband ecosystem—that is, substantively similar regulation of the data practices of ISPs, edge providers, and other entities in the Internet ecosystem—and do not view ISPs as a primary threat to their privacy.[8] As recounted in CTIA's Opening Comments, the Pew Survey results cited in the NPRM are not to the contrary;[9] that consumers generally are concerned about the privacy of their online data has no bearing on the question of whether asymmetric regulation of ISPs is necessary, desirable, or expected. In short, the Pew Survey

---

all industries, providing a welcome degree of predictability and uniformity via a model of regulatory oversight that has allowed the Internet economy to thrive.").

[6] *See, e.g.*, Staff of the Bureau of Consumer Protection of the Federal Trade Commission Comments at 8 ("FTC Comments").

[7] *See generally* PPI Comments.

[8] *See* PPI Comments at 2 ("By an overwhelming margin, [90%-8%,] Internet users strongly agree that all [I]nternet companies should operate under the same set of rules and regulations.").

[9] *See* NPRM ¶ 58 & n.94.

cited in the NPRM, like the similar surveys discussed in several comments supportive of the NPRM, cannot serve as a foundation for the Proposed Rules,[10] and the Commission likewise should be skeptical of conclusory and uncited assertions regarding customer expectations.[11]

In addition to being inconsistent with both the FTC's effective and time-tested privacy regime and customer expectations, the Proposed Rules are flawed along many other axes as well. As CTIA and others explained in their opening comments, the Proposed Rules exceed the Commission's statutory authority. They also violate the First Amendment—and these First Amendment infirmities, even if not fatal on their own (which they are), deprive the Commission of *Chevron* deference.[12] Furthermore, the Proposed Rules are bad policy—in addition to not reflecting customer expectations, they will harm consumers by locking in stagnant business models, resulting in higher prices; they will simultaneously impose substantial costs on ISPs while depriving them of new sources of revenue, thereby threatening future broadband deployment; they will harm competition and innovation;[13] they will result in customer notice fatigue and frustration, given their complexity and the fractured regulatory framework they will create; and they will compromise data security practices that are necessary to prevent online malfeasance.

Many commenters across the ideological spectrum shared these concerns. Indeed, the diversity of commenters with privacy and technology expertise—ranging from current and

[10] *Cf. U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1238-39 (10th Cir. 1999) (finding that the Commission had drawn unsupportable inferences from survey results about customer preferences vis-à-vis uses of customer proprietary network information ("CPNI")).

[11] *See Sorenson Commc'ns, Inc. v. FCC*, 755 F.3d 702, 708-09 (D.C. Cir. 2014) (invalidating final rule where Commission relied on its "predictive judgment" but lacked evidence beyond speculation and failed to provide a satisfactory explanation).

[12] *See* CTIA Opening Comments at 75; Tribe Comments at 8, 38-39.

[13] *See, e.g.*, Moody's Investor Service, *FCC's Broadband Privacy Proposal Credit Negative for Linear TV and Wireless Providers* (Mar. 14, 2016), http://www.netcompetition.org/wp-content/uploads/FCC%E2%80%99s-broadband-privacy-proposal-credit-negative-for-linear-TV-and-wireless-providers.pdf.

former FTC staff and officials, computer scientists, economists, advocacy groups, consumer groups, trade associations, and others, to say nothing of thousands of individual commenters—who identified flaws in the NPRM approach should give the Commission pause.[14]

So too should the lack of support in the record. As CTIA set forth in its Opening Comments, and as many other comments confirmed, ISPs' practices do not present unique or substantial privacy threats to consumers.[15] Here too, the comments of privacy advocates like EPIC and Consumer Watchdog, as well as industry associations, economists, technologists, and others, demonstrate that there is no evidence of unique harm arising from wireless ISPs' use or

[14] *See, e.g.*, FTC Comments at 8 ("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."); Leibowitz Comments at 2-3 (explaining that proposed deviations from FTC's privacy regime will "undercut benefits to the very consumers [the NPRM] seeks to protect"); Beales Comments at 2-3 (discussing shortcomings in the NPRM and emphasizing that there is "*no* evidence of *any* inadequacies" in FTC's privacy regime based on ex post enforcement); Wright Comments at 4 ("[T]he rules, as proposed, are unlikely to further [privacy] principles, and could in fact result in unexpected and unintended consequences, particularly with respect to consumer choice. . . . [T]he proposed rules will likely result in higher prices to consumers, fewer options in the market for broadband services, reduced innovation, and less competition in the market for online advertising."); ITTA Comments at 2 (noting that Proposed Rules are "well-intentioned but ill-considered" as well as "overbroad" and inconsistent with "the time-tested, balanced, and demonstrably effective privacy protection regime created and enforced by the far more experienced FTC" in that they would constitute "new and extremely complex and burdensome rules" that ignore "consumer expectations" and "whether any harm is caused to consumers"); Consumer Technology Association Comments at 7-10 (explaining that proposed Choice Rules and approval framework will deter innovation and hurt consumers).

[15] *See, e.g.*, Consumers' Research Comments at 6-7 (explaining that "[t]he predicate for this action is not a crisis of ISP privacy invasions or abuses"; noting that the NPRM "does not cite any serious injury to consumer privacy by ISP action or inaction"; and noting that there has not been "a sea change in consumer behavior or expectations"); Communications Workers of America Comments at 5 (summarizing categories of edge providers that have comparable access to customer information); Beales Comments at 2-3 ("The FCC offers *no* evidence of *any* inadequacies in [the FTC's] privacy regime. It notes that all of the largest [ISPs] already have publicly available privacy policies, but it makes *no* substantive case at all as to why those policies are inadequate. It identifies no adverse consequences to consumers that have resulted from [ISP] privacy practices. It identifies no privacy problems that have resulted from either accidental or deliberate sharing of information by [ISPs]."); ITIF Comments at 3-6 (discussing increasing limits on ISPs access to information and existing protections available to broadband consumers under privacy policies and threat of backstop enforcement); Yoo Comments at 2-5 (discussing changes in broadband and online advertising markets that undermine the need for prescriptive, asymmetric regulation of ISPs); *cf.* Security and Software Engineering Center at Georgetown University Comments at 2 ("[T]he proposals would benefit from a clearer explanation of the problems that [the NPRM] seeks to prevent. Although we agree that privacy is critically important in the context of Internet telecommunications, it is unclear to what extent [ISPs] have an interest in collecting [proprietary information] and non-CPNI information or providing this information to third parties. A better assessment of the risks—especially when compared to the practices of non-[ISP] edge providers—could help contextualize the regulations and their intentions.").

disclosure of customer information.[16] As some commenters pointed out, in the light most favorable to the Commission, the Proposed Rules appear designed to address what ISPs theoretically might be able to do, and not what they are currently doing, or even realistically are capable of doing.[17] That is no basis for adopting draconian and discriminatory restrictions on a particular set of entities in an open, competitive ecosystem. Instead, to the extent that there is a privacy "gap" for broadband customers, that is all the more reason to adopt the consensus proposal.

Unfortunately, there are commenters in this proceeding who apparently viewed the NPRM as another opportunity to lock ISPs into a business model limited to mere transmission of broadband service. Like the NPRM itself, these commenters relied on untenable readings of the Communications Act generally and Section 222 specifically. They otherwise requested that the Commission engage in a shotgun, results-oriented approach to exercising its statutory authority that is contrary to D.C. Circuit precedent. They applied the wrong constitutional analysis, ignoring or disregarding controlling precedent. And, in some cases, they recommended *even more restrictive rules*, without regard to the absence of evidence that such rules are needed or to the costs that such rules would impose on ISPs and, ultimately, consumers.

In light of the foregoing, CTIA reiterates that the Commission should proceed with caution and deliberation. Given the aggressive schedule that the Commission set at the outset of

[16] EPIC Comments at 4, 15-16 (focusing on how a few companies and large advertising networks are collecting detailed profiles of Internet users, without mentioning ISPs, and criticizing the Commission's "narrow focus in this rulemaking on ISPs" which "misses a significant portion of invasive tracking practices that threaten the privacy of consumers' online communications"); Consumer Watchdog Comments at 3 ("As the Pew results demonstrate, it is not just [ISPs] that prompt people's privacy concerns. It is the entire Internet ecosystem."); *cf.* Consumers' Research Comments at 6-7, 11-13 (urging the Commission to mimic the FTC's light-touch, case-by-case approach that focuses on actual harms to consumers that outweigh the benefits); Beales Comments at 3-8 (finding no theoretical, practical, economic, or record-based justification for asymmetric regulation of ISPs); American Advertising Federation Comments at 3-5 (discussing effectiveness of industry self-regulation because, among other things, ISPs have incentives to adopt and enforce responsible data practices).

[17] *See* Feamster Comments at 6 (explaining that focus on DPI is a "red herring" because it is not widely deployed and prohibitive costs make extensive retention and analysis practically infeasible).

this proceeding, many were surprised that the Commission would attempt to do in a few short months what it took the FTC years to do. Such a results-driven approach is unnecessary and counter-productive—and, indeed, the need for a reset has become more apparent after the opening round of comments, especially in light of the FTC's recommendations. In total, the NPRM has already generated hundreds of thousands of comments that address the Commission's more than 500 questions, and the Commission is obligated to address hundreds if not thousands of those comments to comply with the Administrative Procedure Act ("APA").[18] Moreover, there is no compelling need for the Commission to rush this process; in the interim, the Commission retains the authority to take *ex post* action on a case-by-case basis against providers for violation of the statute, providing a temporary backstop.

I. THE COMMISSION SHOULD ADOPT MANY OF THE FTC'S SUGGESTIONS.

As noted, among the commenters who criticized the Proposed Rules was the FTC itself. While not resolving all of CTIA's concerns regarding the Proposed Rules, the FTC's comments provide the Commission a way forward and toward a consensus approach that could garner support among CTIA's members. Specifically, if the Commission is committed to moving ahead, we urge the Commission to incorporate the following aspects of the FTC's comments.

A. Regulating ISPs Under a Different Privacy Framework is "Not Optimal."

The FTC stated that the Commission's Proposed Rules, if implemented, "would impose a number of specific requirements on the provision of [broadband Internet access] services that would not generally apply to other services that collect and use significant amounts of consumer

[18] *See Int'l Union, United Mine Workers of Am. v. MSHA*, 626 F.3d 84, 94 (D.C. Cir. 2010) (discussing agency's obligation under APA to address significant comments in substantive, rather than conclusory, manner); *Great Lakes Comnet, Inc. v. FCC*, No. 15-1064, --- F.3d ---, 2016 WL 2990926, at *2-3 (D.C. Cir. May 24, 2016) (explaining that Commission's failure to address or explain issues requires remand under APA).

data," and that such an "outcome is not optimal."[19] The FTC has worked for years to regulate data privacy and security under a flexible framework that is technology neutral and applies uniformly and predictably to entities across the Internet ecosystem. Indeed, as the FTC noted in its comments, the FTC has called on Congress to enact data security and privacy laws that would be "applicable to all entities that collect consumer data" because "such generally applicable laws are needed to ensure appropriate protections for consumers' privacy and data security across the marketplace."[20]

B. The Commission Should Make the Sensitivity of Data the Touchstone for Its Privacy Rules.

The Proposed Rules do not draw distinctions based on the sensitivity of data. Indeed, the NPRM proposes adopting a new category of protected information that includes not only CPNI but other data elements, including personally identifiable information ("PII"), which the Commission proposes to define broadly to include any data that is "linkable" to a consumer. As a result of this broad and extra-statutory definition of "customer proprietary information," the Commission would apply the same restrictions and rules regarding notice, choice, data security, and breach notification to an ISP's use or disclosure of a customer's name or address, on the one hand, and a customer's call detail records, precise geolocation information, or health records, on the other. Further, the Proposed Rules regarding customer "choice" apply graduated protections not based on the sensitivity of the underlying information, but instead on the nature of the product or service that an ISP intends to market—a distinction that lacks any nexus to privacy concerns or customer expectations.

[19] FTC Comments at 8.

[20] *Id*.

The FTC wisely urged the Commission to reverse course and—like the FTC itself, the European Union, and numerous federal and state laws—to rely instead on the sensitivity of data in promulgating rules for the uses and disclosures of broadband CPNI.[21] Throughout these Reply Comments, CTIA identifies how the Commission could implement this recommendation.

C. The Commission Should Exclude From "Customer Proprietary Information" Any Data That Are Not "Reasonably Linkable" to a Consumer.

The Proposed Rules apply the same level of restrictions on the uses and disclosures of de-identified PII and CPNI, on the one hand, and the uses and disclosures of individually identifiable information, on the other. In addition to being statutorily foreclosed, as discussed below,[22] this approach is not in the public interest, does not meaningfully enhance customer privacy, creates disincentives for de-identification, and frustrates important uses of de-identified information to promote not only data security, but also emergency response and public health. The Proposed Rules also inappropriately apply the FTC's data de-identification framework to uses and disclosures of aggregate data, which Congress expressly carved out of Section 222's restrictions. As CTIA explained in its Opening Comments, aggregate data, by their very nature, cannot be re-identified, and therefore cannot and should not be subjected to the FTC's test for de-identification.[23] The Commission should heed the FTC's recommendation to modify the Proposed Rules accordingly.[24]

---

[21] *See id*. at 22-23 (recommending that the Commission "consider the FTC's longstanding approach, which calls for the level of choice to be tied to the sensitivity of data and the highly personalized nature of consumers' communications in determining the best way to protect consumers").

[22] *See infra* Part II.A.

[23] *See* CTIA Opening Comments at 35-37.

[24] *See* FTC Comments at 9 (recommending that the definition of PII be modified to include only information that is "reasonably linkable to an individual" (internal quotation marks omitted)).

D. The Commission Should Distinguish Expressly Between Harmful and Non-Harmful Uses and Disclosures of Data.

Because the Proposed Rules are not based on the sensitivity of data, their application would require an ISP to obtain the same level of consent (primarily opt-in) for all but a handful of uses of customer proprietary information. Indeed, an ISP would need opt-in consent except where engaging in certain limited internal operations and the marketing of broadband or other communications-related services (the latter of which would require opt-out consent). This approach runs contrary to consumer expectations and is not aligned with concerns that consumers have about the uses and disclosures of their sensitive data. As the FTC explained in its comments, this approach is misguided from a privacy perspective.[25]

Likewise, the Proposed Rules do not differentiate between the disclosure of, and permitting access to, information, nor do they distinguish between the types of third parties that could receive information via disclosure or access: *i.e.*, independent contractors, joint venture partners, vendors, affiliates, agents, and so forth. Instead, with limited exceptions for activities such as providing the underlying service and initiating, rendering, billing, and collecting for service, the Proposed Rules would require opt-in consent uniformly for any disclosure or access to customer information to virtually any third party. This approach, in addition to being unnecessary to protect consumer privacy, imposes substantial burdens on ISPs, especially for small providers that must rely frequently on vendors.[26]

E. The Commission Should Eliminate the Strict Liability Data Security Standard.

The FTC identified a serious incongruity between the NPRM and the text of the Proposed Rules with respect to data security. Although the NPRM discusses the use of a "reasonableness"

[25] *See id*. at 19-20, 22-23.

[26] FTC Comments at 21-22.

standard, the Proposed Rules actually would impose strict liability on companies for ensuring the security of data.[27] As CTIA and others set forth in Opening Comments—and as the FTC knows from its extensive experience—a strict liability approach is both unrealistic and contrary to the public interest.[28] The Commission should model any data security rules on the FTC's approach, which is to require companies to adopt reasonable data security practices.

F. The Commission Must Redraft the Data Breach Rules.

As CTIA explained in its Opening Comments, the Proposed Rules would require an ISP to notify a customer of a data breach if an employee inadvertently pulled up that customer's name, without more—*i.e.*, without regard to intent, materiality, or harm.[29] In these respects, the Proposed Rules depart unnecessarily from the voice CPNI rules, which include an intent requirement and limit notification to those breaches that pose a risk of harm to consumers. Given these aspects of the Proposed Rules, there is a substantial risk of notice fatigue and confusion, frustrating the very objectives the Commission is purporting to advance. The Commission instead should adopt the FTC's recommendation to narrow the definition of breach and to exclude good-faith actions by employees.[30]

Compounding the above-stated risks is the fact that the Proposed Data Breach Rules encompass the broad category of "customer proprietary information." The FTC urged the Commission to apply these rules instead to a narrower subset of information, explaining that "because the definition [of a breach] includes unauthorized access to *any* customer proprietary

---

[27] *See* FTC Comments at 27-28 ("[T]he proposed rule text would impose strict liability on companies for 'ensuring' security. FTC staff suggests modifying the language to require [ISPs] to 'ensure the *reasonable* security, confidentiality, and integrity of all customer [proprietary information] . . . .'" (ellipsis in original)).

[28] *See* CTIA Opening Comments at 159-61.

[29] *See id.* at 175.

[30] *See* FTC Comments at 32.

information, companies . . . may be required to collect *other* consumer information such as email addresses in order to provide consumers with breach notification."[31] CTIA agrees.

The Proposed Data Breach Rules also establish an artificial, unrealistic, and unnecessarily short deadline for customer notification. This deadline could lead to consumer confusion, if ISPs have to send out follow-up notices to correct missing or inaccurate information in initial, rushed notices. CTIA agrees with the FTC's recommendation that the Commission lengthen the notification period to "between 30 and 60 days after discovery of the breach," as the proposed period is "too short and may not allow companies sufficient time to conduct an investigation."[32]

G. The Gap Between the Proposed Rules and the FTC's Recommendations Compel a Further Notice of Proposed Rulemaking.

From the beginning, this proceeding has been governed by a schedule that does not accurately reflect the substantial and unexpected restrictions proposed in the NPRM. The statement in the *Open Internet Order* that the Commission would initiate a rulemaking to address broadband consumer privacy under Section 222 certainly did not signal that the Commission would propose rules radically departing not just from its existing voice CPNI rules, but also from the FTC's privacy regime that had governed ISP practices to that point[33]—and any such signal would have been overwhelmed by subsequent statements that the Commission intended to harmonize its approach to the FTC's privacy regime.[34]

---

[31] *See id*. at 30-31.

[32] *See id*. at 32-33, 36.

[33] *See Open Internet Order*, 30 FCC Rcd at 5820 ¶ 462.

[34] *See Thomas Mocarsky, FCC and FTC Privacy Turf War Goes Public*, KatyOnTheHill (Aug. 7, 2015), http://katyonthehill.com/fcc-and-ftc-privacy-turf-war-goes-public/ (quoting Chairman Wheeler's testimony that the Commission "work[s] closely with the FTC" and that whatever the Commission does "in next few months" will be based on "best" efforts "to harmonize, so there will be common concepts").

The far-reaching nature of the NPRM generated thousands of comments, many of which identified significant, substantive problems with the Proposed Rules. The FTC's Comments are noteworthy—but by no means unique—in this regard. If the Commission finds the FTC's recommendations persuasive, that would be a promising step toward developing consensus rules regarding consumer privacy and data security. But the Commission nonetheless must first adopt a Further Notice of Proposed Rulemaking. Doing so would ensure that the FTC's proposals receive a full review by commenters, which, in turn, will ensure that any final rules reflect a reasonable exercise of agency prerogative.

II. THE COMMISSION DOES NOT HAVE LEGAL AUTHORITY UNDER THE COMMUNICATIONS ACT TO ADOPT THE PROPOSED RULES.

As CTIA and numerous other commenters explained, the Proposed Rules exceed the Commission's statutory authority in a variety of ways.[35] As CTIA set forth in its Opening Comments, the text and legislative history (including the legislative history of amendments to Section 222), as well as prior Commission practice, demonstrate that even if broadband service can be regulated as a telecommunications service for purposes of Title II *generally*, Section 222 specifically governs only voice services.[36] Section 222 is replete with references to telephony and voice, and mentions Internet service only insofar as the provision applies to non-traditional VoIP service. Indeed, the fact that Congress had to amend Section 222 to extend it to VoIP

[35] *See, e.g.*, CTIA Opening Comments at 15-50; NCTA Comments at 7-19 (discussing statutory authority under Section 222); Verizon Comments at 53-60 (arguing that Section 222's text, structure, and legislative history, as well as Congress's consistent use of alternative phrasings in other privacy statutes unambiguously foreclose recourse to Section 222(a) in support of Proposed Rules); AT&T Comments at 100-108 (arguing absence of statutory authority under Section 222 and other sections of the Communications Act); Sprint Comments at 5-8 (discussing scope of Commission's authority under Section 222) T-Mobile Comments at 25-37 (discussing statutory authority under Section 222); Comcast Comments at 66-75; ITTA Comments at 3-11; American Advertising Federation Comments at 5-6. Moreover, there remains significant legal uncertainly around the reclassification of broadband service as a telecommunications service under Title II of the Communications Act, notwithstanding the D.C. Circuit's recent decision in *U.S. Telecom Ass'n v. FCC*, No. 15-1063, ---F.3d---, 2016 WL 3251234 (D.C. Cir. June 14, 2016). If the courts ultimately reject Title II reclassification, the Commission could not apply Section 222 ISPs' provision of broadband service. *See* CTIA Opening Comments at 15.

[36] *See id*. at 16-22.

service demonstrates that the Commission otherwise unambiguously lacked the authority to extend Section 222 beyond traditional voice service. And the Commission's determination in the *Open Internet Order* not to apply the voice CPNI rules to the provision of broadband service is a classic example of proving too much: the Commission based its forbearance of the voice CPNI rules on differences between the broadband and voice markets—differences that reflect the inappropriateness of applying not just the Commission's voice CPNI rules, but also Section 222 itself, to ISPs.[37] So far as CTIA is aware, no commenter in this proceeding argued otherwise.

Even if this *second*, *separate* threshold obstacle could be overcome, Section 222 nonetheless unambiguously forecloses the Proposed Rules in a variety of ways—insofar as they (1) purport to protect information beyond CPNI; (2) impose restrictions on the use of de-identified data; (3) define CPNI to include elements of voice services data that have no corollary in the broadband context; (4) prohibit certain practices involving data, even when an ISP obtains customer approval; and (5) impose restrictions on ISPs' use and disclosure of information obtained other than by providing service.[38] Commenters that support the NPRM addressed some of these arguments, but ultimately failed to identify a permissible, coherent interpretation of Section 222, 201, 202, 705, or 706 that would authorize the Commission to adopt the Proposed Rules or the other contemplated restrictions and prohibitions in the NPRM.[39]

[37] *See id*. at 23.

[38] *See* CTIA Opening Comments at 25-49. CTIA does not repeat each of these arguments herein, because many were not addressed by other commenters in the opening comments period. But CTIA reserves each argument, including that the Commission lacks authority to restrict the use or disclosure of information that ISPs obtain other than by providing service.

[39] *See id*. at 60-71.

A. Section 222 Does Not Permit the Commission to Protect Information Beyond CPNI, Limit the Sharing of Information With Affiliates, or Impose Data Minimization Requirements.

Although certain comments offer tortured interpretations of Section 222(a) in support of the Commission's authority to protect additional information,[40] there can be no doubt that Section 222(a) cannot stretch the Commission's reach beyond CPNI. In addition to failing even to address the threshold questions of whether broadband can be classified as a telecommunications service and whether, if it can be so classified, Section 222 is limited to voice service in any event, the proffered readings of Section 222(a) contravene basic principles of statutory interpretation and the legislative history of the 1996 Act.

CTIA and others made clear in their opening comments that the text, legislative history, and structure of Section 222 all compel the conclusion that CPNI is the only customer information that Congress intended to protect.[41] None of the comments that make assertions to the contrary genuinely dispute that the Commission lacks authority to expand the scope of information covered by Section 222. In fact, commenters supportive of the NPRM failed to clearly articulate an argument that Section 222(a) gives the Commission authority to adopt rules that cover customer information beyond CPNI despite this question having been fully developed in response to CTIA's Lifeline Petition for Partial Reconsideration.[42]

---

[40] *See, e.g.*, Center for Democracy and Technology Comments at 11-12 (relying on Section 222(a) to support rules protecting information beyond CPNI); Free Press Comments at 8-10 (similar); EFF Comments at 2 (similar); Public Knowledge, *Protecting Privacy, Promoting Competition* 15-16 (*PK Thinks White Paper* Feb. 16, 2016), https://www.publicknowledge.org/assets/uploads/blog/article-cpni-whitepaper(1).pdf ("*PK White Paper*").

