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
	)	
	)	

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

May 26, 2016

TABLE OF CONTENTS

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
	)	
	)	

COMMENTS OF CTIA

CTIA[1] hereby submits its 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 of their customers, and have long done so under applicable federal and state privacy laws and self-regulatory enforceable codes of conduct. Furthermore, CTIA members support keeping customer information confidential and have implemented robust data security programs to do so. Indeed, carriers already are required to protect the security of personal information under relevant state and federal laws. Beyond their legal obligations, CTIA members also recognize that protecting the privacy and security of customers' data is a good business practice. Indeed, they have strong incentives to earn and maintain consumer trust and loyalty by doing so.

---

[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*").

Broadband customers have come to expect, and benefit from, a consistent regulatory regime that protects their personal information as it flows through and among all of the entities that comprise the online data services ecosystem.[3] The Federal Trade Commission ("FTC") has successfully provided just that, protecting the privacy of online consumers' personal information through its flexible notice-and-choice framework, and through the threat of enforcement as a backstop to ensure that companies in the ecosystem implement and adhere to their privacy policies.[4] The NPRM, however, departs radically from this approach and from a similar framework recently proposed by the Obama Administration.

In this comment, CTIA encourages the FCC to reconsider most of its proposed rules because they will not protect consumers. They also harm competition because they deviate from the regulatory framework that the FTC continues to apply to the rest of the internet ecosystem,

---

[3] Comments of Progressive Policy Institute, filed May 26, 2016 (noting that a recent survey of Internet users conducted by Public Opinion Strategies and Peter D. Hart showed that "[b]y an overwhelming 94%-5% margin, Internet users agree that '[*a*]*ll companies collecting data online should follow the same consumer privacy rules so that consumers can be assured that their personal data is protected regardless of the company that collects or uses it,*' including 82% of Internet users who say they 'strongly' agree with that statement").

[4] The Federal Trade Commission Act authorizes the FTC to investigate and enforce the Act's prohibition against "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45. The FTC has successfully brought numerous privacy enforcement actions against a range of Internet companies. *See, e.g.*, *In re Facebook, Inc.*, No. C-4365 (F.T.C. July 27, 2012) Complaint, https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf, Decision and Order, https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf (settling charges that Facebook deceived consumers by failing to keep its privacy promises to users); *In re Google, Inc.*, No. C-4336 (F.T.C. Oct. 13, 2011) Complaint, https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzcmpt.pdf, Decision and Order, https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf (settling charges Google used deceptive tactics and violated its privacy promises to consumers when it launched its social network, Google Buzz), *United States v. Google, Inc.*, Order, No. 12-04177 (N.D. Cal. Nov. 16, 2012), ECF No. 30 (approving stipulated order for permanent injunction and civil penalty judgment); *In re Twitter, Inc.*, No. C-3416 (F.T.C. Mar. 2, 2011) Complaint, https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twittercmpt.pdf, Decision and Order, https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twitterdo.pdf (settling charges that Twitter failed to safeguard users' personal information); *In re Snapchat, Inc.*, No. C-4501 (F.T.C. Dec. 23, 2014) Complaint, https://www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf, Decision and Order, https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf (settling charges that Snapchat deceived consumers about the amount of personal data it collected and the security measures it took to protect that data from misuse and unauthorized disclosure).

that the Administration has supported, and that applied to ISPs for decades before the FCC reclassified broadband under Title II. In summary:

- The proposed rules exceed the Commission's statutory authority, in particular their attempt to sweep into the scope of the rules customer data beyond customer proprietary network information ("CPNI"), which is the specific data that Congress deemed worthy of protection.
- The proposed rules are overbroad and harmful in that they attempt to cover data that is not linked to consumers, which is valuable to businesses and society in the development of smart cities and other applications of big data that benefit consumers.
- The proposed rules will harm consumers and competition because they fail to account for the sensitivity of data and the need for companies to adapt to changing technologies and consumer expectations.
- The proposed rules will harm competition in the digital advertising market, by placing ISPs, who are new entrants to this market, at a competitive disadvantage.
- The proposed rules concerning ISPs use of their customers' data also are a prior restraint on valuable speech and thus violate the First Amendment.