[41] *See* CTIA Opening Comments at 25-35 (explaining that the text and structure of Section 222 as well as legislative history unambiguously foreclose reliance on Section 222(a) to protect information other than CPNI); *see also* AT&T Comments at 103-108; Verizon Comments at 53-60; T-Mobile Comments at 18-19; ITTA Comments at 3-10.

[42] CTIA Reply Comments to Opposition to CTIA's Petition for Partial Reconsideration, *In re Lifeline and Link Up Reform and Modernization, Telecommunications Carriers Eligible for Universal Service Support, Connect America Fund*, WC Docket Nos. 11-42, 09-197, 10-90 (Oct. 19, 2015), at 6-8.

Although Public Knowledge at least attempted the traditional motions of statutory interpretation,[43] it nonetheless failed to establish that the Commission can regulate customer information beyond CPNI. Public Knowledge's reliance on the congressional Conference Report to suggest that Section 222(a) contains a broad grant of general rulemaking authority, in particular, misses the mark.[44] Arguing that the shift in the statute's title from "Privacy of Customer Proprietary Network Information" to "Privacy of Customer Information" somehow "dramatically expand[ed] the *general* duty of carriers to protect customer information" and thus the Commission's privacy authority, Public Knowledge attempted to gloss over Congress's decision to limit the customer information to which the final bill applied to the specific categories listed in Section 222(h).[45] Public Knowledge also failed to even acknowledge that Congress declined to include in the enacted statute the open-ended categories of information that had appeared in prior versions and could have potentially stretched beyond CPNI.[46] As CTIA and others explained in their comments, this legislative history unambiguously shows that Congress did not intend to provide the Commission with unbounded authority to regulate carriers' privacy practices under Section 222(a).[47]

In addition, despite Public Knowledge's attempt to construct an argument to the contrary, Section 222(b) cannot be interpreted to limit access to or the use of information by an affiliate of a telecommunications carrier that provides other services. In its "White Paper" on broadband privacy and comments in this proceeding, Public Knowledge invoked Section 222(b) to hint at a

[43] *PK White Paper* at 9-19.

[44] *PK White Paper* at 15-16; *accord* Center for Democracy and Technology Comments at 11 (discussing 1996 Conference Report as support for proposition that Section 222(a) protects more than CPNI).

[45] *See PK White Paper* at 15.

[46] *See id.*

[47] *See* CTIA Opening Comments at 28-29; *see also* Verizon Comments at 55; ITTA Comments at 6-7.

variety of arguments about competition and the relationship between ISPs and their broadband affiliates.[48] However, Public Knowledge never offered more than a nebulous request that the Commission consider Section 222(b)—without explaining how it relates to any of the proposed rules or alternatives in the NPRM.[49] If the Commission intends to rely on Section 222(b), it must issue a further NPRM, as commenters have not had an adequate opportunity to address this provision, notwithstanding Public Knowledge's tenuous and incomplete analysis. To act otherwise would only encourage sandbagging in a proceeding that has already generated hundreds of thousands of comments.

Finally, the Commission does not have authority to mandate data minimization for ISPs. Indeed, neither Section 222 nor any of the other sources of potential authority that commenters cite provides a legal basis for a data minimization requirement.[50]

1. Public Knowledge's Comparisons to Other Provisions Do Not Support Its Claims that Section 222(a) Provides a Grant of General Authority.

Public Knowledge's argument that Section 222(a) provides a large grant of regulatory authority to the Commission is not bolstered by its citation of statutory provisions in other parts of the communications laws that purportedly contain a broadly interpreted "general duty"

[48] *PK White Paper* at 6, 13, 67.

[49] Public Knowledge Comments at 34.

[50] The Electronic Frontier Foundation argued that the Commission may impose data minimization requirements under its general authority in Section 222(a). EFF Comments at 7. However, unlike the Cable Communications Privacy Act, which expressly requires data destruction under 47 U.S.C. § 551(e), and the Satellite Privacy Act, which does the same under 47 U.S.C. § 338(i)(6), Section 222 does not expressly mandate that carriers destroy customer data. Section 222 is therefore not a basis for authority. The other sources commenters cited similarly do not give the Commission such authority. Specifically, none of the draft "Consumer Privacy Bill of Rights Act," which is proposed legislation—not an enacted law—voluntary data minimization guidance from the National Institute for Standards and Technology, the Fair and Accurate Credit Transactions Act, or various state laws give the Commission authority to promulgate data minimization rules. *See* EPIC Comments at 10 (urging the Commission to rely on the proposed Consumer Privacy Bill of Rights Act); Farsight Security Comments at 24 (urging the Commission to rely on NIST guidance); FTC Comments at 28 (urging the Commission to model rules on the data minimization requirements under the Fair and Accurate Transactions Act); NCL Comments at 13 (urging the Commission to look to state data minimization laws).

followed by subsequent specific instructions.[51] Specifically, Public Knowledge claimed that the later subsections of Section 222 do not limit the purportedly expansive authority of Section 222(a) to CPNI but merely prescribe additional, CPNI-specific responsibilities. Public Knowledge overreached to find examples of supposedly similar provisions, however.[52]

Indeed, the structure of Section 222 differs significantly from the cited provisions. Unlike Section 222, none of Section 628, or provisions of the Cable Television Consumer Protection and Competition Act of 1992 the statutory authority on which Public Knowledge relied for support, define in their subsequent subsections the duties *of different regulated entities* identified in their initial subsections.[53] And, unlike Section 222, these other provisions are not rendered internally incoherent when the "general duty" provision is interpreted as a broad, separate grant of authority. For instance, reading 47 U.S.C. § 225(b) as a separate grant of general authority to ensure the availability of relay services for the deaf is perfectly consistent with § 225(d)'s requirement that particular regulations be immediately enacted to implement that grant of general authority. Public Knowledge's interpretation of Section 222, by contrast, leads to patently absurd results that cannot reflect congressional intent.[54]

---

[51] *See PK White Paper* at 17-19.

[52] *Id*.

[53] *Compare* Section 222(c) (setting forth specific application of 222(a)'s mandate to customers as opposed to other entities enumerated in Section 222(a)), *with* Cable Television Consumer Protection and Competition Act of 1992 § 628(b), 47 U.S.C. § 548 (setting forth particular regulations the Commission shall impose with regard to deceptive practices by networks affiliated with cable operators in addition to general prohibition on deceptive practices), 47 U.S.C. § 225(c)-(d) (setting forth particular regulations the Commission shall impose with regard to telecommunications relay services in addition to general duty to ensure relay service availability), *and* 47 U.S.C. § 251(b)-(c) (setting forth particular interconnection responsibilities of local exchange carriers *in addition* to general interconnection duties proscribed by § 251(a)).

[54] CTIA Opening Comments at 27-28 (explaining how reading Section 222(a) as an independent requirement would effectively negate requirements imposed by subsections (e) and (g), and render the exceptions listed in subsection (d) applicable to CPNI while purportedly regulated information beyond CPNI could not be disclosed in, among other situations, emergencies involving first responders).

Finally, prior Commission precedent and practice clearly contradict any theory, like the one propounded by Public Knowledge, that Section 222(a) provides an independent grant of authority. Although the Commission is not bound by prior interpretations, an agency's discovery of novel, expansive powers hidden in established statutory provisions is understandably viewed with significant skepticism.[55]

2. The 2007 *Pretexting Order* Does Not Hold That CPNI Includes PII.

Public Knowledge also mistakenly argued that the Commission conclusively determined, in its *Pretexting Order*, that CPNI includes PII.[56] The gymnastics Public Knowledge performed to make this argument illustrate the general weakness of its Section 222(a) arguments (and of similar arguments made in other comments). While claiming that the statement in the *Pretexting Order* that "CPNI includes personally identifiable information derived from a customer's relationship with a provider of communications services" is the "conclusion" and "central basis upon which the rest of the [Pretexting] [O]rder rested," Public Knowledge simultaneously admitted, as it had to, that this statement was placed "in a footnote."[57] Just as Congress does not hide elephants in mouseholes,[58] the Commission knows better than to hide a "conclusion" whose "rationale provides the very basis for the decision" in a footnote.[59]

Moreover, Public Knowledge failed to provide authority or even an explanation for its assertion that this statement was the holding—or was essential to the holding—of the *Pretexting*

[55] CTIA Opening Comments at 62 n.191 (citing relevant case law); Verizon Comments at 56.

[56] Public Knowledge Comments at 27-28.

[57] *Id*. at 27.

[58] *See Whitman v. American Trucking Ass'ns*, 531 U.S. 457, 468 (2001).

[59] *See Davis Broad. Inc. v. FCC*, 63 F. App'x 526, 527 (D.C. Cir. 2003) ("As the FCC correctly notes, however, Davis' opening brief offers only a perfunctory argument on this issue in a footnote, and we should therefore consider the argument waived.").

Order.[60] That is because there is no support for such a bizarre interpretation of the *Pretexting Order*. Indeed, in its Opening Comments, CTIA demonstrated the fallacy of this line of argument. As CTIA explained, far from supporting the Commission's authority under Section 222(a), the *Pretexting Order*'s reference to CPNI as including certain "personal customer information" does not establish that *all* PII is CPNI, but only that such personal information renders CPNI "individually identifiable."[61]

B. Section 222(c) Neither Restricts the Use of De-identified Data Nor Mandates Opt-In Consent.

The Commission also should reject the arguments that (1) Section 222(c) can be interpreted to restrict the use of de-identified data,[62] and (2) Section 222(c)'s use of "approval" requires prior opt-in consent.[63]

1. Section 222(c) Cannot Be Interpreted to Restrict Uses and Disclosures of De-identified Data.

Section 222(c)(1) unambiguously regulates only "individually identifiable" CPNI. As CTIA and others explained in their comments, de-identified data are not "individually identifiable" CPNI and the protections of Section 222(c)(1) do not apply to those data.[64] The

---

[60] *See* Public Knowledge Comments at 27-28.

[61] *See* CTIA Opening Comments at 30-31.

[62] *See* New America OTI Comments at 21-22, 27-28 (urging the Commission to adopt a definition of "customer proprietary information" that is open and reflects ease of re-identification and claiming that Section 222 does not reserve to ISPs the right to use aggregate PII); EFF Comments at 14-16 (urging stringent requirements related to anonymization and aggregate data and concluding that "de-identified but non-collective data do[] not fall under the exception for use and disclosure of aggregate customer data enumerated in § 222(c)(3) . . . because such data [are] not collective"); Access Now Comments at 11 (discussing risks of re-identification and "welcom[ing] the FCC approach to protect the aggregated [customer proprietary information]").

[63] *See* Public Knowledge Comments at 31 (suggesting that "approval of the customer" should be defined to "require affirmative opt-in consent"); New America OTI Comments at 39 (arguing that "plain meaning" of "approval" is to "require some active consent").

[64] *See* CTIA Opening Comments at 35-43; T-Mobile Comments at 34-37; *see also In re Implementation of the Telecommunications Act of 1996, Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14,409, 14,413 ¶ 4 (1999) ("Where information *is not specific to the customers* . . . section 222 permits the free flow or

Commission's proposed approach to de-identified data thus exceeds the scope of its authority under Section 222(c), and is inconsistent with the approach taken by the FTC, National Institute of Standards and Technology ("NIST"), and various other entities with privacy expertise, who have attempted to create a balanced standard based on a principle of "reasonability."[65]

CTIA appreciates the comments of the FTC suggesting that the Commission adopt a "reasonable linkability" standard, particularly insofar as it could allow uses of de-identified data that are in the public interest.[66] The FTC's caution that considering any data that are "linkable" as PII could "unnecessarily limit the use of data that do[] not pose a risk to consumers. While almost any piece of data *could* be linked to a consumer, it is appropriate to consider whether such a link is practical or likely in light of current technology."[67]

The FTC, like the NPRM, also appropriately took the position that linkability to a device can be, but is not necessarily always, tantamount to linkability to an individual.[68] The FTC explained that certain devices, such as mobile handsets, "are extremely personal, almost always on, and almost always with the user."[69] However, there are other "non-personal" devices that should not be considered "reasonably linkable" to an individual, particularly amongst the emerging generation of "Internet of Things" ("IoT") devices, "such as an autonomous ride-sharing vehicle that can be summoned by any member of the public."[70] The Commission should

---

dissemination of information beyond the existing customer-carrier relationship." (emphasis added)) ("*1999 CPNI Order*").

[65] *See, e.g.*, State Privacy and Security Coalition Comments at 5 (encouraging the Commission to revise its definition of "de-identified" data to match that of the FTC).

[66] FTC Comments at 10.

[67] *Id*. at 9.

[68] *Id*. at 10.

[69] *Id*. at 10 n.36.

[70] *Id*.

confirm that it will adhere to this sort of case-by-case approach with regard to data linkable to a device.

A flexible approach to linkability is particularly important given that, as the record reflects, de-identification is in the public interest. Numerous commenters observed that there are substantial public benefits to de-identification.[71] For instance, using de-identified data provides the ability to monitor and improve traffic patterns and disaster recovery efforts.[72] It makes significant contributions to health research and allows researchers to slow contagion of infectious diseases.[73] It creates economic value by providing information that businesses can use to improve their services and to offer their customers innovative products that meet their needs.[74] Moreover, de-identification accords with consumer preferences and expectations about how data can and should be used.[75]

The commenters urging the Commission to restrict the use and disclosure of even de-identified data overstated the ease of re-identification, asserting that "de-identified data can often be re-identified"[76] and that data can merely be "cross-referenced" with other sources to re-

[71] *See, e.g.*, Future of Privacy Forum Comments at 3-7 (discussing spectrum of data and that reasonable de-identification is in the public interest, including with respect to facilitating competition in the market for online advertising); T-Mobile Comments at 36 (discussing public interest benefits of de-identification, including with respect to privacy and security, public health, disaster recovery, and socio-economic conditions); Consumers' Research Comments at 22-24 (discussing privacy and security benefits of de-identification as recognized in multiple consumer privacy regimes); IMS Health Comments at 3 (discussing how de-identification permits use of "big data" in the healthcare context in a way that "offers real value for patients by improving quality, safety, value and outcomes"); CTIA Opening Comments at 42-43.

[72] T-Mobile Comments at 36.

[73] T-Mobile Comments at 36; *see also* IMS Health Comments at 3.

[74] Consumers' Research Comments at 23.

[75] Consumers' Research Comments at 22 (de-identification "overwhelmingly benefits consumers" and is a practice "that consumers tend to prefer") & 22 n.100 (consumer studies show that consumers think "that de-identified data holds a different status to identifiable data and should be used without specific consent in research that aims to benefit society"); *see infra* Part IV.B.2 (discussing the data security benefits of de-identifying data).

[76] New America OTI Comments at 21.

identify a particular consumer.[77] However, research reflects that de-identification is highly effective when executed correctly and that re-identification is a complex process requiring both an alternative data source and a highly skilled expert to have any chance of success.[78]

Comments arguing that ISPs should publicly disclose their de-identification protocols and administrative controls, or reveal them to researchers for independent testing, mistakenly assume that ISPs will make only minimal de-identification efforts absent public scrutiny.[79] In fact, as the record in this proceeding makes abundantly clear, ISPs care deeply about the security of their customers' information and go to great lengths to respect their choices with regard to information-sharing.[80] Moreover, these commenters ignore that the Commission's approach to de-identification conflicts with the approach taken by the FTC, NIST, and other entities with privacy expertise.[81] In particular, there is an important distinction between making data publicly available, on the one hand, and sharing data exclusively with known individuals or entities in a controlled environment, on the other. Although administrative controls cannot keep publicly disclosed de-identified data from being re-identified, the combination of appropriate technical protocols and administrative controls recommended by the FTC can ensure that data will be

[77] Access Now Comments at 11; *see also* Privacy Rights Clearinghouse Comments at 5 (asserting that "seemingly singular, non-identifying data points" can be combined to identify individuals).

[78] *See* Ann Cavoukian & Daniel Castro, *Big Data and Innovation, Setting the Record Straight: De-identification* Does *Work*, 4, 5-6 (June 16, 2014), http://www2.itif.org/2014-big-data-deidentification.pdf (explaining that "[r]e-identification is only possible if there is an alternative data source" and that it "requires the knowledge of a highly trained, highly skilled 'expert' in the field," and noting that research shows de-identification is highly effective if appropriate methods are used); FPF Comments at 6 (noting "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").

[79] EFF Comments at 14-15 ("If BIAS providers are *not* required to disclose the methods they use to generate aggregate CPI…the lack of public scrutiny will inevitably lead to the use of weak aggregation methods instead."); FPF Comments at 3-6 (describing the various ways in which online advertising companies can and do de-identify data under self-regulatory frameworks).

[80] *See*, *e.g.*, CTIA Opening Comments at 107-19, 158-75.

[81] *See*, *e.g.*, *id*. at 37-43; State Privacy and Security Coalition Comments at 5; SPSC Comments at 5.

maintained in de-identified form when shared in a controlled environment.[82] The Commission should draw on the extensive work done by those entities in establishing privacy frameworks that embrace the benefits of de-identification and avoid consumer harm.[83]

2. Section 222(c) Cannot Be Interpreted to Always Require Opt-In Consent.

The Commission cannot construe the term "approval" in Section 222(c)(1) to require affirmative, opt-in consent for all uses and disclosures of CPNI, other than those necessary to provide the service or as permitted under the exceptions in Section 222(d).[84] First and foremost, multiple appellate decisions have confirmed that the word "approval" is ambiguous as to the level of consent required.[85] It is also clear that when Congress wants to mandate affirmative approval, it knows how to accomplish that goal. For instance, in Section 222(f)(1), Congress used the phrase "express prior authorization" to make clear that it intended carriers to obtain opt-in consent from consumers before utilizing certain call location information. Moreover, the Commission must consider that interpreting "approval" in Section 222(c) to require opt-in consent would signal that the voice CPNI rules of the past two decades have been unlawful

[82] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012) at 2 ("*FTC Report*"), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (stating that FTC will consider data to be "de-identified" when (1) the data is no longer reasonably linkable to a particular individual, (2) the company holding the data has publicly committed not to re-identify the data, and (3) the company requires third parties to which it discloses the data to keep the data in de-identified form); *see also* AT&T Comments at 67, 70 (noting the FTC's test for data de-identification and urging the Commission to follow the FTC's approach); CenturyLink Comments at 17-18 (urging the Commission to adopt a test for data de-identification that is consistent with the FTC's test); T-Mobile Comments at 35-36 (same).

[83] *See, e.g.*, Mobile Future Comments at 2, 7 (noting that inconsistent regulatory regimes stifle competition and create consumer confusion).

[84] *See* Public Knowledge Comments at 31; New America OTI Comments at 39.

[85] *See U.S. West, Inc.*, 182 F.3d at 1238 (finding opt-in requirement was not appropriately tailored because the Commission could have interpreted "approval" to require only opt-out consent); *id.* at 1240 (Briscoe, J., dissenting) (agreeing that Section 222 is ambiguous with respect to level of approval required); *cf. Nat'l Cable & Telecomms. Ass'n v. FCC*, 555 F.3d 996, 1002 (D.C. Cir. 2009) (acknowledging, for purposes of evaluating the tailoring of implementing regulations under First Amendment analysis, that "approval" could require opt-in or opt-out consent).

insofar as they operate, in part, on implied, and opt-out consent.[86] Finally, for the reasons explained below, interpreting Section 222(c) to require affirmative consent would fail as a constitutional matter.

C. Commenters' Misunderstandings of Section 222(d) Underscore That the NPRM's Interpretation of Section 222 Is Untenable.

Certain parties argued that the Commission cannot extend the exceptions enumerated in Section 222(d) to any "customer proprietary information" beyond CPNI, asserting that because Section 222(d) explicitly references only CPNI, these exceptions cannot apply to any broader category of information.[87] Although the effect is unintentional, this argument forcefully illustrates the unsound nature of the NPRM's interpretation of Section 222.

As CTIA and others noted in their opening comments, Section 222(d)'s reference to CPNI, and only CPNI, shows that Congress intended Section 222 to apply only to CPNI with respect to *customers'* information.[88] To construe the statute otherwise creates patently absurd results—for instance, by defining "customer proprietary information" broadly under Section 222(a), but excluding all such information other than CPNI from the disclosure exceptions under Section 222(d), carriers would be permitted to share CPNI with emergency responders in a life-threatening situation, but could not disclose anything considered "customer proprietary information" under the NPRM, such as the names of other individuals associated with the

---

[86] *See In re Implementation of the Telecommunications Act of 1996*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8080 ¶ 23 (1998) ("We believe that the language of section 222(c)(1)(A) and (B) reflects Congress' judgment that customer approval for carriers to use, disclose, and permit access to CPNI can be *inferred* in the context of an existing customer-carrier relationship. This is so because the customer is aware that its carrier has access to CPNI and, through subscriptions to the carrier's service, has implicitly approved the carrier's use of CPNI within that existing relationship.").

[87] *See* EFF Comments at 8 ("We also disagree with the Commission's proposal to interpret the statutory exception in [Sections] 222(c) and (d) to include any customer [proprietary information], and not only CPNI." (internal quotation marks omitted)); New America OTI Comments at 38-39 (arguing that the Commission should not extend statutory exceptions to cover customer proprietary information other than CPNI); *cf.* Access Now Comments at 7 (urging strict and narrower rules implementing Section 222(d) exceptions).

[88] *See, e.g.*, CTIA Opening Comments at 28.

account.[89] This result is utterly contrary to public policy and common sense and cannot reflect Congress' intent in enacting Section 222.[90]

D. Commenters That Claim That Sections 201 and 202 Support the Proposed Rules or Other Privacy Rules Are Wrong.

Perhaps recognizing that Section 222 unambiguously forecloses the Proposed Rules, several commenters instead argued that Sections 201 and 202 of the Communications Act provided purported primary or supplemental authority for the Commission to adopt the Proposed Rules or other contemplated restrictions and prohibitions.[91] This move fails for two reasons: Section 222 supersedes Sections 201 and 202 with respect to privacy issues, and the record is inadequate to support data privacy rules under either Section 201 or Section 202.[92]

1. Section 222 Supersedes Sections 201 and 202 with Respect to the Protection of Privacy.

The Commission has appropriately recognized that this is a Section 222 proceeding.[93] This conclusion necessarily follows from both the legislative history of the 1996 Act and settled

---

[89] *See id*.

[90] *See id*. at 28 n.60 (citing case law regarding statutory interpretation canon against absurdity).

[91] *See, e.g.*, Center for Democracy and Technology Comments at 25 ("The Commission should draw upon [Section 201] to put rules in place that will restrict pay-for-privacy programs if [an ISP] is not transparent about the program or inflates service prices to essentially coerce the customer into accepting a discount in exchange for opting in to data sharing."); Free Press Comments at 14-17 (arguing that Sections 201 and 202 augment Commission's authority to adopt prescriptive rules regarding privacy and asserting that "[i]t is entirely conceivable than [sic] an ISP might mislead consumers, or engage in other practices implicating their privacy rights, yet [] not expressly violate the restrictions in Section 222 . . . ."); New America OTI Comments at 12 (arguing that a Section 201 "inquiry could, for example, find that [ISPs'] 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").

[92] *See, e.g.*, CTIA Opening Comments at 60-63; NCTA Comments at 25 ("Because Congress enacted a comprehensive privacy regime under Section 222, Section 201(b) cannot serve as an independent source of authority for the Commission to impose privacy protections on ISPs subject to Title II."); Comcast Comments at 68-70 (describing that "Section 222 represents the *maximum* privacy authority the Commission has under the Act" to the exclusion of other provisions including Section 201(b).

[93] In recent testimony before the Senate Judiciary Committee, Chairman Wheeler explained that the Commission is "doing this under Section 222." *See* Tom Wheeler, Testimony Before the Subcomm. on Privacy, Technology, and the Law of the S. Comm. on the Judiciary, *Examining the Proposed FCC Privacy Rules* at 54:44 -55:10 (May 11, 2016), http://www.judiciary.senate.gov/meetings/examining-the-proposed-fcc-privacy-rules.

principles of statutory interpretation. There can be no other legislative font for the Proposed Rules or the other contemplated restrictions and prohibitions, because Congress expressed its clear intent in the 1996 Act to "balance both competitive and consumer privacy interests with respect to *CPNI*" in the market for telephone voice services,[94] and Section 222 reflects that balance. Moreover, as the Commission has previously acknowledged, it is a settled principle of statutory interpretation that general provisions of a statute cannot trump more specific requirements and permissions contained in the same statute.[95] In short, any authority that the Commission has with respect to customer privacy rests exclusively in Section 222.[96]

Equally important, because Section 222 is the exclusive provision balancing the competing interests in privacy and competition, the Commission lacks *any* authority to regulate ISP practices that are not covered by Section 222 but that relate to customer privacy. The NPRM and commenters' discussions of deep packet inspection ("DPI") and persistent tracking therefore wholly miss the mark.[97] Insofar as the Commission believes that DPI and persistent tracking implicate customers' privacy interests, the only tool available to the Commission to regulate those practices is Section 222. But DPI and persistent tracking themselves do not involve the use, disclosure, or access to customer information—*i.e.*, the only practices addressed in Section

[94] H.R. Rep. No. 104-458, at 205 (1996) (Conf. Rep.) (Joint Explanatory Statement of the Committee of Conference) (emphasis added).

[95] *See Open Internet Order*, 30 FCC Rcd at 5822 ¶ 465 & n.1392.

[96] *See 1999 CPNI Order*, 14 FCC Rcd at 14,491 ¶ 153 ("We conclude that the specific consumer privacy and consumer choice protections established in section 222 supersede the general protections identified in sections 201(b) and 202(a).").

[97] *See, e.g.*, Public Knowledge Comments at 24-25 (arguing that DPI must be prohibited under any meaningful consent regime); Center for Digital Democracy Comments at 21 ("We urge the [C]ommission to prohibit the use of [DPI] as proposed. DPI will provide [ISPs] with an unfair advantage for the creation of consumer data profiles, and such intrusive practices are unacceptable."); EFF Comments at 10 ("[A]s part of its general duty to protect customer [proprietary information], the FCC should find that carriers must refrain from utilizing [DPI] of content that exceeds what is required of them to provide telecommunications service."); Online Trust Alliance Comments at 5 (similar); Access Now Comments at 15 (similar).

222.[98] Instead, they facilitate the *collection* of information, and Section 222 does not impose any restrictions on collection. The fact that Section 222 does not cover collection does not mean that the Commission can look elsewhere in the Communications Act to regulate collection practices; it means that Congress did not intend for those practices to be restricted at all, and, accordingly, that the Commission lacks authority to regulate DPI or persistent tracking—or any other kind of information collection.

The tension between the commenters' urged use of Sections 201 and 202 to restrict or prohibit DPI and persistent tracking, on the one hand, and the text of Section 222, on the other hand, is not merely abstract. With one exception, commenters conveniently ignored that Section 222 expressly reserves to carriers the right to use, disclose, and permit access to customer information "with the approval of the customer."[99] These commenters either would interpret this savings clause entirely out of Section 222(c)(1) or would interpret Sections 201 and 202 to prohibit that which Section 222 expressly allows; neither is permissible.[100] The only commenter that addressed this tension is Public Knowledge, which creatively claimed that DPI cannot be consented to, insofar as it involves collecting information from third parties involved in online interactions, which third parties do not have the opportunity to provide consent.[101] But the fact that DPI may reveal information about a third party is a concern that is entirely outside the scope

[98] *See* 47 U.S.C. § 222(c)(1).

[99] *See id.*; *see also* CTIA Opening Comments at 45-48.

[100] *See TRW Inc. v. Andrews*, 534 U.S. 19, 31 (2001) ("It is a cardinal principle of statutory construction that a statute ought, upon the whole, to be construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant." (internal quotation marks omitted)); *Sec. Indus. Ass'n v. Bd. of Gov. of Fed. Reserve Sys.*, 807 F.2d 1052, 1057 (D.C. Cir. 1986) ("[S]ection 21 cannot be read to prohibit what section 16 permits.").

[101] *See* Public Knowledge Comments at 25.

of Section 222: insofar as the third party is not a customer of the ISP, its information is neither "customer"-related nor "proprietary" to that ISP and therefore does not fall under Section 222.[102]

2. There Is an Inadequate Record to Justify the Proposed Rules or the Contemplated Restrictions or Prohibitions in Any Event.

The adoption of rules under Sections 201 and 202 must be supported by substantial evidence and must be reasonable.[103] While this standard of review allows for the Commission to make predictive judgments, it does not permit the Commission to adopt solutions in want of problems. Accordingly, even if the Commission could permissibly adopt rules to protect customer privacy under Sections 201 and 202, which it cannot, there is an inadequate record to support the adoption of either the Proposed Rules or the prohibitions or restrictions on the specific practices that the NPRM contemplates restricting or prohibiting—*viz.*, DPI, persistent tracking, take-it-or-leave-it offers, and financial inducements.[104]

With respect to the Proposed Rules, as CTIA and others argued in their opening comments, there is simply an inadequate record both that ISPs present a unique risk of harm and that regulation under a regime modeled on the FTC's privacy regime would be ineffective.[105] These same omissions likewise undermine reliance on Section 201 and 202 to restrict or prohibit DPI or persistent tracking. That is because, as discussed at greater length below, the use of DPI to collect information for marketing is not, and is unlikely to become, widespread due to its prohibitive costs and other incentives against its use, and because edge providers are also capable

[102] The same analysis demonstrates why the Commission cannot prohibit take-it-or-leave-it offers or financial inducements under Section 222, on the one hand, or Sections 201 and 202, on the other. Specifically, the Commission must allow carriers to use or disclose customer information with "approval." The term "approval" must reflect the common law contract law principle that neither take-it-or-leave-it offers nor financial inducements are unconscionable. *See* CTIA Opening Comments at 46. No other commenter appears to have addressed this argument.

[103] *See Great Lakes Comnet*, 2016 WL 2990926, at *2 (explaining that to survive arbitrary and capricious review, the Commission must provide findings of fact supported by substantial evidence on the record as a whole).

[104] *See* NPRM ¶¶ 258-272.

[105] *See infra* Part IV; *see also* sources cited, *supra*, note 15.

of engaging in persistent tracking that is qualitatively nondistinct from ISP persistent tracking or use of DPI.[106]

With respect to potential restrictions or prohibitions on take-it-or-leave-it offers and the offering of financial inducements, there is no economic or even anecdotal evidence in the record that these offers are coercive, abusive, or predatory such that they could be prohibited as unreasonable or unfair under Section 201(b). Moreover, so long as these offers are made available on a facially neutral basis, it is untenable to prohibit them as discriminatory under Section 202. Indeed, as will be discussed at greater length below, far from being unreasonable, unfair, or discriminatory, such offers not only are commonplace in the industry and offered by the largest and most popular edge providers, but, as argued by numerous public interest groups in this proceeding, also have the potential to give disadvantaged communities access to broadband services that they otherwise might not be able to afford.[107]

E. Virtually No Commenters Advocated Reliance on Section 705 or 706, Because Those Provisions Do Not Support the Proposed Rules or Other Privacy Rules.

Very few commenters took up Sections 705 and 706 of the Communications Act as possible foundations for the Proposed Rules. This is hardly surprising, given the shortcomings of these provisions for the Commission's present purposes.

---

[106] *See infra* notes 218-219 and accompanying text.

[107] *See* MMTC Comments at 8 (explaining that not "all alternative payment programs are necessarily wrong or abusive" and noting that "low-income consumers [] could benefit from discounts or other 'financial inducements' offered by ISPs" which could "serve to significantly drive online usage" and further noting that such programs "should not be seen as presumptively coercive" where basic procedural safeguards are in place); AAPI Comments at [unpaginated] 3 ("If the Commission were to prohibit financial inducements that were designed to support low-income broadband adoption, more vulnerable AAPI consumers would be deterred from online use. Without affordable alternatives, efforts to prevent the aforementioned [discounted] services would only hurt . . . low-income communities."); Mobile Future Comments at 7-8 ("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….Consumers generally understand the benefits they receive for sharing their information.").

In the case of the former, the NPRM identifies Section 705 as a possible basis only for prohibiting DPI—*i.e.*, not as a basis for imposing other rules regarding notice, choice, data security, data breach, and so forth.[108] But Section 705 cannot support a prohibition on DPI for three reasons, as CTIA explained in its Opening Comments: first, just as it cannot use Sections 201 and 202, the Commission cannot rely on Section 705 to prohibit that which Section 222 expressly permits; second, there is an inadequate record demonstrating the need to prohibit or restrict DPI; and third, DPI is not comparable to the types of malfeasance (*e.g.*, pirating), that the Commission can prohibit under Section 705.[109]

Section 706 is no less availing. Indeed, the Proposed Rules and the other contemplated restrictions and prohibitions are *flatly inconsistent* with Section 706. No commenter of which CTIA is aware seriously contended otherwise. New America OTI argued that protection of personal information is necessary to encourage broadband adoption, but never expressly claimed that this proposition, if true, supports the adoption of the Proposed Rules under Section 706.[110]

Assuming that New America OTI intended to make a Section 706 argument, it fails. As set forth in CTIA's Opening Comments, the Commission has never found anything more than a correlation between privacy concerns and broadband non-adoption, and even that correlation is suspect, given recent data that broadband adoption has *increased* over time, notwithstanding concerns about online privacy. Moreover, there is no evidence anywhere in the record that privacy concerns are primarily, or even at all, connected to ISPs as opposed to edge providers. Further, the Commission lacks substantial evidence or even any inferential basis for concluding that asymmetric regulation of ISPs would address privacy concerns, when Google, Facebook,

[108] *See* NPRM ¶ 267.

[109] *See* CTIA Opening Comments at 63-64.

[110] *See* New America OTI Comments at 9-11.

and other edge providers would continue to use and disclose customer information under the FTC's privacy regime the day after final rules are adopted. And in any event, the overwhelmingly negative effects that the Proposed Rules would have on ISP revenue would limit the ability of ISPs to make the capital intensive investments necessary for network deployment. These investments are more directly the object of Section 706 than is any indirect effect that general privacy concerns might have on broadband adoption.[111]

New America OTI failed to offer substantial evidence to the contrary. Specifically New America OTI cited the Commission's 2010 broadband survey,[112] which CTIA addressed in its Opening Comments: that survey suggests at best a *correlation* between privacy concerns and broadband non-adoption, which has since been disproved, as broadband usage has increased despite concerns about privacy connected with websites that exchange in health and other sensitive information.[113] New America OTI also cited a recent analysis from NTIA.[114] But this analysis, as discussed in CTIA's Opening Comments, proves the exact opposite of the proposition for which New America OTI cited it—*viz.*, broadband usage, including with respect to health and financial services, has increased over time, notwithstanding privacy concerns.[115]

F. The Arguments of Other Commenters Do Not Justify the Commission's Proposal to Prohibit the Use of Arbitration.

1. The Commission Lacks Authority to Prohibit or Regulate Arbitration.

As explained in CTIA's Opening Comments, the Federal Arbitration Act ("FAA") expressly makes arbitration agreements enforceable, except where Congress overrides the FAA

[111] *See* CTIA Opening Comments at 65-71.

[112] *See* New America OTI Comments at 10.

[113] *See* CTIA Opening Comments at 67-68.

[114] *See* New America OTI Comments at 10.

[115] *See* CTIA Opening Comments at 68.

through a "contrary congressional command" in another federal statute.[116] And the Communications Act of 1934, the statutory authority on which the Commission would presumably rely for any rule purporting to prohibit or limit arbitration, does not contain such a congressional command. The Communications Act does not say a word about arbitration provisions in agreements for telecommunications services; its legislative history is silent on consumer arbitration; and its purpose is entirely consistent with bilateral arbitration under the FAA.[117] In short, therefore, even if the Commission believes—contrary to the evidence—that prohibiting arbitration would benefit consumers, it lacks legal authority to adopt the proposed regulation on arbitration. If the Commission promulgates a rule restricting or prohibiting arbitration agreements between ISPs and their customers, that rule will be invalidated by the courts.

Several commenters nonetheless attempted to argue indirectly that the Commission has authority to regulate arbitration, citing certain statutes that give customers a private right of action for alleged privacy-related violations or allow customers to file complaints with the Commission regarding carrier practices.[118] The commenters argue that arbitration agreements constitute "unjust and unreasonable" practices under Sections 201 and 202 because they "place arbitrary obstacles in the way of" individuals who might wish to access these statutory remedies.[119] But these agreements are not contrary to law: neither the remedies created by the Communications Act, nor Sections 201 and 202's prohibition on "unjust and unreasonable" and "discriminatory" practices, override the FAA's mandate that arbitration agreements be enforced.

---

[116] *Id*. at 56.

[117] *Id.* at 56-57.

[118] Public Knowledge Comments at 33 (citing 47 U.S.C. §§ 208, 338(i), 551); American Association for Justice at 6 ("AAJ Comments").

[119] *Id*.

Nor do Sections 201 and 202 set forth a "contrary congressional command" to preclude arbitration. That is so for two reasons: First, neither statutory provision mentions arbitration at all, and when a statute is "silent on whether claims . . . can proceed in an arbitral forum, the FAA requires [an] arbitration agreement to be enforced according to its terms."[120] Second, it is simply not true, as some commenters claimed, that arbitration places an obstacle in the way of vindicating privacy rights—arbitration agreements simply require claims to be resolved in a different forum.

2. Arbitration Provides Wireless Consumers a Better Opportunity to Resolve Disputes Than Lawyer-Driven Class Actions

Several commenters filed comments dealing exclusively with the issue of arbitration, arguing that arbitration "[h]arms" consumers in various ways and that consumers must be able to "band together" in class actions rather than resolving disputes through arbitration.[121] They are wrong on both counts. Arbitration offers numerous benefits to wireless consumers; class actions, by contrast, largely enrich plaintiffs' lawyers who bring them while benefiting consumers very little.

a. Arbitration is Beneficial for Consumers.

As CTIA explained in its Opening Comments, arbitration benefits wireless consumers by providing them with a fair and efficient means of resolving disputes that realistically cannot be resolved in court. Arbitration is faster than litigation; it uses simpler procedures; and it often does not require an attorney or in-person appearance by the consumer. Furthermore, under the terms of their arbitration provisions, most wireless providers pay all costs of arbitration, as well

[120] *CompuCredit Corp. v. Greenwood*, 132 S. Ct. 665, 673 (2012).

[121] National Association of Consumer Advocates Comments ("NACA Comments") at 3 ; *see also* AAJ Comments.

as incentive payments to any customer who wins more in arbitration than he or she was offered in a settlement.

Certain commenters nonetheless argued that arbitration is a "deeply unfair practice" that favors businesses over consumers.[122] But each of the charges leveled against arbitration is either wrong or irrelevant.

First, these commenters objected that arbitration decisions are "rarely appealable."[123] But finality is a necessary component of arbitration: the point of arbitration is to save both sides time and expense by resolving a dispute more quickly and efficiently than the court system, and that goal would be undermined if the losing party in an arbitration were able to relitigate the entire matter in a court after the arbitration ended. (Businesses, like consumers, are "rarely" able to appeal arbitration decisions). In any event, whether there is judicial review of arbitration decisions is irrelevant unless arbitration itself is biased against consumers—which, as explained below, it is not.

Second, the commenters argued that arbitration is "subject to little public scrutiny." Indeed, the American Association for Justice contended in its comments that arbitration agreements "always" require confidentiality from arbitration participants.[124] But this is simply not true: there is nothing in most arbitration provisions in the wireless industry to prevent

[122] NACA Comments at 2. Indeed, a group of consumer advocacy organizations argued that the Commission has already "acknowledged" that arbitration is unfair, citing the 2015 *Open Internet Order*. *Id.* But that argument has little force. In the *Open Internet Order*, the Commission declined to require arbitration for open Internet complaint proceedings, based on concerns that arbitration "may more frequently benefit the party with more resources." 30 FCC Rcd at 5718 ¶ 267. Specifically, the Commission cited a commenter's suggestions that in arbitration, (1) consumers are required to pay filing fees and arbitrator costs, (2) the business selects the arbitration location, (3) arbitration decisions are unreviewable, and (4) arbitration decisions are often not public. *Id.* at n.689. But as CTIA demonstrated in its Opening Comments and further explains in these comments, these concerns are unfounded: arbitration provisions in the wireless industry do *not* require consumers to pay fees, provide for arbitration at a convenient location, and do not prohibit the consumer from making the decision of the arbitrator public. *See* CTIA Opening Comments at 52-53.

[123] NACA Comments at 2; *see also* AAJ Comments at 3.

[124] AAJ Comments at 2.

consumers from disclosing the facts of their cases and the details of their arbitration decisions if they choose to do so.

Third, the commenters argued that arbitration is a "rigged system" because the rules of arbitration favor businesses.[125] They claimed that arbitration plaintiffs "do not have a full opportunity to prove their case" because "the rules of evidence and discovery do not apply" in arbitration; that a business can "unilaterally set the terms of arbitration" and "decide on the arbitrator as well"; that arbitrators need not be trained in the law or follow the law; that arbitration does not allow for deposing witnesses or taking interrogatories; and that arbitration suffers from a repeat-player effect that gives arbitrators a "built-in incentive . . . to rule for the business."[126] They also argued that because arbitration does not generate precedent, it "hinder[s]" the development of the law in the area of consumer protection.[127]

Tellingly, this laundry list of allegations is not supported by *any* citation of evidence. That should be reason enough for the Commission to discredit these claims. But in any event, none of the charges has merit:

- Although arbitration does use streamlined procedures, consumers are still able to obtain evidence from businesses that is needed to prove their case through discovery-like procedures.[128] The commenters ignored the obvious benefit of arbitration's simplified and streamlined procedures: they allow consumers to bring their claims and obtain relief without needing to retain a lawyer.
- The argument that businesses "unilaterally set the terms of arbitration" is misleading. As explained in CTIA's Opening Comments, businesses' arbitration provisions must comply with the minimum standards of the American Arbitration Association ("AAA") and/or JAMS, the country's leading arbitration providers.

[125] NACA Comments at 4.

[126] *Id.*; *see also* AAJ Comments at 2-3.

[127] AAJ Comments at 3.

[128] *See, e.g.*, Am. Arbitration Ass'n, *Consumer Arbitration Rules* 20, https://www.adr.org/aaa/ShowProperty?nodeId=/UCM/ADRSTAGE2021425&revision=latestreleased (allowing arbitrator to "direct 1) specific documents and other information to be shared between the consumer and business, and 2) that the consumer and business identify the witnesses, if any, they plan to have testify at the hearing").

These minimum standards prevent businesses from drafting arbitration provisions that unfairly favor them.[129] Moreover, arbitral organizations like the AAA set forth the basic rules governing consumer arbitrations; those rules are largely incorporated into arbitration agreements.

- Businesses generally do not "decide on the arbitrator," as the commenters contend. Arbitration provisions in the wireless industry specify the organization (generally AAA or JAMS) that will oversee the arbitration, but the rules of those organizations do not allow any party to choose the arbitrator(s) for a dispute unilaterally.[130]

- Contrary to the commenters' insinuation that arbitrators "need not be trained in the law," arbitrators are generally experienced legal professionals. For example, virtually all the neutrals on JAMS's roster are lawyers or retired judges.[131]

- It is wrong to suggest that arbitrators do not have to follow the governing law. For one thing, given that most arbitrators have substantial legal experience, they can be expected to follow the law. And in addition, courts retain the ability to overturn arbitration decisions that disregard applicable law.[132]

- There is no evidence that arbitrators are biased against consumers, as some commenters suggested. On the contrary, the evidence shows that claimants win at least as often, if not more often, in arbitration than they do in court.[133]

- Although arbitration does not generate case law, class actions—the commenters' preferred alternative to arbitration—*do not generate case law either*. That is because, as a recent study by the Consumer Financial Protection Bureau ("CFPB") revealed, class actions are almost never resolved with a judgment on

[129] CTIA Opening Comments at 51-52.

[130] *See* Am. Arbitration Ass'n, *Consumer Due Process Protocol Statement of Principles* 1 (Apr. 17, 1998), https://adr.org/aaa/ShowPDF?doc=ADRSTG_005014 ("The Consumer and [Business] should have an equal voice in the selection of Neutrals in connection with a specific dispute."); JAMS, *JAMS Policy on Consumer Arbitrations Pursuant to Pre-Dispute Clauses Minimum Standards of Procedural Fairness* (Jul. 15, 2009), http://www.jamsadr.com/rules-consumer-minimum-standards/ ("The arbitrator(s) must be neutral and the consumer must have a reasonable opportunity to participate in the process of choosing the arbitrator(s).").

[131] *See* JAMS, *Neutral Search Results*, http://www.jamsadr.com/professionals/xpqProfResults.aspx?xpST=ProfessionalResults.

[132] *See generally* Michael H. LeRoy, *Are Arbitrators Above the Law? The "Manifest Disregard of the Law" Standard*, 52 B.C. L. Rev. 137 (2011).

[133] *Compare* Christopher R. Drahozal & Samantha Zyontz, *An Empirical Study of AAA Consumer Arbitrations*, 25 Ohio St. J. on Disp. Resol. 843, 898 (2010) (studying claims filed with the American Arbitration Association and concluding that consumers win relief 53.3% of the time), *with* Theodore Eisenberg et al., *Litigation Outcomes in State and Federal Courts: A Statistical Portrait*, 19 Seattle U. L. Rev. 433, 437 (1996) (observing that in 1991-92, plaintiffs won 51% of jury trials in state court and 56% of jury trials in federal court, while in 1979-1993 plaintiffs won 50% of jury trials).

> the merits: rather, they are either dismissed or settled.[134] Thus, prohibiting arbitration would do nothing to promote the development of the law.

Fourth, these commenters argued that arbitration must be unfair because very few consumers use it—citing what they believe are low numbers of arbitrations filed against companies such as Verizon and Time Warner Cable.[135] The commenters contended that these figures show that arbitration provisions "simply block claims" rather than serving as an "actual means" of resolving disputes.[136]

But the number of arbitrations filed is a misleading measure of the value of arbitration, for two reasons. *First*, consumers' claims are often resolved before the filing of a formal arbitration proceeding. Individuals who file arbitration demands—just like those who file small claims court cases or lawsuits in court—are almost always a very small group of consumers whose concerns were not resolved through less-formal customer service mechanisms. When companies have millions of customers, it is likely that thousands—perhaps tens of thousands—of customers will at some point in their relationship have concerns that may or may not develop into full-fledged disputes. But the vast majority of those customer concerns are resolved through informal channels, such as customer service processes, negotiation, or mediation, before a concern ripens into a dispute and a formal arbitration demand is filed.

Dispute resolution is especially important in the wireless industry in which CTIA's members operate because it is a competitive industry. Wireless customers have more opportunities than ever to raise complaints and make their voices heard, particularly through social media, and providers must be responsive to these complaints in order to retain customers

---

[134] Consumer Fin. Protection Bureau, *Arbitration Study: Report to Congress, pursuant to Dodd-Frank Wall Street Reform and Consumer Protection Act § 1028(a)* at 37 (Mar. 1, 2015) ("*CFPB Study*") (finding that only 1.8% of class actions in sample reached a judgment on the merits).

[135] NACA Comments at 3.

[136] *Id.*

and stay competitive. Providers thus have a particularly strong incentive to resolve complaints before any lawsuit or arbitration commences.

Even when internal dispute resolution mechanisms fail and consumers do file for arbitration, there are significant incentives for businesses to settle claims before arbitration begins. As explained in CTIA's Opening Comments, wireless companies subsidize most or all of the costs of arbitration, and many have adopted arbitration agreements that provide for potential bonus payments to customers who do better in arbitration than a company's last settlement offer.[137] Significantly, a great many arbitration provisions require the company involved to pay all or nearly all of the arbitration costs, and many of the provisions include bonus provisions. Those agreements provide a very powerful incentive for pre-arbitration settlement of any non-frivolous consumer claim.