CTIA urges the Commission to recognize these harms to consumers and competition, and instead to move forward in accordance with this Administration's policy of consistent privacy regulation across the Internet. Consistent with the limits of its statutory authority, the Commission should adopt rules based on the FTC's deception and unfairness standard, which has provided strong privacy protections for consumers while allowing online companies to offer consumers innovative services and products that are the backbone of the U.S. economy.

A Consensus Path Forward. As the Obama Administration recommended in 2012 in its privacy report outlining a "Consumer Privacy Bill of Rights," a twenty-first century privacy regime should reflect the reality of the Internet economy and should regulate the same data

consistently across regulatory regimes and the ecosystem.[5] The Administration established such a framework, a key component of which was the use of multistakeholder processes, led by the Department of Commerce's National Telecommunications and Information Association ("NTIA"), to develop enforceable codes of conduct that would implement the general principles that comprise the Consumer Privacy Bill of Rights.[6]

If the Commission is determined to move forward with rules governing broadband privacy, it should abandon its prescriptive approach, and instead, work with other regulators, such as the FTC and NTIA, to develop a flexible and technology-neutral approach, buttressed by a multistakeholder process. To that end, CTIA urges the Commission to adopt the consensus privacy framework for CPNI, which CTIA and others proposed and the NPRM references.[7] This framework, which is modeled on the FTC's notice-and-choice regime and unfair and deceptive acts and practices authority, will ensure that consumers are protected under a similar regulatory regime across all platforms while having access to a broad array of services. The industry privacy framework is based on four principles: (1) transparency; (2) respect for context and consumer choice; (3) data security; and (4) data breach notification. The NPRM invokes these same values, but its proposed regime is unlike the industry privacy framework, which is flexible and harmonized with the well-established and successful FTC framework, providing strong enforcement for unfair or deceptive acts or practices that materially harm consumers.

---

[5] *See generally* 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) ("*2012 White House Privacy Framework*"), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[6] NTIA thus far has conducted three such processes, and CTIA has signed on to the most recent code of conduct governing the use of drones.

[7] *See NPRM*, 31 FCC Rcd at 2589-90 ¶¶ 280-282. On March 1, 2016, several leading trade associations, including CTIA, sent a letter to Commission Chairman Wheeler proposing and explaining a privacy framework for the Commission to adopt in this rulemaking proceeding. A copy of this letter is attached as Exhibit A.

The industry's privacy framework will align with consumers' expectations that their data will be subject to consistent privacy regulation across the ecosystem, regardless of whether it is used by their ISP, operating system, or edge provider. It also will allow ISPs to use the flexible choice mechanisms available to all other entities in the Internet ecosystem, enabling ISPs to use or disclose CPNI when consistent with the context in which the customer provides, or the provider obtains, the information. By avoiding inconsistent requirements, this approach will further one of the principal goals cited in the *Open Internet Order*: providing strong consumer protection while encouraging innovation and growth. In addition, this flexible framework will allow ISPs to both implement and update their practices in ways that meet the privacy and security needs and wants of their customers and address changing and new developments in this space.

The Commission Needlessly Diverges from FTC Model. Although the NPRM acknowledges that the FTC's approach is the gold standard for establishing a coherent, cross-sectoral approach to protecting consumer privacy, the Commission fails to incorporate into the rules proposed in the NPRM (the "Proposed Rules" or "Rules") the FTC's core unfair and deceptive acts and practices authority, which is the essence of the privacy standard that applies to the Internet economy. The NPRM also cites the FTC's 2012 report on privacy ("*FTC Report*")[8] only selectively and fails to incorporate or even acknowledge several of the *FTC Report*'s key elements. Specifically, the NPRM does not (1) reflect the *FTC Report*'s findings that consumers are best served by a flexible approach to notice and choice that is technology neutral; (2) make the regulatory distinction that the *FTC Report* makes between non-sensitive and sensitive data;

[8] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers* (Mar. 2012) ("*FTC Report*"), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

(3) exempt from its privacy regime data that are not reasonably linkable to an identifiable individual; or (4) incorporate the principle that companies should not have to provide consumers choice for data use and disclosure that is consistent with the context of the transaction or with the company's relationship with the consumer.

Instead, the Commission proposes strict regulations regarding the use and disclosure of a newly-minted broad category of data that it calls "customer proprietary information," and it proposes to impose these regulations on just one type of entity in the online data services ecosystem—broadband Internet access service providers ("broadband service providers" or "ISPs")—while leaving the edge providers—search engines, social networks, mobile apps, online advertising networks, and other large platform providers—regulated under the FTC's flexible framework and *ex post* enforcement regime. The Commission does not identify any harms or particular problems posed by ISPs that necessitate a divergence from the effective regulatory framework that has applied to ISPs for years. Indeed, it ignores completely the comprehensive fact-gathering and analysis that the FTC conducted several years ago and that led the FTC to conclude that ISPs did not warrant heightened regulation. For this reason alone the Commission's proposal is fatally flawed.

But the Commission's proposed asymmetrical regulatory regime is ill-advised for several other reasons, as well: it fails to reflect the nature of the online data services ecosystem, where multiple entities have access to and use consumers' online data to provide consumers ad-supported content and services; it threatens to create consumer confusion and frustration; and it will inhibit competition, innovation and routine business operations. In short, it will not achieve the Commission's goal of materially improving consumers' privacy.

At a fundamental level, by singling out ISPs for special treatment, the Commission ignores the economic and technological realities of the digital environment in which ISPs and other entities operate. Unlike the closed and concentrated ecosystem for telephone voice service in which carriers historically had exclusive access to CPNI that they acquired through the carrier-customer relationship, broadband customers' data in the competitive online data services ecosystem are available to, and shared among, many entities to provide a variety of ad-supported content and services.[9] ISPs are just one set of players in this ecosystem, and they should not be regulated differently from other large platform providers, such as operating systems, social networks, search engines, and advertising networks.[10]

Indeed, contrary to the Commission's assumptions, ISPs' access to online consumers' personal information in this ecosystem is neither comprehensive nor unique. Academic research and empirical studies show that certain technologies—such as encryption and Virtual Private Networks—substantially limit ISPs' visibility into users' online activity and are widely available and increasingly used.[11] This trend will continue: by the end of 2016, without any action on the part of consumers, it is estimated that 70 percent of online traffic will be encrypted.[12] Moreover, the typical Internet user accesses the Internet through multiple devices, some of which are mobile, and connect to the Internet through various ISPs and Wi-Fi networks at any given time throughout the day.[13] As a result, ISPs, at best, have fractured and variable access to the typical

[9] *See generally* Peter Swire et al., *Online Privacy and ISPs* (The Institute for Information Security & Privacy at Georgia Tech, Working Paper, Feb. 29, 2016) ("*Swire Report*"), http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf; *see also* sources cited, *infra* Part V.A.2.

[10] *See Swire Report* at 4, 8-14.

[11] *See id.* at 23-24, 28-34.

[12] *See id.* at 29.

[13] *See id.* at 24-25.

user's daily online activity. This shift to mobile and multiple devices, however, has not hampered edge providers' ability to continue to collect, use, and share more, and a wider variety of, data about users. Indeed, the top online ad-selling companies, none of which is an ISP, have honed the ability to track users across different devices and contexts, earning the top ten such companies over 70 percent of online advertising revenue.[14]

The Commission nonetheless ignores the role that other large platform providers play in the ecosystem and instead proposes draconian rules for ISPs that would, among other things, inhibit ISPs' ability to use consumers' personal information even for first-party marketing of most services, including those that are related to, and integrated with, the broadband Internet access services ("broadband services") that ISPs provide. Specifically, the Commission proposes to require ISPs to obtain opt-in consent from customers before using their personal information for nearly all activities, including marketing most services and products other than the service to which the customer already subscribes.

The Commission's proposal is diametrically opposed to the FTC's approach. Under the FTC framework, companies generally do not need to provide consumers with choice about the use of their data for first-party marketing, because such use of data is considered consistent with the context of the consumer's relationship to the company, and the customer's consent therefore can be inferred. The FTC recommends that companies provide consumers with an opt-out mechanism when the context does not allow consent to be inferred, and recommends *opt-in* consent only in certain, very limited circumstances, such as when companies deliberately collect and market using sensitive data.[15] The FTC's approach has protected consumers while allowing

[14] *See id.* at 8.

[15] *See FTC Report* at 40-41, 57-60.

innovation and economic growth in the Internet economy. Indeed, many of the ad-supported online services that consumers enjoy today at no cost, or at a low cost, are available because of the frictionless, free flow of data made possible by the FTC's flexible, context-driven choice regime. The Commission's Proposed Rules, however, would prevent ISPs from adopting this business model, while allowing other online entities to continue doing so.