Second, plaintiffs' lawyers have long been waging a concerted campaign to invalidate arbitration agreements. They vigorously resisted arbitration (with success in certain "magnet" jurisdictions for class actions) before the U.S. Supreme Court's decision in *AT&T Mobility v. Concepcion*. And after the Supreme Court held in *Concepcion* that class waivers in arbitration agreements are enforceable, the plaintiffs' bar has continued to search for ways to avoid their clients' agreements to resolve their disputes in arbitration. The unfortunate effect of these widespread efforts is that class-action lawyers and their allies in consumer advocacy organizations have discouraged consumers from pursuing their disputes in simplified, often cost-free arbitration.

Plaintiffs' lawyers have a strong interest in preserving class actions because class actions are far more lucrative for the plaintiffs' lawyers than for class members—their ostensible clients.

[137] CTIA Opening Comments at 52-53.

Indeed, the CFPB study found that plaintiffs' lawyers attorneys' fees amount to 41 percent of the average class action settlement fund, and the average attorneys' fees in class actions are more than $1 million per case.[138] Meanwhile, the average settlement payment to class members was just $32.35.[139]

Finally, some commenters argued that arbitration agreements are harmful because they are entered into before disputes occur. They claimed that arbitration should be "an option for telecom customers to choose only after disputes arise."[140] But pre-dispute agreements are necessary in order for arbitration to function properly: a rational business cannot justify the costs of making arbitration available to customers (including by paying all arbitration fees) if it also is forced to bear the cost of litigating in court. Prohibiting predispute arbitration would thus prompt businesses to eliminate their arbitration provisions altogether, depriving consumers of access to arbitration.

In short, commenters' attacks on arbitration are unfounded: arbitration gives wireless consumers a fair and accessible forum in which to resolve disputes with their service providers.[141] The Commission should not deprive consumers of this valuable resource through administrative fiat.

---

[138] *CFPB Study* at 33.

[139] *Id.* at 27-28. The CFPB found that a total of $1.1 billion was awarded in class actions involving a total of 34 million class members.

[140] NACA Comments at 3; *see also* AAJ Comments at 2.

[141] One other comment regarding arbitration merits mention: The Consumer Federation of California argued that arbitration systems should be opt-in, rather than opt-out. It reasoned that because "most consumers do not understand pre-dispute arbitration agreements" and do not know whether their service contracts have arbitration clauses or not, the choice offered by opt-out provisions is an "illusory choice." Consumer Federation of California Comments at 12. But this reasoning is seriously flawed. As two scholars at George Mason University observed with respect to the financial services industry, the fact that consumers are often unaware of whether the services they use are subject to arbitration agreements indicates that consumers *do not care* about arbitration provisions. That is because instead of litigating disputes when they arise, consumers generally prefer to simply take their business elsewhere. Jason Scott Johnston & Todd Zywicki, *The Consumer Financial Protection Bureau's Arbitration Study: A Summary and Critique*, Mercatus Working Paper, George Mason University (Aug. 2015), http://mercatus.org/publication/consumer-financial-protection-bureau-arbitration-study-summary-critique.

b. The Commission Should Not Prohibit Arbitration In Favor of Lawyer-Driven Class Actions

A group of consumer advocacy groups also predictably argued that arbitration must be prohibited so that consumers can join in class action lawsuits. However, class actions generally line the pockets of lawyers while providing little to no benefit to consumers.[142] These groups' erroneous arguments do nothing to shake that conclusion.

The commenters first raised *AT&T Mobility v. Concepcion*, in which, they complained, "AT&T customers were prohibited from banding together to challenge" certain surcharges on their bills.[143] What the commenters omitted, however, is that the lower court in *Concepcion* found, and the Supreme Court agreed, that AT&T customers were "*better off* under their arbitration agreement with AT&T than they would have been as participants in a class action, which could take months, if not years, and which may merely yield an opportunity to submit a claim for recovery of a small percentage of a few dollars."[144]

The groups then cited certain other cases in which class actions were not allowed to proceed because of arbitration agreements.[145] But as in the *Concepcion* case, there is every reason to suspect that the consumers affected by the purported unfair practices in these cases would be better off resolving the problem with the company in arbitration—or informally, before any arbitration began—than they would in a class action where the primary benefit would accrue to lawyers, not class members.

The groups similarly cited cases in which class actions purportedly yielded substantial benefits for consumers. But their two examples are badly chosen, because neither of those class

[142] CTIA Opening Comments at 54-55.

[143] NACA Comments at 4.

[144] *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333, 352 (2011) (internal quotation marks omitted).

[145] NACA Comments at 6-7.

actions yielded much benefit for the average consumer. In one case, a class action involving allegedly improper charges for state and local taxes on bills, the named plaintiffs complained to their provider about the charge, received a credit of 74 cents, and were not charged the tax again—yet they proceeded with a class action, the main results of which were to enrich lawyers and encourage businesses to *undercollect* the taxes owed to states and local jurisdictions.[146] And with respect to the other class action, which also involved an allegedly improper tax charge, the commenters stated that the settlement of the case "distributed 20 million dollars" to class members—omitting the fact that up to $5 million of that amount would be diverted to pay the plaintiff's lawyers.[147]

Finally, the consumer groups argued that if not for class actions, many consumer complaints would "go unheard" because the potential recovery for an individual consumer would not justify bringing a claim.[148] But as CTIA noted in its comments, many wireless companies now use customer-friendly arbitration provisions that shift *all* arbitration fees to the company and allow the consumer to recover incentive payments, attorneys' fees, and/or expert witness costs if she wins more in arbitration than she was offered in a settlement.[149] These features provide ample incentive for plaintiffs to pursue even small claims and thus, as Justice Kagan has observed, they make it possible to vindicate consumer interests without class actions.[150] Indeed, because wireless companies are usually bound to pay all arbitration fees if a consumer initiates

---

[146] Rachel Wilson & Charlotte F. Noel, Jones Day, *AT&T v. Allen: Oklahoma Decision More Than "O.K." For Class Action Attorneys, But Bad For Business And States* (Dec. 10, 2004), http://www.mondaq.com/unitedstates/x/29977/Corporate+Tax/ATT+v+Allen+Oklahoma+Decision+More+Than+OK+For+Class+Action+Attorneys+But+Bad+For+Business+And+States.

[147] *See* Order at 11, *Hesse v. Sprint Spectrum LP*, No. 2:06-cv-00592 (W.D. Wash. Dec. 2, 2014).

[148] NACA Comments at 5-7.

[149] CTIA Opening Comments at 52-53.

[150] *Am. Exp. Co. v. Italian Colors Rest.*, 133 S. Ct. 2304, 2318 (2013) (Kagan, J., dissenting) (noting that arbitration agreements permitting "informal coordination among individual claimants" and allowing for "amelioration of arbitral expenses" would permit effective vindication of claimants' interests in arbitration).

arbitration, which can amount to hundreds of dollars or more, they have a powerful incentive to settle nonfrivolous claims before arbitration even occurs.

What is more, arbitration is often the *only* feasible means of bringing a consumer dispute. Many wireless consumer disputes involve facts unique to a particular customer's situation. These individualized disputes cannot be resolved in class actions, which require that class members' claims involve "common" questions.[151] And because of their low value, these claims cannot practicably be brought in individual litigation, where cost-shifting is unavailable and a consumer is responsible for filing fees. Thus, *prohibiting* arbitration—not maintaining it—is what will cause many consumer complaints to "go unheard."

III. COMMENTERS THAT SUPPORT THE NPRM EITHER ENTIRELY IGNORED OR DRASTICALLY UNDERSTATED THE PROPOSED RULES' FIRST AMENDMENT PROBLEMS.

The NPRM at least tacitly acknowledges that imposing restrictions on ISPs' use and disclosure of information generated in the ordinary course of business implicates ISPs' First Amendment interests.[152] The NPRM even requests comment on whether certain proposed restrictions could satisfy the constitutional test set forth in *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*.[153] These requests for comment miss the mark, insofar as the controlling First Amendment precedent is not *Central Hudson*—it is *Sorrell v. IMS Health, Inc.*[154]—but at least they demonstrate the Commission's awareness that a robust constitutional inquiry would follow the adoption of the Proposed Rules. It is therefore surprising that, by CTIA's tally, the vast majority of comments that supported the NPRM did not take up the constitutional questions at all—let alone the more difficult questions under *Sorrell*. This

[151] Fed. R. Civ. P. 23(a)(2).

[152] *See* CTIA Opening Comments at 73-74 & n.228; Tribe Comments at 9-14.

[153] *See, e.g.*, NPRM ¶ 126.

[154] 564 U.S. 552 (2011).

silence is deafening and underscores that the constitutional problems CTIA has identified compel a reviewing court to invalidate the rules, if adopted, on constitutional grounds.[155]

A. The Proposed Rules Impose Prohibited Speaker-Based and Content-Based Restrictions on Speech and Fail to Satisfy Strict Scrutiny Under *Sorrell*.

In 2007, Vermont enacted the Prescription Confidentiality Law, which "restrict[ed] the sale, disclosure, and use of pharmacy records that reveal the prescribing practices of individual doctors" including "for marketing purposes."[156] In its review of the law, the Supreme Court explained that these restrictions had to be "subjected to heightened judicial scrutiny" under the First Amendment and could not "satisfy this standard."[157] That is so, because the law "on its face burden[ed] disfavored speech" (*i.e.*, marketing) "by disfavored speakers," (*i.e.*, pharmaceutical manufacturers) relative to research institutions and other entities.[158] The constitutional problems that the law suffered did not stop at its text and structure, however; "[f]ormal legislative findings . . . confirm[ed] that the law's express purpose and practical effect [we]re to diminish the effectiveness of marketing by manufacturers of brand-name drugs," and "[j]ust as the inevitable effect of a statute on its face may render it unconstitutional, a statute's stated purpose may also be considered."[159]

Here too, the structure and text of the Proposed Rules demonstrate their invalidity. On their face, the Proposed Rules impose unique restrictions on ISPs relative to other entities in the Internet ecosystem, and they impose heightened restrictions to deter not just marketing, but specific types of marketing (*i.e.*, marketing unrelated to broadband service). Like the statute at

---

[155] *See* CTIA Opening Comments at 75; Tribe Comments at 8, 38-39.

[156] *Sorrell*, 564 U.S. at 557.

[157] *Id*.

[158] *See id*. at 564.

[159] *See id*. at 565 (citation and internal quotation marks omitted).

issue in *Sorrell*, the restrictions are both content- and speaker-based, either of which is presumptively fatal.[160] Similarly, like the Vermont legislature's express findings in support of the Prescription Confidentiality Law, comments in support of the NPRM confirm that the Proposed Rules' intended effects are to "diminish the effectiveness of marketing" by, or delivered by, ISPs. Public Knowledge in particular reveals the clear censorious intent that underlies the Proposed Rules by claiming (incorrectly in most respects) that (1) predictive advertising is qualitatively different from, and more effective than, traditional behavioral advertising; (2) ISPs have unique technical capacity to harvest subscriber information, analyze it, and monetize it through the delivery of predictive advertisements; and (3) the Proposed Rules would restrict ISPs' capacities in this regard, rendering their marketing, and the advertisements they deliver, less effective.[161] Even though these factual propositions are not supported by the record, they nonetheless confirm that the Proposed Rules are animated by an unconstitutional purpose; that is effectively dispositive.

B. Public Knowledge's Attempt to Preserve the Proposed Rules Under *NCTA v. FCC* Is Based on an Erroneous Analysis That Fails on Its Own Terms in Any Event.

As noted, very few commenters addressed the constitutional questions posed by the NPRM. That is likely because of the heavy burden that the Commission would face in confronting a constitutional challenge to the Proposed Rules. It is a fundamental principle of constitutional law that, even under intermediate scrutiny as described in *Central Hudson*, the state entity that seeks to censor commercial speech has the burden at every step.[162] This burden

[160] *Sorrell*, 564 U.S. at 571 ("In the ordinary case it is all but dispositive to conclude that a law is content-based and, in practice, viewpoint-discriminatory."); Tribe Comments at 23-24; 30-32.

[161] *See* Public Knowledge Comments at 7-10.

[162] *See* CTIA Opening Comments at 78-81.

reflects that even purely commercial speech has value[163]—a proposition that is uniquely true for the online ecosystem, where ISPs and edge providers are constantly offering new and innovative products, services, and bundles, thereby stimulating consumer demand and driving further competition.[164] The Commission's heavy burden also reflects that it is better to entrust consumers to opt out of undesirable speech than to empower government agencies to burden that speech in the first instance.[165]

1. The Proposed Rules Fail as Applied to Any Use Case That Does Not Involve Disclosure or Dissemination to a Third Party.

According to Public Knowledge, the Proposed Rules satisfy this burden under the D.C. Circuit decision, *NCTA v. FCC*.[166] At the outset, however, it is important to note that *NCTA* is utterly irrelevant to the vast majority of uses that the Proposed Rules restrict, which uses do not implicate the state's interest in protecting privacy *at all*.[167] Like its review of survey data regarding customer expectations, here too, the Commission must resist uncritical assertions from commenters about "privacy"—in this case, the relevant assertion is that there is a substantial state interest in the protection of "privacy" in the abstract. Precisely because of the potential breadth of "privacy" as a state interest, a censoring government entity must define the concept in a particularized and cognizable way to justify speech restrictions.[168] At most, *NCTA*, on which Public Knowledge relied, stands for the proposition that there is a cognizable interest in

---

[163] *See Edenfield v. Fane*, 507 U.S. 761, 766 (1993) ("[S]olicitation allows direct and spontaneous communication between buyer and seller. A seller has a strong financial incentive to educate the market and stimulate demand for his [or her] product or service, so solicitation produces more personal interchange between buyer and seller than would occur if only buyers were permitted to initiate contact.").

[164] *See* CTIA Opening Comments at 79-80.

[165] *See Bates v. State Bar of Ariz.*, 433 U.S. 350, 374-75 (1977); *Rowan v. U.S. Post Office Dep't*, 397 U.S. 728, 737 (1970).

[166] *See* Public Knowledge Comments at 35-39 (relying on *Nat'l Cable & Telecomms. Ass'n v. FCC*, 555 F.3d 996 (D.C. Cir. 2009)).

[167] *See* CTIA Opening Comments at 82-90; Tribe Comments at 39-40.

[168] *See* CTIA Opening Comments at 81-82.

controlling the dissemination of information outside of a customer-provider relationship, where restrictions on dissemination would be effective and prevent tangible harm to consumers.[169] Uses of customer information that do not involve disclosure or an increased risk of disclosure to a third party—*i.e.*, any ISP first-party marketing or delivery of third-party marketing, whatever the level of sophistication, that does not involve disclosure—simply do not implicate *NCTA*.

Nor can the Commission rely on a purported substantial interest in protecting customers from vexatious or burdensome advertising, because there is no record supporting the applicability of that interest here.[170] To the contrary, Public Knowledge's extensive discussion of predictive advertising suggests that consumers actually *benefit* from such advertising: according to Public Knowledge, companies that used this form of advertising experienced a 25 percent increase in their return on investment, showing that consumers responded affirmatively more frequently to the ads that they received.[171] As CTIA argued in its Opening Comments, the Commission also must proceed with caution before announcing an unsupportable, novel interest in protecting consumers from sophisticated or predictive profiling and advertising based on the uncited, conclusory intuition that some consumers may find such advertising unwelcome.[172] At the very least, such an interest, if valid at all, cannot support an opt-in approval standard, which is not proportionate to the state's interest in protecting such consumers.[173]

Even if the state interest articulated in *NCTA* did somehow extend to ISP uses that do not involve disclosure of customer information, the Proposed Rules would still fail constitutional

---

[169] As will be discussed at greater length below, even this articulation of *NCTA* is untenable given the intervening *Sorrell* decision. *See infra* notes 184-185and accompanying text.

[170] *See* CTIA Opening Comments at 84-85.

[171] *See* Public Knowledge Comments at 8.

[172] *See* Consumers' Research Comments at 10 (citing *Sorrell* and stating "[t]hat some consumers do not welcome targeted marketing cannot justify broad and complex restrictions for all consumers").

[173] *See* CTIA Opening Comments at 89.

review. As CTIA explained, the Proposed Rules are not narrowly tailored, given the number of entities in the ecosystem that will continue to use the same customer information, and given the reliance on opt-in approval, which unnecessarily restricts more speech than necessary.[174]

2. Given Gaps in the Record, the Proposed Rules Also Fail as Applied to Use Cases That Involve Disclosure to Third Parties.

Even with respect to ISP uses of "customer proprietary information" that involve disclosures or access to third parties, the Commission cannot rely on *NCTA* to justify the Proposed Rules. *NCTA* is both no longer controlling and distinguishable in critical ways that the NPRM and Public Knowledge failed to consider.[175]

First, insofar as *NCTA* ever could have been construed to stand for the broad proposition that there is a privacy interest in preventing the commercial exchange to *all third parties* of information that companies generate in the course of business, that reading is now squarely foreclosed by the Supreme Court's intervening decision in *Sorrell*, described above, which found that companies have a First Amendment interest in engaging in precisely those exchanges.[176]

Second, *NCTA* involved the Commission's decision to adjust the level of protections for an ISP to disclose CPNI. CPNI is a uniquely proprietary category of information that, at the time, was available only to the customer and to his or her provider by virtue of providing service. *NCTA* therefore is inapposite with respect to the Commission's authority to regulate "customer proprietary information," which includes swaths of information that are not unique to the ISP-customer relationship, and indeed may be public or easily acquired from third parties.[177]

---

[174] *See id*. at 85-87.

[175] *See* Public Knowledge Comments at 35-39 (arguing that *U.S. West* does not control the constitutional inquiry).

[176] *See Sorrell*, 564 U.S. at 570 (finding a "strong argument that prescriber-identifying information [itself] is speech for First Amendment purposes"); Tribe Comments at 40.

[177] Tribe Comments at 39-40.

Third, Public Knowledge argued that record-based distinctions between *NCTA* and *U.S. West, Inc. v. FCC* compel the conclusion that the former controls and the latter is irrelevant. This argument is ironic: Public Knowledge got it *exactly right* when it said that the validity of an opt-in restriction would turn on the completeness of the appellate record,[178] but *exactly wrong* in supposing that there is an adequate record here.

At the state interest stage of the inquiry, the *Pretexting Order* rulemaking process stands in stark contrast to this proceeding. There, the Commission justified an incremental increase in protections based on record evidence of emerging specific practices that were exposing consumers to substantial risk of harm and that a locus of this risk was the sharing of information with independent contractors and joint venture partners.[179] Here, there is an inadequate record (1) that there is a black market for broadband CPNI or various "customer proprietary information" elements; (2) that malfeasors are using such information for harmful online or offline practices; or (3) that ISPs' disclosure of, or providing access to, such information to independent contractor or joint venture partners—let alone affiliates, agents, vendors, or other third parties—is how such information enters the stream of commerce. Public Knowledge's arguments about ISPs' unique capacities to develop and support predictive advertising, even if

[178] Public Knowledge Comments at 35 (explaining that the "key difference" between *U.S. West* and *NCTA* "rests on the completeness of the appellate record insofar as it reflects the government's constitutional burden in defending the opt-in framework's limitation on commercial speech").

[179] *See In re Implementation of the Telecommunications Act of 1996, Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6947 ¶ 37 (2007) ("*2007 CPNI Order*") (adopting enhanced restrictions based on "new circumstances" and "new privacy concerns"); *id.* at 6947-48 ¶ 39 (describing that "[t]he black market for CPNI has grown exponentially with an increased market value placed on obtaining this data, and there is concrete evidence that the dissemination of this private information does inflict specific and significant harm on individuals, including harassment and the use of the data to assume a customer's identity"); *id.* at 6950 ¶ 44 ("The record in this proceeding . . . is replete with specific examples of unauthorized disclosure of CPNI and the adverse effects of such disclosures on customers."); *id.* at 6950 ¶ 45 (explaining "based on the record in this proceeding" that "unauthorized disclosure of CPNI is a serious and growing problem" and further noting the "undisputed evidence demonstrating that unauthorized disclosures of CPNI constitute a serious and prevalent problem . . . [i]n light of the serious damage that unauthorized CPNI disclosures can cause").

true, have nothing to do with the disclosure of information to third parties or the risks of inadvertent disclosure. Accordingly, these arguments are irrelevant under *NCTA*.

At the tailoring stage of the inquiry, too, the pretexting rules fare better than the Proposed Rules. Specifically, the pretexting rules governed disclosures of information in what was, at the time, a closed market—*i.e.* where information was held only by the carrier and customer. Restrictions vis-à-vis third parties were therefore plausibly likely to preserve customers' control of information. In contrast, the Proposed Rules will govern entities in an open ecosystem, where other entities have access to the same "customer proprietary information" that ISPs do, such that restrictions on ISPs' use and disclosure cannot prevent data from entering the stream of commerce through edge providers and data appenders and brokers.

Fourth, for similar reasons, the Proposed Rules fail to reflect customer expectations or preferences. In the *Pretexting Order*, the Commission pointed to record evidence that there was "less customer willingness for their information to be shared without their express authorization with others outside the carrier-customer relationship."[180] There is and can be no such evidence in the record here. Opt-out mechanisms are the norm in the ecosystem under the FTC's privacy regime. The imposition of a much more restrictive protection is therefore not proportionate to the state's interest in protecting the control of information. Likewise, there is compelling evidence that consumers do not expect asymmetric regulation of ISPs; instead, they expect uniform regulation of entities in the ecosystem.[181] The imposition of unique restrictions on ISPs therefore is not proportionate to the state's interest in regulating online privacy. And finally, the restrictions cannot even be justified on a theory of advancing customer *preferences*—which has never been held to be a legitimate state interest in any event. That is so because, as will be

[180] *See 2007 CPNI Order*, 22 FCC Rcd at 6948 ¶ 40.

[181] *See generally* PPI Comments.

discussed at greater length below, the rules actually impose the costs of the few privacy-conscious customers on the majority of privacy-neutral customers, and therefore are not proportionate to a customer-preferences-based state interest.

IV. THERE IS AN INSUFFICIENT RECORD FOR ADOPTION OF THE PROPOSED RULES.

CTIA, like numerous other commenters, expressed concerns that the NPRM identified solutions in need of a problem. Commenters that supported the NPRM inadvertently amplified these concerns by failing to establish a record supporting several propositions that are necessary preconditions for the Proposed Rules: (1) that ISPs possess unique capabilities with respect to the collection and use of information; (2) that ISPs otherwise present a unique privacy risk or are engaging in practices that have some nexus to traditional privacy concerns; (3) that customer expectations align with the Proposed Rules' asymmetric regulation of IPSs; and (4) that there is reason to depart from the FTC's privacy regime, which is based on principles of sensitivity, on the one hand, and flexibility, on the other, and which has maximized customer privacy while allowing for further innovation and competition. An agency's action is arbitrary and capricious if the agency fails to consider important issues that it seeks to address or if the evidence offered fails to support the proposed rules.[182] Thus, in addition to the reasons stated in CTIA's Opening Comments, this absence of a record to support the Proposed Rules deprives the Commission of *Chevron* deference.[183]

[182] *Int'l Union, United Mine Workers of Am. v. MSHA*, 626 F.3d 84, 94 (D.C. Cir. 2010) (discussing agency's obligation under the APA to address significant comments in substantive, rather than conclusory, manner); *Great Lakes Comnet, Inc., v. FCC*, __ F.3d __, 2016 WL 2990926, at *2 (D.C. Cir. 2016) (explaining that Commission's failure to address or explain issues requires remand under the APA).

[183] As CTIA noted in its Opening Comments, the APA prohibits the Commission from adopting the Proposed Rules because they are, among other things, "in excess of statutory . . . authority[] or limitations." CTIA Opening Comments at 14.

A. ISPs Do Not Possess Unique Capabilities with Respect to the Collection or Use of Consumer Information and Are Constrained by a Robustly Competitive Market.

The NPRM was based on numerous assumptions about, among other things, the nature of the online ecosystem, the availability of data to other entities in that ecosystem, and the state of competition in the wireless broadband market. The record now confirms that these assumptions were mistaken, and that asymmetric regulation of ISPs would be counterproductive.