The Commission's divergence from the FTC's well-established approach to choice would confuse consumers, who do not expect different privacy protections for the same data depending on which entity holds the data or the kind of product or service that is being marketed. After consumers exercise their choice through ISPs' opt-in mechanisms, they may not understand that edge providers remain regulated under the FTC's regulatory regime. The Commission's proposed opt-in regime thus risks confusing consumers about their control over their personal information. Regardless of the choice consumers register with their ISPs, without additional action on their part, their data will continue to be available for marketing and profiling by countless other entities online with whom consumers may or may not have a relationship. The Commission's proposal likewise would frustrate consumers. Requiring ISPs to provide consumers with frequent and intrusive notices and opt-in mechanisms for the use of their personal information will interrupt broadband service and create a negative user experience.

In addition, the Commission's proposal would inhibit innovation, reduce investment, and limit competition. The Commission's proposed opt-in consent regime would limit ISPs' ability to market new services other than those to which the customer already subscribes. If ISPs are not able to freely market new services, they will have less incentive to invest in the development of such services, and without the additional sources of revenue that such services could provide, ISPs may be less inclined to invest in the deployment of network infrastructure. Likewise,

reducing ISP revenue streams will hurt competition in the ISP market by making it harder for new companies to enter. In addition, the Commission's Proposed Rules would put the government's thumb on the scale in favor of edge providers, reducing competition and limiting consumer choice for new services in a nascent and growing Internet advertising market. ISPs are new entrants to the market for online data services, where the edge providers now are and—under the Commission's Proposed Rules—will continue to be the incumbent, dominant players.

Finally, the Commission's proposal would not materially advance the privacy interests of consumers. Specifically, the Commission proposes (1) expanded notice requirements regarding ISPs' privacy policies that would degrade consumers' experiences and risk causing notice fatigue; (2) ineffective and counterproductive customer choice requirements that, as explained above, are inconsistent with well-established privacy regulation that consumers have come to expect; do not address actual privacy harms; and do not meaningfully protect consumers as their information inevitably travels throughout the Internet ecosystem; (3) data security requirements that are misguided and deeply flawed as a matter of technical security and regulatory policy; would worsen security and degrade consumers' experiences; reflect a simplistic and static view of the Internet ecosystem, network design, and risk management; and stray from well-accepted cybersecurity approaches and Administration policy; and (4) data breach notification requirements that are harmful to consumers, as they will result in over-notification and ineffective breach responses. The NPRM also asks whether the Commission should prohibit other activities like discounts for data use or arbitration procedures to resolve disputes, both of which benefit consumers and are beyond the Commission's authority to restrict. The consensus framework offered by CTIA and others would protect consumers and avoid these issues.

The Commission's Proposal is Legally Flawed. The Commission's proposal is unlawful, both as a statutory and a constitutional matter, and unnecessary, given the model that the Commission already has to draw from in the FTC's privacy framework.

As an initial matter, Section 222 does not apply to broadband Internet access services. Even leaving aside the question of whether the Commission has authority to classify broadband service as a telecommunications service in the first instance, the language of the statute and well-established principles of statutory construction make clear that Section 222 protects only a limited category of customer information of telephone *voice service* customers. And even if Section 222 were a basis for rulemaking in this proceeding, the scope of data covered by Section 222 is limited to CPNI. Section 222(a) does not provide a separate source of authority to expand the data covered by Section 222 or to impose rules for CPNI beyond those articulated in Section 222(c). Indeed, the structure of Section 222 is incoherent if Section 222(a) is interpreted otherwise. Several of the proposed rules in the NPRM exceed Section 222's limitations in other ways, including by failing to exempt de-identified data from the scope of data covered. And none of the other statutory provisions that the Commission references in the NPRM—Sections 201, 202, 705, 706, or Title III of the Communications Act, as amended—provide alternative sources of authority for the Commission's proposed rules.

Furthermore, the Commission's reading of Section 222 would lead to public policy results that would be inconsistent with the goals of Congress. Congress intended that Section 222 would *both* enhance competition *and* protect consumers in the telephone voice services marketplace. For this reason, Congress chose to protect customers' "*proprietary*" network information (*i.e.*, information that carriers could use to retain or obtain a competitive market advantage) and not customers' "*personally identifiable information*," which Congress protected

in privacy laws elsewhere in the Communications Act, both before and after Congress enacted Section 222 in 1996. As part of this dual purpose, Congress drafted Section 222, in part, to regulate incumbent carriers' marketing activities in a way that would bring competition to the telephone services market. The Commission must interpret Section 222 against this backdrop and in the context of the current marketplace, in which ISPs are actually the new entrants, adding competitive choice and options in the mobile advertising market.