Congress enacted Section 222 to address problems that it perceived within a closed and historically non-competitive telecommunications market: customers shared information with their telecommunications providers, risking customer privacy and potentially entrenching incumbent providers. Because the market was closed, Congress intuited that it was possible to prevent customer information from entering the stream of commerce by restricting, among other things, the disclosure of, or access to, customer information.[184] This description stands in stark contrast to the online ecosystem, a fundamental principle of which is the open and free flow of information. In this ecosystem, vast amounts of information are already, and constantly, part of the stream of commerce, where they are available to numerous entities at any given time. Indeed, this free flow of data is essential to the proper functioning of the ecosystem.

Commenters here repeated their favorite refrain that ISPs function as "gatekeepers" in the market and therefore have unique and comprehensive access to customer information.[185] But after extensive review and fact-gathering regarding the nature of the ecosystem and multiple workshops on this issue, the FTC determined in 2012 that ISPs should not be singled out for heightened restrictions; instead, it took a technology-neutral approach that appropriately focused

[184] *See* CTIA Opening Comments at 110-11.

[185] *See, e.g.*, Public Knowledge Comments at 3; Free Press Comments at 21; EFF Comments at 10.

on the sensitivity of customer data.[186] As documented in the *Swire Report* and the comments of several technologists and others in this proceeding, intervening changes since 2012—including the continued proliferation of encryption, the development of new persistent tracking technologies available to non-ISP entities, and the steady adoption of Virtual Private Networks ("VPNs")—confirm that the FTC's approach was not only sound from a policy standpoint, but also technologically prescient.[187]

Commenters attempted to undermine the *Swire Report* by arguing with certain specific findings.[188] Peter Swire and his colleagues can respond to these technical objections in reply comments. But even apart from his reply, these attacks on the *Swire Report* fall short for several independent reasons. First, even if each of the objections to the *Swire Report* were valid, which they are not, that fact at most would demonstrate that ISPs' access to customer information has

[186] *See* CTIA Opening Comments at 121-22; *see also FTC Report* at 40-41; FTC, *The Big Picture: Comprehensive Online Data Collection* (Dec. 6, 2012), https://www.ftc.gov/news-events/events-calendar/2012/12/big-picture-comprehensive-online-data-collection; Leibowitz Comments at 4 (noting the importance of technology neutrality to FTC framework, because "ISPs are just one type of large platform provider," and emphasizing that the most important privacy distinction is "the sensitivity of the type of data collected").

[187] *See, e.g.*, Leibowitz Comments at 2 ("[T]here have been fundamental changes in the way consumers access and use the Internet itself. Despite these changes, the framework established in 2012 and the principles within the framework not only remain the same, but also are more applicable than ever, as proven through repeated testing and enforcement in the dynamic Internet marketplace." (footnote omitted)). Paul Ohm argued in his Reply Comments that if encryption and VPNs increasingly are preventing ISPs from collecting customer information, then ISPs will be less able to collect information that is valuable for marketing, and as a result, ISPs should not be burdened by the proposed rules. Ohm Reply Comments at 4-5. However, Ohm fails to account for the sweeping nature of the proposed choice rules, which could require opt-in consent for *all* first-party marketing of non-communications-related services, including marketing for which no information about customers' online activity would be necessary (*e.g.*, marketing a new video content service to all existing customers). Thus, regardless of whether encryption and VPNs limit the extent to which ISPs can obtain information about customers' online activity, ISPs would nonetheless incur tremendous compliance costs under the proposed rules, and ISPs' ability to engage in a wide variety of first-party marketing would be curtailed significantly. As a result, consumers would be harmed because they would be denied access to information about new and discounted products and services.

[188] *See, e.g.*, Public Knowledge Comments at 9-11; Upturn Comments at 3-10; Feamster Comments at 6-7; Center for Democracy and Technology Comments at 16-17 (acknowledging that "the use of encryption by both subscribers and edge providers has risen significantly in the last few years" and asserting that "many transmissions remain unencrypted"). CTIA notes that Upturn *actually expressly confirmed* that the *Swire Report* is "technically accurate in most of its particulars" and that its comments were not intended to support the NPRM. *See* Upturn Comments at 1-2. Likewise, although cited favorably by Public Knowledge, Professor Nick Feamster actually concluded that the NPRM would "harm" "operators of ISP networks," "researchers," and "vendors and protocol developers." *See* Feamster Comments at 1.

not declined as much as Swire has asserted; but no commenter seriously disputed that various edge providers—especially search platforms and operating systems—have access to the same information as, if not more than, ISPs. In other words, it can be correct that encryption is not as widespread as the *Swire Report* suggests and that operating systems, social networks, search engines, and others also have comprehensive visibility into consumer activity. Moreover, many of these other entities have been the subject of an FTC enforcement action because of their privacy or data security practices.[189] Second, no commenter seriously disputed that the general trend is toward diminished ISP visibility into customer activity; even if the pace of change—for example, adoption of encryption and VPNs—is slower than suggested in the *Swire Report*, which it is not, that would not undermine the *Swire Report*'s general conclusion about the capacities of ISPs vis-à-vis the edge. Third, the Commission should accord considerable weight to the fact that even commenters who otherwise supported the NPRM acknowledged that edge providers often have at least comparable access to customer information.[190]

Many commenters ignored other inconvenient facts about the open Internet ecosystem. For example, there is a robust and growing market for data brokers and data appenders,[191] and their services allow virtually *any* edge provider to fill in gaps that may exist in its own tracking of consumer activity and behavior.[192] Edge providers also can engage in predictive analytics and modeling to fill in gaps regarding customers' offline activities, and these techniques are

[189] *See* CTIA Opening Comments at 2 n.4.

[190] *See* sources cited, *supra* note 16.

[191] *See* CTIA Opening Comments at 135-36.

[192] ISPs, like all companies, must comply with relevant laws and regulations, such as the Fair Credit Reporting Act, Pub. Law No. 91-508, 84 Stat. 1114 (1970), which seek to prevent the types of abuse that animate some of Public Knowledge's concerns. *See* Public Knowledge Comments at 15-17.

becoming even more sophisticated.[193] Accordingly, while CTIA does not agree that operating systems and browsers need to "barter" or "purchase" information to obtain access—nor do Facebook or Google[194]—the very fact that edge providers, like ISPs, *can* barter and purchase information that they do not possess demonstrates the ineffectiveness of trying to build a dam exclusively around ISPs' data practices.

Commenters also trotted out the familiar refrain that the broadband market is a "near monopoly," suggesting that ISPs lack incentives to protect their customers' information.[195] The Commission should not credit these self-serving assertions that are ungrounded in any economic analysis, and that clearly fail with respect to the mobile broadband marketplace, where there is competition and where switching costs are low.[196] So far as CTIA is aware, no commenter provided *any* evidence in the record of lack of competition in the market for mobile broadband or high switching costs for customers of mobile providers. CTIA, on the other hand, submitted empirical evidence of strong and growing competition in this market and highlighted campaigns by mobile providers to compete for each other's customers. The Commission should reject efforts by commenters to blur these distinctions by describing a homogenous "broadband" market.

The Consumer Federation of America argued that bundling of products and services increases switching costs,[197] but it provided no authority in support of this assertion and is wrong

[193] Peter Swire et al., *Online Privacy and ISPs* 53-55 (2016), http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf ("*Swire Report*").

[194] Center for Democracy and Technology Comments at 18.

[195] *See, e.g.,* Public Knowledge Comments at 3 ("[T]he economic reality of the American broadband market, with its market concentrations that tend toward monopoly, means that there has been zero competition . . . .").

[196] *See* CTIA Opening Comments at 113-16.

[197] *See* Grant Comments at 2-3 (stating that "consumers have a relatively small number of [ISPs] to choose from and often get their email service and other bundled services from them, making switching less likely," but not citing any support for this assertion).

in any event. In a competitive market, which the wireless broadband market is, providers will compete to offer more innovative packages and bundles of products and services. That is already happening today, and demonstrates that innovative uses of customer information can increase competition and stimulate demand.[198]

Not only is the mobile broadband market currently dynamic and competitive, but there is also every reason to think it will become only more so. The Commission's ongoing broadcast incentive auction will help ensure that more providers have access to the resources necessary to meet growing consumer demand for wireless broadband.[199] Moreover, the Commission—to its credit—is engaged in an ongoing rulemaking process to clear additional spectrum, including in bands above 24 GHz, for mobile usage, which will support the transition to fifth-generation ("5G") mobile networks and the increasing usage of IoT devices and applications.[200] These efforts will unleash innovation and greater competition in the market for wireless broadband service.

B. Even If ISPs Had Unique Access to Customer Information and Were Quasi-Monopolists, There Still Would Be Inadequate Evidence That They Pose a Unique Privacy Risk.

Given their insistence that ISPs possess unique capabilities to track customer online activity and use customer information, commenters offered surprisingly little analysis of (1) how or why these practices constitute a privacy threat; (2) whether ISPs are currently engaging in these practices—or have any incentive to do so now or in the future; (3) whether these practices

[198] *See* CTIA Opening Comments at 126-27. CTIA's Opening Comments also documented why the market for various edge services *are highly concentrated* and why switching costs for these providers *are uniquely high*. *See id.*

[199] *See, e.g.*, Ben Munson, *FCC Clears Maximum Amount of 126 MHz of Spectrum for 600 MHz Incentive Auction*, FierceWireless (Apr. 29, 2016), http://www.fiercewireless.com/story/fcc-clears-maximum-amount-126-mhz-spectrum-600-mhz-incentive-auction/2016-04-29.

[200] *See In re Use of Spectrum Bands Above 24 GHz for Mobile Radio Services*, Notice of Proposed Rulemaking, 30 FCC Rcd 11,878, 11,884-85 ¶ 12 (2015) (seeking comment on rules for licensing and secondary market transactions involving spectrum in bands above 24 GHz).

are inconsistent with customer expectations or preferences; and (4) whether there is any need to adopt substantially more restrictive protections than those provided by the FTC privacy regime, which is based on principles of sensitivity and flexibility. Instead, these commenters appear to have taken it as a given that even routine uses of information by ISPs are harmful. By so assuming, they deprived the Commission of a record that supports the Proposed Rules.

1. There Is an Unstated and Flawed Assumption in Many Comments That Routine Uses and Disclosures of Information, Without More, Constitute Privacy Harm.

As CTIA explained in its Opening Comments, this proceeding thus far has been unmoored from traditional privacy concerns.[201] This problem was apparent in the NPRM, and manifests again in many pro-NPRM comments. For example, Public Knowledge focused disproportionately on describing how evolving techniques for predictive advertising are different from, and more efficient than, traditional behavioral advertising.[202] But this description is noteworthy for what is missing. For example, there is no quantitative analysis of ISPs' share of the predictive advertising market. In fact, ISPs comprise a relatively small share of the growing online advertising market, which includes predictive advertising. In other words, in this market, ISPs are the disruptive new entrants who have the potential to introduce competition to the 10 dominant firms, none of which is an ISP, that currently comprise 70 percent of the market.[203] Public Knowledge likewise offered no qualitative analysis of how predictive advertising compromises a customer's control over his or her information. To the extent that such advertising is based on information gathered, analyzed, and used by any entity (whether an edge provider or an ISP) without disclosure to a third party, there is no loss of control of information

[201] *See* CTIA Opening Comments at 119-35.

[202] *See* Public Knowledge Comments at 6-11.

[203] *See Swire Report* at 14.

or enhanced risk of breach. And to the extent that such advertising requires some amount of disclosure of identifiable information to a third party, the predictive quality of the advertising does not change the privacy calculus, because there is no evidence in the record that a majority of customers do not want, let alone do not expect, sophisticated advertising to become more common. To the contrary, as noted above, the only evidence in the record addressing customer expectations and preferences regarding predictive advertising conclusively demonstrates that consumers find such advertising beneficial: Public Knowledge notes that advertisers using predictive analytics experience a substantial increase on their return on investment. That outcome would not have occurred if consumers had not found such advertisements useful.[204] Such advertising also has other beneficial effects, including driving economic growth.

Further, no commenter attempted to create a record that demonstrates *when* or *how* the purported harms that *theoretically could* arise from increased use of predictive advertising (such as self-censorship, surveillance, etc.) become real or even likely, as opposed to merely hypothetical. Such concerns appear to be the atmospherics for this proceeding, but that is insufficient under the APA; a reviewing court could not defer to the Commission's predictions about the hypothetical effects of such advertising without some evidence.

2. ISPs Lack Incentives, and Often the Technical Infrastructure, to Engage in the "Parade of Horribles" in the NPRM and Supportive Comments.

Commenters that support the NPRM also failed to distinguish between the *capacity* of ISPs to engage in certain practices (such as deliberate collection of highly sensitive information, constant use of DPI, and so forth) and their *incentives* actually to do so. This distinction is critical, however, because it too demonstrates that asymmetric regulation of ISPs is unnecessary.

[204] *See* Public Knowledge Comments at 8.

For example, although the Proposed Rules do not account for the sensitivity of customer data, the Commission at least acknowledged that sensitivity is a relevant consideration,[205] and has been urged by CTIA, the FTC, and others to incorporate sensitivity as the touchstone of any final rules.[206] As will be discussed at greater length below, even Public Knowledge endorsed this principle, at least in the abstract.[207] Neither the Commission nor any supportive commenter, however, articulated—let alone attempted to articulate—a coherent account of why ISPs ever would deliberately collect and use sensitive information (*e.g.*, health information, financial information, the information of children, or precise geo-location information). What of the specter of ISPs' constant monitoring of online activity through DPI? Far from being an actual possibility, such monitoring is neither financially practical nor strategically useful for ISPs. Indeed, even according to Public Knowledge's preferred academic, the issue is a "red herring."[208] That is because the costs of using DPI for all connections, storing all of the monitored information for analysis, and conducting that analysis for use in marketing are prohibitive and would not generate a return on investment:

> First, DPI is typically not widely deployed in many ISP networks. Several ISPs have stated in various forums that DPI capabilities are deployed on less than 10% of the link capacity in an ISP network; even if DPI were widely deployed, the cost of retaining the traffic that could be collected from DPI for any length of time would be prohibitive. Second, contrary to some conventional beliefs, ISPs often do not retain much of the data they collect because the cost of doing so can be substantial; at some of the networking companies I have worked for, we have, in some cases, had to

[205] *See* NPRM ¶¶ 20-21 (explaining that "the NPRM recognizes that the sensitivity and confidentiality of personal communications is one of the oldest and most established cornerstones of privacy law" and requesting comment on "whether there are particular types of information . . . [that] are so sensitive that they deserve special treatment").

[206] *See supra* Part I.B.

[207] *See infra* note 229 and accompanying text.

[208] Feamster Comments at 6; *see also* Public Knowledge Comments at 9-11 (relying on analysis by Professor Feamster to criticize *Swire Report*).

> argue stridently that certain data be retained so that we could use it for a study or a research project.[209]

Moreover, engaging in routine monitoring would expose ISPs to financial risk, because it would potentially deprive them of safe harbor status under the Digital Millennium Copyright Act with respect to copyright infringing activities on their networks.[210]

As important, ISPs *do* have incentives to adopt and adhere to responsible privacy and data security practices. That is because the status quo business model for all ISPs is to develop ongoing relationships—and, in the case of larger ISPs, ongoing *multi-service* relationships—with customers. The only way to retain relationships is through customer-friendly practices and a strong reputation.[211] The existing privacy policies of the four largest providers and the existence of industry-wide self regulatory regimes reflect the force of these incentives.[212] In contrast, many edge providers have ephemeral relationships with customers and therefore can be expected to maximize data revenue sources, notwithstanding customer interests in privacy and data security.[213] And those edge providers that also depend on ongoing relationships—such as social media platforms—can take advantage of the network effects that keep their users from switching.

---

[209] *See* Feamster Comments at 6.

[210] *See* WTA - Advocates for Rural Broadband Comments at 2 ("WTA Comments").

[211] *See* Beales Comments at 6 ("[ISPs] are large, typically publicly traded corporations with high levels of firm-specific reputational capital. Such firms are subject to reputational damage if they are seen as engaging in conduct that is harmful to consumers, and are thus less likely than other firms, *ceteris paribus*, to do so.").

[212] *See* CTIA Opening Comments at 108 & n.337.

[213] *See* Beales Comments at 6 ("[E]dge providers, ad networks and other online entities . . . have only ephemeral relationships with consumers, [whereas] [ISPs] have ongoing business relationships with their subscribers and therefore must safeguard their privacy in order to retain their trust and their business. The fact that firms with high levels of repeat purchasers are relatively unlikely to engage in opportunistic behavior towards consumers is widely agreed upon in the consumer protection literature.").

C. There Is No Record Evidence That Customers View ISPs as a Unique Privacy Risk or Otherwise Expect or Prefer Asymmetric Regulation of ISPs.

An alternative basis in the NPRM and supportive comments for adoption of the Proposed Rules is that the Rules reflect customer expectations regarding how ISPs will use and disclose information obtained through the provision of service. As noted, however, these assertions are generally conclusory and uncited, or, where they are cited, inadequately supported. For example, New America OTI claimed that focus groups conducted by the City of Portland offered "clear" evidence that consumers' concerns about their broadband providers' privacy practices "can chill consumers' willingness to get online and to use the network to its full potential."[214] New America OTI cited not the study, however, but a blog post that offers conclusory statements about the study. CTIA located the underlying report,[215] which offers *no* support whatsoever for either the conclusory statements on the blog post or New America OTI's claim. Indeed, the word "privacy" does not appear *anywhere* in the report. To be clear: CTIA is not aware of any comment quantitatively demonstrating—or even purporting to demonstrate—that customers' expectations of privacy are different vis-à-vis their ISP and other entities in the online ecosystem. In contrast, however, PPI conducted a rigorous survey on this question and found that customers overwhelmingly expect and prefer uniform regulation of data practices in the Internet ecosystem.[216]

As CTIA and many other commenters argued, asymmetric regulation that conflicts with customer expectations would be counterproductive. In the event that the Proposed Rules are adopted, many consumers would lack the time or interest to appreciate that ISPs would need to

[214] New America OTI Comments at 10-11.

[215] JLA Public Involvement for Office of Community Technology, City of Portland, *Digital Equity: Needs and Opportunities Report* (Aug. 24, 2015), https://www.portlandoregon.gov/revenue/article/545834.

[216] *See* PPI Comments at 2.

obtain different levels of consent to use or disclose information for routine practices that previously had not required opt-in consent—let alone that withholding consent from an ISP would do nothing to prevent edge providers from using or disclosing that same information without missing a click. The inevitable result of such asymmetry will be confusion and uncertainty, which in turn can lead to customer carelessness, compromising the very privacy values that the Commission purports to protect.[217]

D. The Record Strongly Supports That Any Rules the Commission Adopts Should Reflect Two Fundamental Principles: Data Sensitivity and Flexibility to Adapt Data Practices.

As CTIA set forth in its Opening Comments, any rules that the Commission adopts in this proceeding should be based on the sensitivity of the data protected and should provide the flexibility that ISPs need to adapt and innovate.[218] The benefits of such an approach are manifold: it would protect customer privacy in a manner consistent with domestic and international privacy regimes; it would ensure ISPs can address evolving data security threats and risks; it would facilitate competition and innovation in a dynamic market; and it would secure the buy-in of not only privacy advocates but also industry.

---

[217] *See, e.g.*, CTIA Opening Comments at 116 & n.364; Mobile Future Comments at 7 ("Applying new and different rules to one subset of the complex Internet ecosystem while other participants in the ecosystem remain subject to the FTC's existing regime will create customer confusion" which can result in "frustration."); Consumers' Research Comments at 10-11 ("The proposed regime is complex and confusing, both on its own and in conjunction with policies that would govern edge providers. As a court said years ago about early CPNI efforts, 'it defies credulity that consumers will understand the complicated regulatory framework sufficiently to effectively implement their preferences.'"); *id.* at 14 (explaining that asymmetric regulation "will be difficult for consumers to appreciate" and "may lead consumers to assume that the FCC's restrictions apply to all online activity" leading consumers "to be less vigilant online"); Consumer Technology Association Comments at 3-4 ("[D]espite the fact that frameworks in place today are currently working to protect consumers, the Commission proposes to muddy the regulatory waters with onerous and prescriptive rules. This proposed approach will inhibit the ability of [ISPs] to innovate and will confuse consumers, all with little to no benefit to consumers."); *cf.* Level 3 Communications Comments at 8 (explaining that differentiated restrictions for uses for broadband and voice services could result in customer confusion).

[218] *See* CTIA Opening Comments at 94-97.

As explained in the *FTC Report*, the touchstone of privacy protection should be customer control over the deliberate use of their sensitive information.[219] Even Public Knowledge did not challenge this general proposition in its comments.[220] Some commenters suggested, however, that there is a tension between advocating for a regime that is technology neutral and that also differentiates between uses of sensitive and non-sensitive data.[221] Nothing could be further from the truth. The FTC administers a technology neutral, uniform regime, and likewise has adopted rules pursuant to, and enforces, sectoral statutes that relate to uniquely sensitive data, including health data, financial data, and children's data.[222]

In its comments, the FTC recounted that certain information that the Commission purports to define as "customer proprietary information"—*e.g.*, name, address, and phone number—qualifies as PII under various privacy statutes and regulations.[223] CTIA does not disagree with this proposition, but it is a non-sequitor. Under the privacy regime articulated in the *FTC Report*, those data are not sensitive, so their use within a first-party marketing context should be subject to implied consent.[224] Moreover, as noted, the Commission has previously

[219] *See FTC Report* at 47; *see also* CTIA Opening Comments at 119-23.

[220] *See* Public Knowledge Comments at 26 ("We agree with the FTC's recognition that certain types of data are, *prima facie*, more sensitive than others."). New America OTI took a slightly different approach, arguing that in modern privacy regimes, customer expectations are more relevant even than the sensitivity of data. *See* New America OTI Comments at 7 ("Over the past several years, the privacy field has shifted toward an understanding of privacy expectations as anchored to the *context* in which information is shared, rather than to the sensitivity of a particular piece of information."). It is unnecessary for CTIA to wade into this theoretical debate. As CTIA set out more fully in its opening Comments, the Proposed Rules reflect neither that heightened protections should be available for sensitive data nor that protections should reflect customer expectations.

[221] *See generally* Peha Comments (arguing that regulatory parity is an unnecessary goal).

[222] *See* FTC Comments at 3-4.

[223] *See id*. at 11.

[224] *See FTC Report* at 36.

concluded that these elements are unambiguously excluded from the category of CPNI,[225] and the Commission lacks authority to protect any category of information other than CPNI.[226]

Further, consistent with the other major privacy regimes that exist in the United States and abroad, restrictions on legitimate and routine uses and disclosures of information should be flexible to promote innovation and competition. Many commenters agreed.[227] Moreover, this general principle is particularly salient in the context of the communications and online advertising markets, which are nascent, dynamic, and evolving—and also are major drivers of economic growth.[228] In this respect, commenters missed the mark by assuming or expressly claiming that ISPs provide (or should provide) purely transmission without any ancillary services;[229] it is not in the public interest to so limit ISPs' business models. ISPs also need flexibility to adapt to their customers' evolving expectations of privacy—in particular, they must be able to provide the kinds of notices that will best be understood and that will be delivered to customers through channels that make sense in the context of the relationship with their ISP. ISPs also need to have the flexibility to provide choice mechanisms that take advantage of new technologies.

---

[225] *See* CTIA Opening Comments at 45; *see also 1998 CPNI Order*, 13 FCC Rcd at 12,395-96 ¶¶ 8-9.

[226] *See supra* Part II.A and accompanying text (addressing Section 222(a) arguments).

[227] *See* Consumers' Research Comments at 2 ("Rather than adopt prescriptive, ex-ante regulation, the FCC should consider the [FTC's] more flexible approach, which considers consumer harm and cost-benefit analysis."); Wright Comments at 6 ("Rather than imposing a rigid regulatory framework, the FTC focuses on the sensitivity of the data at issue and the potential harm to consumers deriving from disclosure or misuse of that data. In this way, the FTC looks to consumer welfare as its lodestar. . . . Such an approach allows innovative technology companies freedom to responsibly use data in ways that result in new products, lower prices, and increased consumer welfare."); Consumer Technology Association Comments at 3 (urging Commission to adopt more flexible approach to "achieve [the] desired goals of transparency, choice, and security without intrusive, burdensome regulation that would have significant negative consequences for consumers"); Mobile Future Comments at 9-10 (urging Commission to engage in multi-stakeholder process to develop flexible, uniform, technology neutral rules).

[228] *See* CTIA Opening Comments at 94-97, 119-36.

[229] *See, e.g.*, Greenlining Institute and Media Alliance Comments at 15-23 ("Greenlining Comments").

V. THE RECORD DOES NOT SUPPORT THE COMMISSION'S OVERLY PRESCRIPTIVE PROPOSED RULES REGARDING NOTICE AND CHOICE.

A. The Commission Should Adopt Flexible Notice Rules.

Transparency and notice are fundamental principles of the FTC's privacy regime, and CTIA and its members incorporated these principles into the consensus proposal.[230] As CTIA explained in its Opening Comments, the Proposed Notice Rules—whether related to notice of privacy policies and changes thereto, notice of uses of information to obtain consent, or notice of data breaches—are not in the public interest, because they are overly prescriptive, likely to result in consumer notice fatigue, and will quickly become outdated.[231] The NPRM expressly acknowledges but simultaneously understates these risks.[232] The Commission would be better served by recognizing, as the FTC has, that ISPs know their customers better than the Commission, and therefore should be entrusted to ensure that customer notice is effective in terms of timing, format, and so forth.

More specifically, a mandated, standardized, lowest-common-denominator approach to notice is inappropriate for ISPs.[233] That is because different ISPs offer different services and different bundles of services—and are constantly updating their services and bundles—frustrating the efficacy of any template. Moreover, past regulatory experimentation with standardized notice forms has not been successful.[234] CTIA and its members are not opposed to the use of a standard form as a safe harbor,[235] but urge the Commission to allow some variation

---

[230] *See* CTIA Opening Comments, App. A.

[231] *See id.* at 98-101.

[232] *See* NPRM ¶ 23 ("Recognizing the harms inherent in over-notification (or 'notice fatigue'), the NPRM proposes to adopt a trigger as to when notice is needed, and seeks comment on under what circumstances [ISPs] should be required to notify customers of a breach of their [proprietary information].").

[233] *See* FTC Comments at 12-13, 26.

[234] *See* CTIA Opening Comments at 102 & n.320.

[235] *See* FTC Comments at 14.

in wording. For similar reasons, the Commission should not mandate dashboards, which are not desired or used by customers; are onerous and expensive for providers; and quickly become obsolete.[236] Further, dashboards can present security risks by concentrating customer information in a central location which can become a target for hackers.[237] To the extent that industry develops such tools, it needs flexibility, not mandates. Finally, even pro-regulatory commenters did not make the adoption of a standardized notice form or a dashboard a priority.

CTIA likewise does not object to the proposal that ISPs be required to provide advance notice of material, *retroactive* changes to privacy policies.[238] This proposal is consistent with the FTC's privacy regime.[239] But CTIA believes that requiring *60-day advance notice* is unnecessary, inconsistent with customer expectations and current business practices, and counterproductive. Such notices would become stale. Moreover, given the ease of switching providers, customers do not need more than 30 days to respond to a retroactive material change to a provider's privacy policy of which they disapprove. CTIA also respectfully submits that the calculus is different for material *prospective* changes to privacy policies. Certainly, customers should receive notice of such changes, but the level of consent required for such change should not depend on the *fact* of a change; instead, it should depend on the *nature* of the particular change. That is to say, for example, that a material prospective change in how an ISP uses customer information to prevent fraud or combat cybercrime might be appropriate following notice on a theory of implied consent; a material prospective change in how an ISP uses precise

[236] *See* CTIA Opening Comments at 104-05.

[237] *See id*. at 151-53; Consumers' Research Comments at 21; American Cable Association Comments at 26–27. The few commenters urging mandatory dashboards ignored their potential dangers, *see, e.g.*, Privacy Rights Clearinghouse Comments at 4 (supporting the dashboard but failing to address dashboard security), and offered arguments that, in some cases, are downright frivolous, *see* EPIC Comments at 11–12 (arguing for a right to know the specific logic of processing and algorithms used by ISPs).

[238] *See* FTC Comments at 14.

[239] *See FTC Report* at 57-58.

geo-location information to market services to a customer, on the other hand, might reasonably require notice and consent.

B. The Proposed Choice Rules Are Flawed in Design and Should Be Abandoned.

As CTIA and others explained in their opening comments, the Proposed Choice Rules suffer from numerous shortcomings. In addition to being based on mistaken assumptions about the nature of the online ecosystem and the broadband market, addressed above, the Proposed Choice Rules are unnecessary, would not enhance privacy, do not reflect customer expectations, and would cause substantial public interest harms.

As a threshold matter, the NPRM reveals that the Commission started from two flawed assumptions about the status quo—namely, that customers currently receive no protections from their ISPs and that opt-in is the only effective form of choice. Numerous commenters, however, confirmed that ISPs have developed best practices with respect to the uses and disclosures of customer information through experimentation and self-regulation.[240] And the FTC's fact-gathering and enforcement experience confirms that for all but a very small subset of uses and disclosures of specific categories of information, requiring opt-in consent is overly restrictive.

Moreover, separate from these flawed baseline assumptions, the mere fact that the Proposed Choice Rules are a radical departure from the FTC's approach to privacy is itself a gating problem. As CTIA explained in its Opening Comments, the FTC developed its approach to privacy following a multi-year process that involved not just an extensive comment period,

[240] Consumer Technology Association Comments at 12-13 ("[I]ndustry players across [the] Internet ecosystem have worked for years devising privacy best practices, understanding that good privacy practices are essential to maintaining a customer's trust and loyalty."); Verizon Comments at 6-7 (describing efforts of Verizon and other broadband providers to comply with the FTC privacy framework and to urge the Commission to consider measures that will offer consumers consistent protection across the Internet); Beales Comments at 2-3 (explaining that NPRM failed to identify any inadequacies or adverse consequences of current privacy practices of broadband providers); ITIF Comments at 12 ("This may seem counterintuitive, but companies that do not face sector-specific regulations are still face [sic] many incentives to devise effective privacy practices . . . . Regulated industries tend to focus narrowly on compliance and reducing the risk of a data breach, rather than focusing on how to design products and create internal policies that meet the privacy expectations of their consumers.").

but also workshops, discussions, and specific topic breakouts.[241] The resulting framework, like privacy regimes under federal law and international law, bases the extent of protection accorded to customers on the sensitivity of their data being used or disclosed. In its comments in this proceeding, the FTC strongly urged the Commission to move in this direction[242]—a recommendation that CTIA echoes.

The Proposed Choice Rules also fail to reflect customer expectations. The market for communications services is dynamic and converging, and customers understand both that services are typically bundled and that ISPs can provide not just traditional services but also innovative and related products and other offerings. Restricting ISPs' abilities to market new offerings to customers according to customers' preferences will harm consumers.[243] There also is no reason to restrict an ISP to marketing services to which a customer already subscribes; competition in the market is robust and dynamic, and most first-party marketing occurs within the context of a provider-carrier relationship.

Additionally, as many commenters noted, the Proposed Choice Rules also will harm consumers in the form of higher prices for services. Because ISPs operate in multi-sided markets, and can engage in commercial transactions with not just consumers but also edge providers and others, ISPs should have the ability to experiment with new, innovative business models. The identification and implementation of new revenue streams will allow ISPs to reduce customer-facing prices.[244] Moreover, such experimentation will support further

[241] *See* CTIA Opening Comments at 120 & nn.369-71.

[242] *See supra* Part II.B.

[243] *See* CTIA Opening Comments at 126-27; Consumer Technology Association Comments at 8-10; Verizon Comments at 24-28; Wright Comments at 20-24.

[244] *See* Wright Comments at 7-8; Beales Comments at 8 ("The online market is a multi-sided market. . . . Competition takes place along multiple dimensions."); ITIF Comments at 6 ("[B]roadband providers exist within a broader system of modular platforms competing along different fronts.").

competition—not just between and among ISPs, but also in other markets, including for online advertising.[245]

Finally, the Proposed Choice Rules will have absurd (and presumably unintended) effects with respect to when and how ISPs can share information with affiliates, agents, vendors, and other third parties.[246] For example, the Commission could not have intended to propose rules that would require a customer to provide opt-in consent before an ISP could send a promotional offer through the U.S. Mail, but that is a plausible interpretation of how the Proposed Choice Rules operate. Other commenters agreed with CTIA's concerns, explaining that the Proposed Choice Rules depend on antiquated notions of how ISPs operate, even when it comes merely to the delivery of broadband service and related internal operations.[247] Those commenters that supported the NPRM, however, failed to identify how the disclosure of information to particular types of third parties (especially vendors) creates additional privacy risk—especially given the broad definition of "customer proprietary information" in the NPRM.

The Commission also should reject comments calling for the adoption of a new quantitative or qualitative definition of "affiliates" in the context of CPNI rules and restrictions. Doing so would risk considerable confusion among carriers and customers. Moreover, the Commission can achieve its privacy objectives through the adoption of careful rules that specifically identify how restrictions operate with respect to other parties (whether affiliates or otherwise), without changing the regulatory definition of "affiliate," which is consistent across the Commission's policy areas. Indeed, the Commission should proceed with particular caution

[245] *See* CTIA Opening Comments at 127; Information Accountability Foundation Comments at 4; Beales Comments at 8.

[246] *See* CTIA Opening Comments at 127-31.

[247] *See* Consumer Technology Association Comments at 8-9 (identifying hypothetical uses that are in "a regulatory gray area" under the Proposed Rules); Verizon Comments at 26-27 (noting that broadband providers often utilize separate corporate affiliates to provide different aspects of an integrated service, such as billing or purchasing).

in this area, because changing the definition of "affiliate" could introduce considerable confusion into other areas that the Commission regulates, such as spectrum use and allocation.[248]

C. The Commission Should Reject Public Knowledge's Assertion That Rules Must Treat All Information as Sensitive as a Prophylactic Measure.

Public Knowledge argued in its comments that the Commission cannot adopt rules that differentiate between sensitive and non-sensitive customer information, because such rules effectively would require ISPs to utilize DPI to determine the sensitive nature of customer information before using it, which, according to Public Knowledge, is contrary to the spirit and letter of Section 222.[249] CTIA appreciates Public Knowledge's admission that it is a bedrock principle of privacy regulation that certain information is more sensitive than other information—and that heightened privacy protection should be afforded to protect the deliberate use or disclosure of sensitive information.[250] Furthermore, CTIA does not disagree with the proposition that ISPs should not be required to monitor traffic in order to determine its sensitivity

[248] *In re Policies Regarding Mobile Spectrum Holdings, Expanding the Economic and Innovation Opportunities of Spectrum Through Incentive Auctions*, Report and Order, 29 FCC Rcd 6133, 6244-45 ¶¶ 300-302 (2014) (discussing application of ownership rules to Commission review of competitive bidding for spectrum licenses and secondary market spectrum transactions).

[249] *See* Public Knowledge Comments at 24. The flaws with Public Knowledge's statutory argument about the use of DPI are addressed, *supra*, in Part II.D.1. Paul Ohm makes a related argument in his Reply Comments, urging the Commission not to distinguish between sensitive and non-sensitive data. Ohm Reply Comments at 11. Ohm reasons that the "great virtue of the proposed opt-in rule [for all data] is that it draws bright lines." *Id.* As noted above, however, the Commission's proposed choice rules contravene the First Amendment precisely because they prohibit more commercial speech than is necessary to advance the Commission's purported interest in protecting consumer privacy (*i.e.*, prohibit the use of a broad category of data regardless of the risk of privacy harms) . *See infra* Part III. B. Moreover, as explained above, the Commission's proposed rules diverge without justification from the FTC's approach, which recognizes that privacy risks vary depending on the nature of the data used and disclosed, and rules regulating marketing activities involving personal data likewise should be calibrated to protect consumers while allowing companies to engage in legitimate business activities within the context of their relationships with their customers. *See infra* Part I.B, D. The FTC's requirement that companies obtain opt-in consent for *some*, but not all, uses of sensitive data is not difficult for companies to implement, or for the Commission to enforce, because it turns on whether the company intended to target marketing to the consumer based on information inferred from the sensitive data. *FTC Report* at 47-48.

[250] *See* Public Knowledge Comments at 25-26.

before use.[251] Such a requirement could result in unnecessary monitoring that would not otherwise occur, and indeed would impose unreasonable and unnecessary costs.[252]

Those points of agreement aside, however, Public Knowledge took this argument to an unnecessary conclusion that is inconsistent with the *FTC Report*. Specifically, the FTC has never endorsed heightened protections every time a provider uses sensitive information; instead, heightened protections are appropriate when a provider *deliberately* uses sensitive information *qua* sensitive information.[253] Public Knowledge failed to make that distinction in its comments, instead arguing for a blanket rule that would give even greater market power to those entities that have access to the very information that Public Knowledge wants to protect and that already dominate the online advertising market.[254] Public Knowledge elsewhere purported to support a regulatory level playing field to ensure a fair and competitive marketplace for online services. As explained above, its proposals would do just the opposite, however.[255] Additionally, at the very least, Public Knowledge's argument for prophylactic coverage of all information, including non-sensitive and even *already public* information, demonstrates that the Proposed Rules cannot survive First Amendment scrutiny even under *Central Hudson*; it is now conceded that the Proposed Rules would regulate categories of speech that lack any nexus to privacy and more speech than is necessary.

---

[251] *See Id*.; EFF Comments at 5 (arguing that if the adopted rules protect customer proprietary information as proposed, there is no need to differentiate between sensitive and non-sensitive information, and further arguing that any such distinction would require ISPs to inspect data).

[252] *See FTC Report* at 47. Public Knowledge urged the Commission not to "[allow] an ISP to actually read the information in the customer's bit-stream." Public Knowledge Ex Parte Letter at 2. Such a rule would be untenable, however. ISPs must engage in some reading of such information to render broadband service, which uses are outside the scope of restriction under Section 222.

[253] *See FTC Report* at 47.

[254] *See* Public Knowledge Comments at 24-26.

[255] *See supra* at Part IV.A-IV.B.

D. The Commission Should Reject Calls for Even More Routine Use of Opt-In Protections and Just-in-Time Notice for Uncontroversial Uses and Disclosures.

Amazingly, several commenters appear to have concluded that the NPRM does not go far enough when it comes to requiring opt-in consent for uses of customer information. For example, some commenters urged the Commission to require opt-in consent for *all* marketing or for any use other than the delivery of service itself.[256] The Commission should reject these requests.

Indeed, these requests appear to be based on the uncited and unsupported theory that the context of the provider-customer relationship is limited to the provision of broadband service, and, accordingly, that implied consent is appropriate only for using information for that purpose. Admittedly, the *FTC Report* emphasizes the importance of context in determining the appropriate level of protection, but it also expressly concludes that, regardless of provider *type*, most first-party marketing occurs within the provider-customer relationship.[257] There is no reason that should be any different for ISPs than it is for any other type of provider.[258] Other privacy regimes, including the EU GDPR, allow companies to engage in legitimate business uses of information without providing customers with an opportunity for prior choice, and they, too, generally treat first-party marketing as a "legitimate business use."[259]

---

[256] *See, e.g.,* Center for Digital Democracy Comments at 16; Center for Democracy and Technology Comments at 21-24; Free Press Comments at 13; New America OTI Comments at 36-41.

[257] *FTC Report* at 40 ("[M]ost first-party marketing practices are consistent with the customer's relationships with the business and thus do not necessitate consumer choice.").

[258] In its comments, the FTC specifically cited the portions of the *FTC Report* which conclude that, as a general matter, all first-party marketing occurs within the context of the provider-customer relationship, without regard to the type of service or product being marketed. *See FTC Comments* at 16 n.65.

[259] *See* Regulation (EU) 2016/697 of the European Parliament and of the Council Recital 47, Arts. 6, 21 (Apr. 27, 2016) ("EU GDPR"), http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (codifying marketing as lawful processing without prior consent, so long as customer has right to object).

One reason that privacy regimes reserve opt-in requirements for practices that most directly implicate customer privacy is that such requirements are burdensome for consumers. Indeed, commenters that supported further use of opt-in consent have understated the risk of notice fatigue and customer frustration that would ensue if customers were regularly required to opt in to practices either that they have previously opted in to or that other providers engage in *without* providing a prompt for prior explicit consent.[260] Commenters that supported increased use of opt-in requirements also fundamentally misapprehend the significance of the fact that customers might not opt in to certain uses or disclosures. Customers' failure to opt in does not show that customers prefer that providers not engage in those practices; instead, it demonstrates the transaction-related and other inertia costs associated with changing privacy preferences.[261] In other words, many consumers are privacy neutral and accordingly are unlikely to select any option that requires affirmative action.[262] A privacy regime based on opt-in consent therefore unfairly imposes the costs for privacy-conscious consumers onto other consumers.[263]

These costs are not insignificant. *Any* opt-in requirement imposes substantial administrative and transaction costs on ISPs, which ultimately will be passed onto consumers,

---

[260] *See, e.g.*, Consumer Technology Association Comments at 11 (adding to voluminous notices consumers already receive "will leave them desensitized, tuned out, and unable to differentiate between consent requests that involve fairly innocuous data versus those that ask to use highly sensitive data"); Consumers' Research Comments at 26-27 ("Over-notification is not just irritating to consumers; it can also harm them by degrading consumers' experiences with the BIAS provider, making them less likely to pay attention to notices that warn of actual harm").

[261] Beales Comments at 11 ("With privacy preferences, the most important cost of exercising choice may well be the cost of considering the issue at all. . . . Consumers may decide that a decision is not worth the cognitive costs of thinking about an issue at all, particularly when the stakes are small. The default rule is therefore likely to dominate choices. If the default is no sharing, most consumers will end up not sharing."); Wright Comments at 14 ("[F]or many consumers, it is simply not worthwhile to incur the transaction costs of opting in—devoting time and attention to understanding a privacy policy's implications and taking the steps necessary to provide the required consent—because they understand that they will receive the same service from the ISP whether they opt in or not, and they obtain no clear benefit from expending the resources necessary to opt in. . . . [T]hat failure simply indicates that the cost of opting in is high; it does not shed any light on consumers' actual preferences or otherwise indicate that consumers' privacy interests have been better served.").

[262] *See* sources cited, *supra*, note 261.

[263] *See* Wright Comments at 16-20.

and locks in existing business models, which also, in turn, would increase retail prices for consumers.[264] Because retail prices exert tremendous influence on further broadband adoption,[265] further use of opt-in requirements is inconsistent with the Commission's goal of expanding the availability, and increasing the adoption of advanced communications technologies.

E. The Commission Should Not Retain Its Proposed Distinction Between Communications-Related and Other Services, But If It Does, It Should Define "Communications-Related" Broadly.

CTIA, like the FTC itself, recommended that the Commission not adopt the Proposed Rules that differentiate between using "customer proprietary information" to market communications-related and non-communications-related services.[266] The Commission would be better served by adopting final rules that reflect the sensitivity of information being used, rather than vestigial marketing distinctions from an antiquated set of traditional voice regulations. If, however, the Commission elects to retain the Proposed Choice Rules, it must define "communications-related" broadly to encompass any product or service offered by a telecommunications carrier or its affiliates.

Various commenters that generally supported the Proposed Choice Rules also asserted that if the Commission adopts an opt-out regime for uses and disclosures of information to affiliates for purposes of marketing communications-related services, then that category must be

[264] *See id*. at 20-21 (explaining that the NPRM would "raise retail broadband prices" through direct and indirect effects on consumer and ISP behavior); ITIF Comments at 6 (noting that Proposed Rules could "lock BIAS providers out of data-driven business model innovation").

[265] *See, e.g.*, John B. Horrigan & Maeve Duggan, *Barriers to Broadband Adoption: Cost Is Now a Substantial Challenge for Many Non-Users*, Pew Research Center (Dec. 21, 2015), http://www.pewinternet.org/2015/12/21/3-barriers-to-broadband-adoption-cost-is-now-a-substantial-challenge-for-many-non-users/.

[266] *See* CTIA Opening Comments at 123-27; FTC Comments at 22-23 (explaining that while such a framework provides a bright line, it "does not reflect the different expectations and concerns that consumers have for sensitive and non-sensitive data" and accordingly "could hamper beneficial uses of data the consumers may prefer, while failing to protect against practices that are more likely to be unwanted and potentially harmful" and providing examples).

defined narrowly—excluding, for example, over-the-top and streaming services,[267] customer premises equipment ("CPE") and information services,[268] or even anything other than telecommunications, cable, and satellite services.[269] These commenters did not, however, ground their proposals in any coherent theory of customer privacy. Indeed, what is most striking about these comments—like the NPRM—is the utter lack of evidence suggesting that such exclusions would address a privacy risk, on the one hand, or reflect customer expectations or even preferences, on the other.[270] This absence of evidence is fatal from a First Amendment standpoint, given that the burden is on the censoring party to establish that regulations substantially advance a legitimate interest. But the gaps in the record also call into question the soundness of the Proposed Rules from an APA perspective.

The reason commenters failed to identify substantial evidence that customers have different expectations regarding the marketing of communications-related and non-communications-related services is that customers increasingly understand and expect that services will be bundled in a converging communications market. A broad and flexible approach to "communications-related services" therefore would be consistent with not just the FTC's conclusion that first-party marketing generally occurs within the context of an existing provider-customer relationship,[271] but also with general industry trends and customer demand.[272]

---

[267] *See* Public Knowledge Comments at 31.

[268] *See* EFF Comments at 6.

[269] *See* New America OTI Comments at 25.

[270] For example, in each of the Comments cited, *supra*, in notes 267 through 269, there is no citation to quantitative or qualitative evidence that supports the proposed cabining of "communications-related" services.

[271] *See supra* notes 257-259 and accompanying text.

[272] CTIA reiterates, however, that its primary position is that the distinction between communications-related and non-communications-related services reflects neither traditional privacy interests (*i.e.*, differentiating between sensitive and non-sensitive data), nor customer expectations, and therefore the adoption of this distinction would fail for want of reasoned decision making. *Motor Vehicle Mfrs. Ass'n of the U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*,

If anything, commenters' support for a strict definition of communications-related services appears to have been animated by an unstated concern that ISPs today, like ILECs in 1996, can use "customer proprietary information" to exert anticompetitive pressures in markets for non-communications-related services. Public Knowledge's comments, in particular, suggest an argument that Section's 222 competition purpose augurs in favor of narrowly interpreting "communications-related services."[273] There are two related problems with the Commission's accepting this reasoning. The first is that the purpose of this proceeding is the protection of *privacy*. That is not to say the Commission necessarily could not have instituted a rulemaking about competition in the markets for non-communications-related services, but the Commission did not do so, and it cannot repurpose this proceeding at such a late stage. The second is that no commenter that urged adopting a narrow definition of communications-related services offered any evidence that ISPs have the ability to foreclose competition in the market for OTT and streaming services, CPE and information services, or any other products and services, particularly when edge providers have access to, and use, the same consumer data to market such services.

F. Despite Some Commenters' Claims, Opt-Out Is a Meaningful Form of Consent That Best Balances Privacy Interests and Costs.

Several commenters replicated an error in the NPRM by assuming that only opt-in consent is "meaningful."[274] These arguments should not be countenanced. To be clear, CTIA is not arguing that opt-out consent should be a default requirement for routine uses and disclosures of information. Instead, as CTIA argued in its Opening Comments, most uses should continue

---

463 U.S. 29, 43 (1983) (describing that agencies must rely on factors intended by Congress, consider important aspects of problem to be addressed, and provide cogent explanations for decision making).

[273] *See* Public Knowledge Comments at 31.

[274] *See, e.g.*, Comments cited, *supra* note 256.

based on a theory of implied consent.[275] That is the general rule under the FTC privacy regime and, indeed, many privacy regimes in the United States and abroad.[276]

If, however, the Commission determines that there is a record supporting that certain uses and disclosures present a substantial risk or material deviation from customer expectations—which CTIA respectfully submits, there is not—it should adopt opt-out consent as the appropriate approval mechanism. Opt-out consent is appropriate because it strikes a fair balance: it is a robust protection for privacy-conscious customers, who can opt out of those uses and disclosures that are contrary to their preferences, but it also is fairer to privacy-neutral consumers, who are not required to bear privacy-conscious consumers' costs.[277]

Opt-out choice is also preferable in those instances (if any) where the need for enhanced protection is supported by substantial evidence, because opt-out choice is familiar to consumers and the Commission.[278] For example, the Commission and FTC both have experience jointly administering effective opt-out regimes—*e.g.*, the do-not-call list and CAN-SPAM regulations.[279] These regimes are also preferable from a First Amendment perspective, because they do not censor any more speech than is necessary (if any) to protect privacy.[280] And finally, the effectiveness of these regimes demonstrates that the Center for Democracy and Technology was wrong to claim that customers lack sophistication to make informed decisions;[281] even if true for customers in general, this assertion is demonstrably false for *privacy-conscious customers*.

---

[275] *See* CTIA Opening Comments at 117-18, 120-23.

[276] *See supra* notes 257-259 and accompanying text.

[277] *See supra* note 263 and accompanying text.

[278] *See* ITIF Comments at 17.

[279] *See* CTIA Opening Comments at 84-85.

[280] *See generally Mainstream Mktg. Servs., Inc. v. FTC*, 358 F.3d 1228 (10th Cir. 2004).

[281] *See, e.g.*, Center for Democracy and Technology Comments at 22-23 (discussing consumer capacity to engage in notice-and-choice decisions).

G. ISPs' Offers of Service with Financial Inducements or Other Privacy-Related Incentives Are Not Unique and Are in the Public Interest.

As CTIA has explained, the Commission lacks authority under Sections 222, 201, and 202 to restrict or prohibit ISPs from offering service with financial inducements or other incentives for customers to provide approval for the use and disclosure of their information.[282] Even if that were not the case, however, the Commission should not restrict or prohibit such offers, because they help address the digital divide, and because they are fully consistent with customer expectations.

ISPs do not offer financial inducements or incentives for any sinister or coercive reason. These offers are based on a simple economic calculus that when ISPs discover and achieve new revenue streams, they can concomitantly reduce retail prices for consumers. The same is true for other entities in the ecosystem. Indeed, there is nothing unique about ISPs' offering inducements or discounts in exchange for approval to use or disclose customer data—nor are such offers typically designed specifically to target vulnerable consumers. To the contrary, such offers are now a common feature of the Internet ecosystem: one billion Gmail users and more than 1.5 billion Facebook users have accepted effectively identical offers to obtain e-mail and social networking services without a monthly fee. The fact that ISPs historically have offered service exclusively for a fee does not mean that a fee-based model of service is inevitable or even desirable.

As argued by several commenters, these offers are also wins for consumers, and indirectly for the economy, because they have the effect of making broadband more accessible to low-income and minority consumers, for whom the price of service otherwise might be out of

[282] *See supra* Part II.

reach.[283] As the Commission well knows, broadband service affords consumers numerous advantages in terms of the delivery of social and government services; educational and professional opportunities; social, political, and civic engagement; and the consumption of news and content.[284] The Commission should laud the offer of service with *voluntary* incentives and inducements that may facilitate the delivery of these benefits to previously unserved or underserved communities.

The Commission should reject paternalistic claims that giving consumers the voluntary choice to accept incentives or inducements is tantamount to depriving lower-income consumers of "fundamental rights."[285] This is a rhetorical device that may be appealing when the "fundamental right" is described in the abstract—*i.e.*, as "privacy." At a more particularized level, however, this argument boils down to a claim that there is a "fundamental right to receive discounted service unaccompanied by certain forms of advertising or marketing from your ISP." To state this proposition is to refute it. Moreover, these commenters ignored the fact that the delivery of predictive advertising also can be in *the recipient's interest*; any streaming viewer who has ever elected to receive "relevant" advertisements implicitly knows as much. The salient point that commenters who criticized these offers missed is that the offers are *voluntary*; there is always a "choice," and it is paternalistic to claim that low-income consumers are not capable of assessing the benefits and costs of various service offerings and making the appropriate choice—especially where there is an option to change choices and service later in time.[286]

---

[283] *See* Mobile Future Comments at 7-8 (characterizing restrictions on voluntary sharing of information as particularly harmful to low-income consumers).

[284] *See In re Lifeline and Link Up Reform and Modernization, Telecommunications Carriers Eligible for Universal Service Support, Connect America Fund*, Third Report and Order, Further Report and Order, and Order on Reconsideration, 31 FCC Rcd 3962, 3966-68 ¶¶ 12-17 (2016).

[285] *See* Grant Comments at 5; ACLU Comments at 6; Consumer Watchdog Comments at 6.

[286] *See* Comments cited, *supra* note 107.

VI. PROPOSED DATA SECURITY RULES ARE NOT IN THE PUBLIC INTEREST.

A. The Record Confirms that the Data Security Proposals Are Deeply Flawed.

1. The Commission Proposal Abandons Federal Policy Promoting a Collaborative, Flexible, and Voluntary Approach to Cybersecurity.

Agility and flexibility—not static solutions—are the cornerstones of effective data security. Cybercriminals are constantly changing approaches, so network operators have to adjust defenses to manage complex networks.[287] The FTC emphasized the need for flexibility,[288] explaining that its approach gives "businesses the flexibility to tailor their programs to their particular circumstances."[289] Static rules will hurt security more than help.[290]

The Proposed Data Security Rules ignore current administration policy that promotes "multi-stakeholder collaborations between industry, and academia, and government to develop security and privacy frameworks."[291] Since the Commission issued the NPRM, other federal efforts have continued to promote collaborative and flexible solutions.[292] "Top-down regulation covering a specific communication technology is a significant departure from the Administration's approach."[293]

Remarkably, the proposal undermines the Commission's own efforts. It repudiates the work of Communications Security, Reliability and Interoperability Council ("CSRIC") IV,

---

[287] *See, e.g.*, Farsight Security Comments at 24; ITTA Comments at 22-23.

[288] FTC Comments at 27; *see also* Wright Comments at 6 (contrasting the FCC's "rigid" approach with the FTC's approach).

[289] FTC Comments at 27.

[290] Atomite Comments at 1 ("[H]ard and fast rules promulgated by government regulators . . . often lead[] to unintended collateral effects.").

[291] Internet Commerce Coalition Comments at 6.

[292] For example, the White House Precision Medicine Initiative Data Security Framework, released May 25, 2016, does not center around prescriptive rules and was developed through a collaborative interagency process. *See* Sylvia Mathews Burwell & Lisa O. Monaco, *Precision Medicine Initiative and Data Security*, Whitehouse.gov Blog (May 25, 2016, 3:00 PM), *https://www.whitehouse.gov/blog/2016/05/25/precision-medicine-initiative-and-data-security*.

[293] Internet Commerce Coalition Comments at 7; *see also* Direct Marketing Association Comments at 20 (noting that the Commission's approach contradicts efforts by President Obama).

which recommended several *voluntary* mechanisms to enhance Communications Sector risk management, including cybersecurity assurance meetings ("CAMs") protected under the Protected Critical Infrastructure Information ("PCII") administered by the Department of Homeland Security ("DHS").[294] FCC Chairman Wheeler told Congress that "there is no 'correct' or 'minimum' standard against which companies will be measured" in such meetings.[295] But the rules do just that: they impose "minimum"[296] requirements against which companies participating in CAMs necessarily will be measured. As a result, the NPRM undermines CAMs; as Commissioner O'Rielly noted, rules obviate the need for them.[297] Statements that the NPRM is consistent with past efforts are thus incorrect, and CTIA urges the Commission to reconsider the NPRM's misguided approach.[298]

There is no justification for the Commission to stray so drastically from federal and state[299] precedent. A few pro-regulation comments denigrate long-standing collaborative efforts, claiming that cybersecurity is "too important" for multi-stakeholder processes.[300] This is contradicted by real-world experience; the Commission has previously lauded the current

[294] *See Cybersecurity Risk Management and Best Practices*, CSRIC IV Working Group IV Final Report (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf. It recommended "the FCC, in partnership with DHS, participate in meetings with communication sector members, in accordance with PCII protections" or "another legally sustainable construct." *CSRIC WG 4 Final Report* (Mar. 2015) at 30 & n.37; *see also id*. at 6, 7, and 385.

[295] Written Question Submitted by Hon. Ron Johnson to Hon. Tom Wheeler at 9, http://www.commerce.senate.gov/public/_cache/files/6d3caac4-4a5c-4614-96b5-5f39eaef1379/8692A68293184CC559A17FFAB736FAB4.wheeler-qfrs.pdf.

[296] Proposed Rule 64.7005(a).

[297] CAMs would happen outside the PCII construct called for by CSRIC. Industry was working toward meetings, but regulation here threatens to chill cooperation on CAMs.

[298] *See* Charlie Mitchell, *Adm. Simpson: Privacy Proposal Consistent with FCC Cyber Approach, but Adjustments Are Possible*, Inside Cybersecurity (June 9, 2016).

[299] *See* State Privacy and Security Coalition Comments at 11*; see also* Direct Marketing Association Comments at 20.

[300] National Consumer League ("NCL") Comments at 10; *see also* Consumer Watchdog Comments at 6-7 (attacking Department of Commerce approach). In the next breath, however, NCL noted that consensus-based and voluntary frameworks like the FIPPs, "have a proven history of providing a baseline for robust data security." NCL Comments at 11.

approach as yielding effective security and strong consumer protection.[301] The Commission should not go down the NPRM path, which threatens to foster fragmentation by inviting additional, divergent regulation at the state level.

2. The Record Does Not Reveal a Problem that Justifies Imposing Rigid Security Solutions on ISPs.

There is no basis for prescriptive data security measures. The Commission fails to show that the market is not working, and the record provides no support for a drastic departure. No one has shown that the FTC approach fails to work. To the contrary, the record reflects that "the Internet has thrived—and privacy has been protected—under the [FTC's] approach."[302]

Even where commenters flagged data breaches and other issues, they failed to point to ISP-specific problems.[303] They highlighted breaches of major retail chains, entertainment studios, banks, voter registration systems, healthcare providers, and federal government databases.[304] Notably missing from this list is an ISP. Breaches in other sectors are not a reason to burden ISPs. Other arguments fail, as well. For example, some commenters urged the Commission to be vigilant of the dangers they see in broadband, asking the Commission to presume security problems; but fear and speculation are not a substitute for evidence, logic, and authority.[305] Convergence, cited as a reason to regulate,[306] is actually all the more reason the

[301] Internet Association Comments at 4. Likewise, NTIA's 2014 *Exploring the Digital Nation* report shows that "only one percent of American households expressed that privacy was their main concern when deciding not to use the Internet at home." *See* U.S. Chamber of Commerce Comments at 3.

[302] Information Technology Industry Council Comments at 4.

[303] *See, e.g.*, Online Trust Alliance Comments at 3 (flagging breaches, but failing to identify an ISP problem); New America OTI Comments at 41 (same).

[304] Center for Democracy and Technology Comments at 20 & n.75.

[305] *See, e.g.*, Greenlining Comments at 52 ("increased dangers"); EPIC Comments at 23 ("epidemic"); NCL Comments at 2 ("unavoidable threat[s]").

[306] NCL Comments at 3.

Commission should align any policies it pursues with the approach applicable to *every other player in the ecosystem*.

To justify such a radical departure from both the status quo and the FTC's approach, we would expect a robust record of ISP security failures and breaches. There is none. There is no record of pre-texting, as with voice CPNI.[307] There has not been a wave of ISP failings,[308] and nothing has changed since reclassification.[309] The record reflects a few isolated instances of questionable relevance, including investigations of Verizon (that did not find a violation); Level 3 (regarding the E.U.-U.S. Safe Harbor); and Comcast's telephone service (by a California agency).[310] In any case, isolated enforcement actions should not be the basis for broad rules covering the entire industry.[311] Instead, we see a record of success. The Communications Sector Coordinating Council found that "there have been no publically recorded incidents of impact to communications critical infrastructure based on a cybersecurity event."[312] ISPs do not need security mandates; large and small ISPs have robust practices, as the Commission recognizes.[313]

3. These Data Security Proposals Will Have Negative Consequences.

Echoing CTIA's warning, experts provided a robust record showing that the Commission's proposal will harm innovation and security. The proposals will:

---

[307] *See* State Privacy and Security Coalition Comments at 15.

[308] Consumers' Research Comments at 6-7 ("For the many years between the widespread adoption of broadband service by consumers and the FCC's broadband reclassification, the FTC did not bring a single privacy enforcement action against an ISP."). When the FTC had jurisdiction over ISPs, it identified few issues. *Id.* The FTC has brought around 60 data security enforcement actions, FTC Comments at 7, but "not one . . . [was] brought by that agency . . . against a broadband provider." T-Mobile Comments at 12.

[309] *See, e.g.*, Electronic Transactions Association Comments at 6; Information Technology Industry Council Comments at 4.

[310] *See, e.g.*, Comcast Comments at 37; Greenlining Comments at 8-9.

[311] *See* NCL Comments at 9 (discussing "lessons learned from . . . previous Consent Decrees.").

[312] Communications Sector Coordinating Council Sector Annual Report (2015), http://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/jun2016/cs2016_0105.pdf.

[313] NPRM ¶ 177.

- **Make life easier for cybercriminals.** The Proposed Rules threaten mechanisms for preventing spam, bot nets, malware, and phishing. ISPs play a critical role in stopping threats, so making it harder to collect and share information will make it easier for cybercriminals.[314] Also, the Commission should reject calls for a requirement to make cybersecurity practices public.[315]

- **Jeopardize the secure functioning and defense of the Internet.** Several experts explained how the Proposed Rules will impede data collection related to security[316] and site analytics, which in turn will hurt innovation and improvements in network security. Restrictions could endanger the email ecosystem by discouraging critical Domain Name System ("DNS") Blackhole Lists and Feedback Loops.[317] Additionally, restrictions may harm DNS security and Border Gateway Protocol ("BGP"), hindering the ability of ISPs to detect and address malicious behavior.[318] The Proposed Rules also could hamper ISP efforts at taking down bot nets;[319] make it harder for researchers who often lead technological advances;[320] and threaten cybersecurity management of the emerging IoT.[321]

- **Risk the security of new networks.** Network architecture and design are constantly changing. The proposal "throws a wet blanket over startup engineers building additional, novel systems that may substantially increase consumers' privacy and security."[322]

- **Discourage early risk detection and mitigation via anti-virus software.** The Proposed Rules would make it harder for ISPs to bundle anti-malware software with Internet service and hinder the way that anti-malware software operates.[323]

---

[314] *See* Return Path, Inc. Comments at 3-7; Email Sender & Provider Coalition Comments at 2-9; Cloudmark, Inc. Comments at 3-4; Manos Antonakakis et al. Comments at 3 ("Security Experts Comments").

[315] INCOMPAS Comments at 13-14; WTA Comments at 22.

[316] *See* Security Experts Comments at 3 ("[S]ince some security threats are only visible 'at scale' or in the aggregate across the entire ISP network, protecting only the 'opt-in' customers means loss of visibility and precision in detection."); Feamster Comments at 3 (explaining that network traffic data is needed to secure networks); Online Trust Alliance Comments at 5 (same).

[317] Return Path Inc. Comments at 4; Email Sender & Provider Coalition Comments at 4-6; M^{3}AAWG Comments at 2-3.

[318] *See, e.g.*, NCTA Comments at A-21, A-31; M^{3}AAWG Comments at 4.

[319] *See* M^{3}AAWG Comments at 5-6.

[320] *See id.* at 4–5.

[321] *See* NCTA Comments at A-2-3.

[322] CALinnovates Comments at 7; *see* Security Experts Comments at 3 ("without access to user traffic, further innovation and improvements in network security will be greatly complicated").

[323] NCTA Comments at 75, A-34.

- **Discourage beneficial de-identification.** The NPRM and supportive comments ignored a range of de-identification tools that promote privacy and security.[324]

- **Limit critical cybersecurity information sharing.** The Proposed Rules will limit information sharing by ISPs, which is contrary to the Cybersecurity Information Sharing Act ("CISA") and threatens security, as sharing aids in securing email; combating spam; fighting cyber threats like phishing, malware, and botnets; detecting network abuse; and fighting complex network attacks as they occur.[325]

- **Foster a compliance mindset, stagnate solutions, and waste resources.** Cybersecurity should not be about completing a checklist—this leaves consumers and data at risk. Prescriptive rules will force ISPs to spend resources in less productive ways and focus on what the Commission thinks is most relevant, instead of what their own experts prioritize.[326]

B. The Commission Must Change Its Approach.

1. The FTC Agrees the Commission Should Eschew Strict Liability.

The FTC and many others objected to the Commission's proposed strict liability approach, identifying the same dangerous language that CTIA opposes: *ensure*.[327] "[T]he proposed rule . . . is inconsistent with the FTC's sound risk management approach to enforcement that recognizes that 'ensuring' customer [proprietary information] against every threat is not feasible."[328] A strict liability approach is unrealistic and ill-advised, and would especially harm small ISPs.[329] Even the strongest proponents of the Commission's approach acknowledged that "[s]ecurity will never be perfect."[330] Demanding perfection is unwise.

---

[324] *See supra* Part II.B.1; *see also* Consumers' Research Comments at 22-24; Future of Privacy Forum Comments at 6. The FCC should consider a less binary approach to data de-identification, which would enhance consumer security. *See* Future of Privacy Forum Comments at 5.

[325] *See, e.g.*, Online Trust Authority Comments at 5; M^{3}AAWG Comments at 6-7.

[326] *See* Competitive Carriers Association Comments at 35; CenturyLink Comments at 35 (explaining that technical compliance can waste resources).

[327] FTC Comments at 27.

[328] Comptia Comments at 2.

[329] Consumer Technology Association Comments at 10 (calling it a "death knell" for small ISPs).

[330] NCL Comments at 23.

There is no precedent for this strict liability approach. Those arguing that the Commission's security proposals are aligned with voice CPNI rules and federal and state laws are wrong.[331] Strict liability is wholly inconsistent with federal cybersecurity policy, which has avoided such mandates, and other regimes that demand reasonableness.[332] For example, the California law cited by NCL imposes a reasonableness standard.[333] The FTC agreed that reasonableness is the better standard.[334]

2. It Is Apparent that the Commission Should Not Treat All Data as Equal.

Rather than allowing an ISP to prioritize resources, the Proposed Rules would require an ISP to treat all data equally, meaning that even publicly available or de-identified data will be subject to the same security measures as sensitive data. This is "absurd."[335] Federal security recommendations and best practices discourage uniform treatment of data,[336] and commenters overwhelmingly agreed that it is counter-productive to devote security resources equally to all data.[337] FTC Commissioner Ohlhausen separately weighed in regarding the importance of distinguishing between sensitive and non-sensitive data.[338]

---

[331] *Id*. at 2.

[332] *See, e.g.*, 45 C.F.R. § 164.306(a)(2)-(3) (requiring the protection against "reasonably anticipated threats or hazards" and against "any reasonably anticipated [not permitted] uses or disclosures"); 16 C.F.R. § 314.1(a) (requiring "reasonable" safeguards).

[333] NCL Comments at 13 (explaining that California requires "*reasonable* security procedures and practices appropriate to the nature of the information" (emphasis added)).

[334] FTC Comments at 27; *see also* CenturyLink Comments at 36; American Advertising Federation Comments at 9.

[335] Consumers' Research Comments at 24; *see supra* Part II.B.1 (discussing how de-identification accords with consumer preferences and expectations about how data can and should be used).

[336] *See, e.g.*, Internet Commerce Coalition at 8 (NIST Framework, the ISO Security Framework, and FTC guidance); State Privacy and Security Coalition Comments at 11 (GLBA).

[337] *See, e.g.*, Internet Commerce Coalition Comments at 8; State Privacy and Security Coalition Comments at 11-12; WISPA Comments at iv; Cloudmark Comments at 5; Beales Comments at 12.

[338] Ohlhausen Comments at 1-2.

CTIA disagrees with commenters who argued that all communications data is "inherently sensitive."[339] Not all data ISPs can access are sensitive. CTIA also disagrees with commenters who said that sensitive and non-sensitive data are inseparable without intrusive measures, and that it is too difficult to know what data are sensitive and what data are not.[340] Indeed, sophisticated operators have been prioritizing data for decades .

3. Nothing in the Record Justifies the Commission's Unrealistic Approach to Mitigation and Risk Management.

The Commission's proposals are fundamentally at odds with best practices for risk management and remediation. The Commission proposes to mandate the specifics and timing of risk assessments and would require ISPs to identify and promptly correct *all weaknesses*. This is unrealistic and counterproductive.[341] The FTC emphasized real risk management.[342] Moreover, FCC Chairman Wheeler has recognized that effective cybersecurity depends on "proactive risk management, not reactive compliance with a cybersecurity to-do list."[343] Risk prioritization is fundamental to effective cybersecurity; however, the record confirms that the Commission's proposal would not allow for prioritization.[344] ISPs must be free to engage in beneficial and effective risk assessments and mitigation, not burdened to conduct prescribed assessments and then expected to fix every weakness identified.[345] Obligating companies to treat all weaknesses

[339] Grant Comments at 5.

[340] NCL Comments at 2; ACLU Comments at 6. *See supra at* Part II.B.

[341] *See, e.g.*, WTA Comments at 22; NTCA Comments at 60-61.

[342] FTC Comments at 27.

[343] Chairman Tom Wheeler, Remarks to the American Enterprise Institute at 3 (June 12, 2014).

[344] *See, e.g.*, American Cable Association Comments at 24.

[345] *See, e.g.*, Centre for Information Policy Leadership Comments at 4.

as high priorities will distort security, waste resources, and endanger networks and consumers. "Compliance cannot be allowed to 'starve' . . . technical security."[346]

4. The Record Is Clear—the Commission Must Avoid Granular Regulation.

Granular regulations are unwise;[347] many commenters agreed.[348] Even some proponents of rules acknowledged that the Commission should not be "overly prescriptive," and that "[w]hat constitutes reasonable data security today will not constitute reasonable security tomorrow."[349] However, some asked for a variety of mandates that border on the frivolous. Specific guidelines, for example, on "multi-factor authentication or other technical measures would provide bad actors with a roadmap of what they need to effectively gain access to systems through social engineering or other methods."[350]

- **The Commission should reject calls to mandate encryption.** In the face of a lack of consensus on the use and impact of encryption,[351] the Commission should not tip the scales. CTIA strongly disagrees with commenters who urged mandatory encryption. Remarkably, some called for free, end-to-end encryption for all.[352] This is naïve, unrealistic, and undermines the privacy community's credibility; it also may conflict with ISP obligations under the Communications

[346] Farsight Security Comments at 23.

[347] Maureen Ohlhausen, *Regulatory Humility in Practice*, American Enterprise Institute (April 1, 2015), https://www.ftc.gov/system/files/documents/public_statements/635811/150401aeihumilitypractice.pdf ("It's a very fast changing area. The threats and the precautions are sort of in a race. So I don't think it would be good for companies really if the FTC chose some level of security. It would be out of date before the ink was dry.").

[348] *See, e.g.*, ViaSat Comments at 7. *But see* Farsight Security Comments at 30-31 (suggesting a laundry list of specific technical measures, from software patches to the use of virtual private networks). Suggestions like Farsight's are out of touch. While many measures may be useful and effective, they are in no way suited for across-the-board, one-size-fits-all requirements.

[349] NCL Comments at 9; *see also* Access Now Comments at 11 ("It is vital to avoid situations that federal legislation like Electronic Communications Privacy Act have caused, wherein changes in technology undermine the rights the laws aim to safeguard.").

[350] *See, e.g.*, WTA Comments at 20.

[351] *Compare* Farsight Security Comments at 31 (supporting a mandate); Security and Software Engineering Research Center at Georgetown University Comments at 15 (same), *with* INCOMPAS Comments at 14 ("Encryption is only one component of data security, and as a result of rapid technological development, carriers require the ability to evolve and use the security safeguards that are most applicable to their business and customers' requirements") and XO Communications Comments at 15 (discouraging encryption requirement).

[352] EPIC Comments at 11, 23.

Assistance for Law Enforcement Act ("CALEA"). Others recommended specific encryption techniques for all data.[353] As discussed, there is no consensus on the value of encryption in all cases, and especially no consensus on the techniques for encryption.[354] Mandating specifics will doom the Commission and—by implication—ISPs to hurt consumer safety more than help it.

- **The Commission should not pursue authentication or password mandates.** The record shows these are not appropriate,[355] and would be unprecedented.[356] Even though security measures like multi-factor authentication ("MFA") and password protection are effective in some contexts, they are not appropriate for every context.[357] Those who urge mandating MFA share the Commission's incorrect, static view of cybersecurity.[358] Even strong proponents of a requirement admitted that "in the future, MFA might not be sufficient to protect consumers' data."[359] A mandate would ignore the complexities and downsides, for both ISPs and consumers. Notably, one commenter that supported an MFA requirement stated, and then promptly ignored, several consumer harms from MFA, including: inaccessibility, inconvenience, and inconsistent user experiences.[360] A mandate would also ignore consumer choice.[361] One commenter claimed that an MFA requirement would not unduly burden small ISPs because "[t]here are third party outsourced identity management providers who can deliver the required technical capabilities."[362] This is vexing, given the

[353] *See* Farsight Security Comments at 31.

[354] *See* Julie Brill, PrivacyCon Workshop (Jan. 14, 2016), https://www.ftc.gov/public-statements/2016/01/remarks-privacy-con-commissioner-julie-brill (remarking that the ease of use for some encryption measures is limited); Karen Scarfone et al., *Guide to Storage Encryption Technologies for End User Devices: Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-111 3–7 (Nov. 2007), http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf ("When evaluating [encryption] solutions, organizations should compare the loss of functionality with the gain in security capabilities and decide if the tradeoff is acceptable. Technologies that require extensive changes to the infrastructure and end user devices should generally be used only when other technologies cannot meet the organization's needs.").

[355] *See* WTA Comments at 20 (opposing MFA requirement); NTCA Comments at 63 (same).

[356] State Privacy and Security Coalition Comments at 11 (explaining that no state law even adopts such requirements). Some suggested the Commission adopt NIST recommendations regarding authentication. *See* Farsight Security Comments at 24. This would fundamentally distort NIST recommendations, which are not meant to compel compulsory private behavior.

[357] Mozilla Comments at 7 (explaining that MFA "*could* be highly useful in *many contexts* related to ISP collection and use of user data" (emphasis added)); Cincinnati Bell Telephone Company Comments at 4 (urging the FCC to establish principle, not micromanage). Likewise, INCOMPAS and XO Communications pointed out differences in business contexts.

[358] *See, e.g.*, NCL Comments at 14-16; Farsight Security Comments at 26; AAJ Comments at 8.

[359] NCL Comments at 15.

[360] Farsight Security Comments at 25-26.

[361] Consumers' Research Comments at 21.

[362] Farsight Security Comments at 27; U.S. Small Business Administration, Office of Advocacy Reply Comments at 3-4 (noting that it will be significantly more costly for small provider to comply with the proposed rules).

proposed third-party liability for ISPs. At least one commenter seemed to think that simple password protection is the only data security protection used by ISPs.[363] This assumption is mistaken.

- **The Commission should not ban deep packet inspection.** Some proposed an outright ban on DPI.[364] This would undermine security, by ignoring the many beneficial ways DPI is used to ensure network security.[365]

- **The Commission should not micromanage other activities.** There is no tangible support for a mandate to train non-employees. Such a requirement is unrealistic and would particularly burden small ISPs.[366] Commenters showed a troubling inclination to micromanage, including in calls to regulate trouble tickets.[367] ISPs know best how to deal with various technical issues and customer communications.

- **The Commission should not impose data minimization requirements.** Data minimization can be important in certain contexts, but there are tradeoffs and complexities, depending on the network and context.[368] Some proponents of data minimization recognized that their proposals may impact public safety,[369] but advised the Commission to ignore the impact because, in their view, it is "impossible" to balance law enforcement needs with privacy and security interests.[370] Putting aside this simplistic and naïve perspective, prescriptive measures are not needed. Worse, they would hurt consumers by decreasing security: mandates could limit ISPs' ability to research and monitor security incidents.[371] In any event, nothing concrete has been proposed. Given the complexities, crafting a rule without proper notice would be arbitrary and capricious.

---

[363] *See* NCL Comments at 15. NCL cited the Sony incident as reason to impose MFA on ISPs. It offered no evidence that this would have prevented the incident, and Sony is not an ISP.

[364] *See* Center for Digital Democracy Comments at 21; EPIC Comments at 26-27; EFF Comments at 10.

[365] Farsight Security Comments at 33; CTIA Opening Comments at 151-152.

[366] WTA Comments at 23.

[367] *See* Greenlining Comments at 47-48.

[368] Email Sender & Provider Coalition Comments at 9. Currently, ISPs already use these principles where appropriate and within the context of their networks. *See* Competitive Carriers Association Comments at 42.

[369] EPIC says the "FCC must also repeal its regulation requiring retention of telephone toll records for 18 months, 47 C.F.R. § 42.6," EPIC Comments at 10. This is unrealistic and unhelpful.

[370] EFF Comments at 7.

[371] ReturnPath Inc. Comments at 5. There is no need to start identifying categories of information that ISPs cannot collect, such as content. *See, e.g.*, EPIC Comments at 26.

5. Commenters Confirmed that the Commission Should Not Hold ISPs Accountable for Third-Party Action.

The Commission should not impose third party liability on ISPs.[372] *First*, the Commission misapprehends ISP market power and wrongly assumes that ISPs can dictate the data security practices of other—often larger—players.[373] *Second*, the approach is unprecedented, going beyond even HIPAA.[374] *Third*, such an unprecedented requirement is not necessary; without any government mandate, ISPs and vendors already have strong incentives to work with each other to protect customer information, through both contractual provisions and FTC and other agency jurisdiction over non-ISPs.[375] The record shows that "[e]xisting contracts between BIAS providers and third parties already protect against third party data misuse."[376] Such business decisions are best left to ISPs and vendors, not the Commission.[377]

Finally, there is ample proof in the record that third-party liability would have a disproportionately negative impact on small ISPs, whose resources and budgets are more limited.[378] They would need to renegotiate existing contracts; be burdened with higher transaction costs in future contract negotiations; be incapable of passing through requirements to vendors, who often have more bargaining power; be left without resources to protect consumer

---

[372] *See* Cloudmark Inc. Comments at 5; NTCA Comments at 65; Cincinnati Bell Telephone Company Comments at 13. The Commission also should reject calls for ISPs to make their contracts with vendors public. *See* EFF Comments at 16. This would compromise business operations and improperly make sensitive information publicly available.

[373] *Cf.* Future of Privacy Forum Comments at 30 (discussing that the proposed regime will not be relevant to the rest of the ecosystem, and will exclude ISPs from the data market).

[374] *See* Audience Partners Comments at 18.

[375] Further, there is record evidence that "contractual commitments with third parties regarding information practices are a relatively weak compliance mechanism when compared with broad regulation under the purview of the FTC and other bodies that have direct jurisdiction over these third parties as well as [ISPs]." Security and Software Engineering Research Center at Georgetown University Comments at 15.

[376] Return Path Inc. Comments at 4.

[377] Cloudmark Inc. Comments at 5-6.

[378] Rural Non-Profits Comments at 10.

data; have to use scarce resources to monitor third party compliance; and have exorbitant legal fees to enforce contractual obligations.[379]

6. The Commission Must Not Limit Cybersecurity Information Sharing in Any Way.

Cybersecurity information sharing is key to securing networks and the data those networks move and store. CTIA is concerned about potential conflict between the Commission's privacy NPRM and the information sharing encouraged by CISA. Congress chose in CISA to "encourage public and private sector entities to share cyber threat information without legal barriers and the threat of unfounded litigation."[380] The Commission should heed that choice.

The Commission's Proposed Rules will make it difficult for companies to share information without fear.[381] Remarkably, some commenters urged additional, onerous Commission limitations on information sharing, such as prior de-identification.[382] These commenters (many of whom opposed CISA) asked the Commission to ignore the will of Congress, which prescribed procedures and limits on cybersecurity information sharing "containing personal information" or otherwise affecting privacy and civil liberties,[383] and authorized companies to share information consistent with these limitations "notwithstanding any other provision of law."[384] In this broad authorization, Congress gave roles to the Attorney General and DHS, but did not provide for Commission involvement.[385] Additional Commission

[379] *See* American Cable Association Comments at 27-30; Rural Wireless Association Comments at 12-13; Competitive Carriers Association Comments at 4-5.

[380] *See* AT&T Comments at 117.

[381] *See* NCTA Comments at 76-77.

[382] *See, e.g.*, Access Now Comments at 8-9; EFF Comments at 9.

[383] 6 U.S.C. § 1504(b)(3); *see also id.* § 1503(d)(2).

[384] *Id.* § 1503(c)(1).

[385] *See id.* § 1504(b)(1)-(2).

limitations on sharing would contravene CISA and impose barriers, slowing response times for ISPs.

The Commission must reject misguided suggestions to limit sharing. In fact, the Commission must avoid any confusion at all. It need not offer definitions and certainly should not add any limitations. It should plainly state that its privacy rules are not a barrier to information sharing. Any uncertainty could result in "fewer companies, especially small providers, sharing threat information in the first place."[386] CSRIC V, Working Group 5 is actively examining information sharing and identifying challenges, including uncertainty created by Commission activity. The Commission should rely on CSRIC and defer to the many activities already underway at various agencies, ensuring its approach to privacy does not inadvertently complicate those efforts. In light of Congress's clear action, the Commission must ensure that nothing in its current rulemaking impedes or slows cybersecurity information sharing.

VII. THE COMMISSION SHOULD MODIFY THE PROPOSED DATA BREACH NOTIFICATION RULES.

Numerous commenters explained that the Proposed Data Breach Rules are burdensome, inflexible, and likely to result in consumer confusion and harm.[387] The Commission should revise the notification rules set forth in the NPRM to mitigate these concerns. The FTC, in particular, recommended sound changes to the proposed breach notification framework based on its decades of experience as the principal federal data security enforcement agency.[388] CTIA

[386] American Cable Association Comments at 33.

[387] *See, e.g.*, FTC Comments at 30-34; INCOMPAS Comments at 14-18; ITTA Comments at 23-24; Verizon Comments at 68-70; NCTA Comments at 67-71; Cincinnati Bell Telephone Company Comments at 13-14; Mobile Future Comments at 4.

[388] FTC Comments at 30-34.

supports these modifications and encourages the Commission to incorporate them into any final breach notification rules.

A. The Record Supports Tailoring the NPRM's Data Breach Notification Requirements.

First, as many parties pointed out, the proposed definition of a breach sufficient to trigger the notification requirement is vastly overbroad.[389] The NPRM sweeps disclosure of *any* "customer proprietary information" into its definition of a breach, effectively prohibiting ISPs from maintaining anonymous browsing data and instead requiring them to link browsing data to a customer's account information so that it could provide notification of a breach involving a persistent identifier.[390] CTIA supports the FTC's recommendation that the notification requirement be applied only to a more limited category of personal information that does not include device identifiers, cookies, or other persistent identifiers standing alone.[391]

Similarly, CTIA and the FTC agree that any final rules should incorporate "an exception to the notification requirement for certain inadvertent, good-faith actions by company employees" in order to further limit the circumstances in which a breach triggers notification.[392] As one commenter pointed out, under the proposed rules, an ISP could be required to send notification even when "a customer service representative accidentally mistypes an account number and thereby accesses the wrong account for an instant."[393] Unless modified by an exemption that extends to an ISP's employees, agents, and vendors, the breadth of the proposed definition of a breach risks subjecting consumers to "overnotification" that would both

[389] *See, e.g.*, CTIA Opening Comments at 175-79; FTC Comments at 31; INCOMPAS Comments at 14-16; ITTA Comments at 23; NCTA Comments at 67.

[390] FTC Comments at 31.

[391] *Id*. at 32.

[392] *Id*.; CTIA Opening Comments at 179; *see also* INCOMPAS Comments at 17; Verizon Comments at 68-69.

[393] Verizon Comments at 68-69.

negatively impact their service experience and jeopardize the long-term security of their information.[394] Consumers who receive "a barrage of notices" can "become numb to such notices,"[395] with "notice fatigue" leaving consumers "desensitized" and "tuned out" to the content of notifications and less likely to read or react to them.[396] By requiring that ISPs send notification for such a wide range of "breaches," the Commission's current proposal will "creat[e] constant annoyances and giv[e] consumers a flawed understanding of how their information is secured."[397] Building an exception for inadvertent, good-faith disclosures into the Proposed Data Breach Rules will help to reduce the demands on consumers' attention and to focus that attention on the situations where it is most needed.

For breach notification to be effective, it is also important that it come from a party with whom the consumer has a preexisting relationship. As such, CTIA is willing to embrace the FTC's recommendation on the treatment of breaches by third parties with whom ISPs have shared information: ISPs should be required to contractually obligate those third parties to give the ISP notice of any breach.[398] ISPs can then collaborate with those third parties in the event of a breach to determine how best to provide the requisite notice, as opposed to customers'

[394] FTC Comments at 31-32; INCOMPAS Comments at 10 (the proposal "makes it likely that customers will receive an increased number of breach notifications, leading to customer confusion, notice fatigue, and decreased confidence in their telecommunications service"); Consumer Technology Association Comments at 11 (proposed rules will "add[] another heap to the mountain of notices" consumers already receive); Verizon Comments at 69 ("[T]he inevitable result of the Commission's proposal is that customers will receive notifications that they do not care about and that create unnecessary confusion and anxiety, such that customers could stop paying attention to notices altogether and miss those that might actually be important.").

[395] FTC Comments at 31.

[396] Consumer Technology Association Comments at 11.

[397] Mobile Future Comments at 4.

[398] FTC Comments at 32; *see also* NCL Comments at 33.

receiving multiple and possibly conflicting notices, including from "a potentially unknown agent" who may be unrecognized and therefore ignored.[399]

The record reflects clear consensus that the Commission's proposed timeline for breach notification is too short.[400] Requiring notification to the Commission and law enforcement within seven days and notification to consumers within 10 days simply does not allow time for adequate investigation and could result in ISPs' providing inaccurate information to consumers.[401] ISPs must undertake a plethora of tasks upon discovery of a breach, including locating and stopping ongoing attacks, determining what data have been exposed, identifying affected individuals, preparing remedies and training staff to assist consumers, and drafting notices compliant with federal and state law.[402] Details about the scope and impact of a breach simply may not be available within the period proposed by the Commission, forcing ISPs to issue incomplete or inaccurate notices that could create confusion and cause unnecessary alarm.[403] The tight timeline for notification is particularly problematic given the NPRM's expansive view of what constitutes a breach. As the ITTA observed, "the proposed rules will expand exponentially the number of events that will qualify as breaches while simultaneously according providers much less time to notify customers about them."[404] CTIA supports the

[399] FTC Comments at 32.

[400] FTC Comments at 32-33; CTIA Opening Comments at 179-82; ITTA Comments at 23-24; INCOMPAS Comments at 17-18; Hughes Network Comments at 6-7; Verizon Comments at 69-70; Cincinnati Bell Telephone Company Comments at 13; NCTA Comments at 92-93.

[401] FTC Comments at 32-33; Verizon Comments at 70 ("For serious and complicated breaches, 10 days is just not enough time...for minor breaches, a 10-day notification period will require resources that could be spent responding to and notifying consumers of significant breaches to be diverted.").

[402] CTIA Opening Comments at 180; INCOMPAS Comments at 17-18 ("[T]he proposed rules do not provide enough time for carriers to make data breach determinations[,] conduct an appropriate investigation, identify affected customers, put remedies in place, and send notifications."); NCTA Comments at 92-93.

[403] FTC Comments at 32-33; CTIA Opening Comments at 180-81; Cincinnati Bell Telephone Company Comments at 13 ("The Commission should not require carriers to give customers premature notices.…[or] to provide notices when critical information about the suspected data breach is not available.").

[404] ITTA Comments at 24.

FTC's suggestion the proposed rules be revised to require breach notice "without unreasonable delay" but not later than 30-60 days,[405] a modification that will alleviate pressure on ISPs to provide notification of a breach before they have assembled the appropriate information.[406]

Finally, CTIA and the FTC concur that breach notifications should include contact information for national credit reporting agencies only in limited circumstances.[407] As not all data breaches have the potential to impact an individual's credit history, consistently including credit agency information in notifications may give consumers a false sense of security with regard to other forms of fraud that cannot be reflected in a credit report.[408] Contact information for credit reporting agencies should be included in breach notices only when the breached information could be used to open a new account in the consumer's name, along with contact information for the FTC and a reference to its IdentityTheft.gov website, which contains general guidance for consumers who have received a breach notice.[409]

B. Calls to Broaden the Proposed Notification Obligations Should Be Rejected.

By contrast, requests by the National Retail Federation ("NRF") and others that the Commission further expand the already overbroad breach notification requirements are misguided and not in the public interest.[410] NRF proposed a notification requirement that would obligate an ISP to notify not only its own business customers, but *all* potentially affected

[405] FTC Comments at 33.

[406] CTIA also supports the FTC's related suggestion that any law enforcement request for a delay in notifying consumers should be made in writing, specifying both a finite period and the reason for the delay. FTC Comments at 33.

[407] FTC Comments at 34.

[408] *Id*.

[409] *Id*.

[410] *See, e.g.*, NRF Comments at 2-6.

consumers, of a network breach.[411] This suggestion that ISPs reach out to all affected individuals, without regard to whether they have a customer relationship with those individuals, makes no sense. An ISP suffering a network breach virtually *never* knows the identities of consumers impacted or whether their personal information was included in the breached data. In order to even ensure that level of insight into a network breach, ISPs would be forced to take additional steps to monitor customer activity and engage more routinely in DPI.

NRF's recommendation of substitute public notification in situations where identification of impacted individuals is impossible is similarly misguided. Obligating ISPs to publicly disclose a breach without an understanding of which or how many people might be affected not only would be irresponsible, causing consumer alarm and potentially leading to unnecessary cancellation of credit cards and services,[412] it also would result in precisely the over-notification that NRF itself purports to oppose on the grounds it would "confus[e] American consumers."[413] As the FTC explained, consumers are already "overwhelmed by the volume of breach notices they receive," and often do not understand the risks these notices are intended to communicate or react appropriately to them.[414] Requiring ISPs to alert consumers to breaches that may not even affect them will only exacerbate this problem.

Instead, ISPs who experience a breach that affects personal information should be required to notify only the entity whose consumers' data was breached, not the individual consumers. ISPs are positioned to efficiently and accurately identify their own affected customers, and the impact of any breach notices that are subsequently issued to individuals will

[411] *Id*. at 7.

[412] *See* CTIA Opening Comments at 181-82.

[413] NRF Comments at 5-6.

[414] FTC Comments at 31-32.

be heightened coming "from an entity with which the consumer has a pre-existing relationship, rather than a potentially unknown agent."[415]

Moreover, NRF's reliance on the Heartland Payment Systems example to support its call for expanded notification requirements is inapposite.[416] Heartland is not an ISP, but a payment processor. Unlike a broadband provider that transmits a retailer's consumers' information from a point of origin to a point of termination, Heartland held and processed consumer payment data itself. Heartland's notification of the public as opposed to retailers was a direct consequence of its access to the sort of in-depth information about the extent of the breach it experienced and the personal nature of the data at issue, something that ISPs lack.

CONCLUSION

CTIA and its members appreciate the Commission's goal of protecting the privacy and data security of broadband consumers. For years, ISPs, like other entities in the online ecosystem, were effectively and efficiently regulated by the FTC under a technology-neutral, flexible privacy and data security regime, as well as enforceable industry codes of conduct and best practices. The FTC's time-tested regime is driven by the context of a customer's relationship with his or her provider and depends primarily on the sensitivity of the data at issue in a particular use case, not the type of provider. As multiple commenters documented, the evolution of the Internet ecosystem has reinforced that the FTC's regime is fundamentally sound.

The Commission's classification of broadband as a Title II telecommunications service removed ISPs from the FTC's jurisdiction, but it did not otherwise change the ecosystem. To the contrary, as multiple commenters meticulously proved, and as the record now makes clear: ISPs do not comprise a unique privacy or data security threat relative to other entities in the

[415] *Id*. at 32.

[416] NRF Comments at 5.

ecosystem; ISPs do not have unique or uniquely comprehensive visibility into consumer online activity; ISPs lack incentives to engage in the hypothetical practices that animated the few commenters that supported the NPRM; ISPs have adopted best practices codifying customer notice, choice, and data security; and ISPs otherwise are engaging in innovative uses of customer information that facilitate the offering of new products, services and bundles, as well as support improved delivery of service, enhanced data security, and numerous other consumer benefits.

In light of this record, the NPRM's departure from the FTC's privacy regime to create asymmetric and highly prescriptive rules that govern only ISPs is, in the measured words of the FTC itself, "not optimal." Indeed, the Proposed Rules are considerably worse than that. They are unlawful, because they are unambiguously foreclosed by, and unambiguously exceed limitations in, the Communications Act. They are unconstitutional, because they facially impose speaker- and content-based burdens on the exercise of ISP speech, without commensurately, if at all, advancing a cognizable interest in protecting consumer privacy. They are overwhelmingly inconsistent with customer expectations in a converging communications landscape. They are unmoored from traditional privacy concerns, because they lack any nexus to the sensitivity of data or risk of harm—instead relying on antiquated and vestigial distinctions between service categories. They will result in customer frustration and fatigue, by asymmetrically regulating only one category of entities in an open ecosystem and by requiring frequent notice, regardless of whether an ISP is engaging in, for example, the routine use of de-identified or widely available data, on the one hand, or the disclosure of highly sensitive data, on the other. They are unnecessary, because the market for wireless broadband is highly (and increasingly) competitive, and because providers are engaging in campaigns that are driving switching costs even lower—where the exact opposites are true in the markets for many edge services. They would impose

inefficient, unnecessary, and substantial costs on ISPs, which costs ultimately will be passed on to consumers in the form of higher retail prices. And they are rigid and prescriptive, at a time when ISPs increasingly need flexibility to account for not only evolving customer demand, but also evolving security threats.

Moreover, even if a court were to conclude that none of these problems is fatal, which they are, the inevitable outcome of the adoption of the Proposed Rules would be protracted litigation, following closely on the heels of at least sixteen months of uncertainty surrounding the legality of the *Open Internet Order*—an outcome that would be all the more wasteful in light of the facts that the record is devoid of any evidence supporting the Commission's feigned urgency and that the Commission currently has authority to take action under the statute.

As set forth by many commenters, including both CTIA and the FTC, there is another way. Starting with the FTC's specific recommendations and the industry proposal, the Commission could propose a new set of rules to create a harmonized, technology-neutral, flexible privacy and data security regime, supported by a multistakeholder process to develop enforceable codes of conduct, that appropriately treats all entities in the Internet ecosystem alike when it comes to the uses and disclosures of consumer data. The Commission, like the FTC, also could take *ex post* enforcement action as necessary in response to failures, breaches, or malfeasance (if any). If the Commission were, in good faith, to pursue this latter course, it might secure buy-in for final rules not just from the usual cast of advocacy groups, but also from the FTC, ISPs, industry associations, and many others, creating a durable framework on which consumers and industry alike could rely. CTIA hopes that the Commission takes the opportunity to chart a consensus path forward.

Respectfully submitted,

/s/ Debbie Matties

Debbie Matties
Vice President, Privacy

Thomas C. Power
Senior Vice President and General Counsel

Scott K. Bergmann
Vice President, Regulatory Affairs

CTIA
1400 Sixteenth Street, NW
Suite 600
Washington, DC 20036
(202) 785-0081

July 6, 2016