Unlike the telephone voice services market that existed when Congress passed Section 222, the marketplace for wireless broadband services is competitive: more than 91.5 percent of the U.S. population can choose among three or more mobile broadband providers.[16] Thus, while rules that regulated incumbent carriers' use of CPNI for marketing may have been justified at one time to promote competition in the telephone voice services market, such rules are indefensible in the market for wireless broadband services, where competition arose without these rules. Indeed, for the reasons stated above, asymmetrical regulation of ISPs' use of CPNI would harm rather than preserve or promote competition.

Finally, the Proposed Rules that would restrict ISPs' use and disclosure of information without obtaining opt-in consent from consumers are unconstitutional. By asymmetrically prohibiting ISPs from engaging in various forms of protected commercial speech—including first party marketing, delivery of third-party advertisements, the sharing of commercial facts for legitimate business purposes, and other forms of disclosure and access to deliver effective service—the Commission has proposed a framework that imposes speaker-based and content-based burdens on speech, either of which independently renders the regulations presumptively

[16] *See In re Implementation of Section 6002(B) of the Omnibus Budget Reconciliation Act of 1993, Annual Report and Analysis of Competitive Market Conditions with Respect to Mobile Wireless, Including Commercial Mobile Services,* Eighteenth Report, 30 FCC Rcd 14,515, 14,542 Chart III.A.3 (WTB 2015) ("*Eighteenth Report*").

invalid. By requiring opt-in approval for most commercial uses, the Commission also has set a default of censorship, when there are less restrictive means of protecting specifically the consumers who desire further protections. Under either strict or intermediate scrutiny, these flaws are fatal, given the lack of any nexus between the rules and the Commission's purported interest in protecting privacy.

I. The Commission Lacks Authority To Adopt the Proposed Regulations.

Under the Administrative Procedure Act ("APA"), the Commission lacks authority to adopt regulations that are, among other things, "in excess of statutory . . . authority[] or limitations."[17] The Proposed Rules fail this standard. Most fundamentally, the Commission lacks the authority to classify broadband service as a telecommunications service—the legal predicate to adopting regulations extending Section 222 to ISPs' provision of broadband service. No less problematic, however, is that the text and legislative history of Section 222 unambiguously foreclose the Commission's attempts to adopt implementing regulations for ISPs' use and disclosure of customer information in connection with the provision of broadband service—whether or not broadband service qualifies as a telecommunications service. And even if a reviewing court were to hold otherwise, the Proposed Rules nonetheless exceed Section 222's limitations in a variety of ways—including by creating out of whole cloth a new category of customer information to be regulated that has no basis in Section 222, by defining broadband CPNI more broadly than the statute can bear, and by writing certain provisions entirely out of Section 222, rendering the statute incoherent and at odds with Congress's clear intent. The Commission fares no better when it asserts (or seeks to find) independent authority for the Proposed Rules under the following provisions in the Act as amended: Sections 201 and 202, Section 705, Section 706, or any provisions of Title III.[18]

[17] 5 U.S.C. § 706(2)(C).

[18] *See, e.g.*, *NPRM*, 31 FCC Rcd at 2596-97 ¶¶ 305-308.

A. The Commission Does Not Have Authority To Reclassify Broadband Services as a "Telecommunications Service" Under Title II of the Communications Act.

Section 222 is a Title II provision that, at its outermost edges, reaches only telecommunications service providers' provision of telecommunications services.[19] If broadband service cannot be classified as a telecommunications service, it therefore follows that Section 222 cannot be extended to ISPs' provision of broadband service. The validity of the Commission's order classifying broadband service as a telecommunications service (the "*Open Internet Order*")[20] is currently pending before the D.C. Circuit, and it is unnecessary for CTIA to rehash its objections to the *Open Internet Order* here. It is instead sufficient merely to note that the classification of broadband service as a telecommunications service is contrary to the text, structure, and history of the Communications Act; is arbitrary and capricious; and is otherwise unlawful, especially with respect to CTIA's members (*i.e.*, mobile broadband providers). Separately, the imposition of common carriage requirements on the providers of broadband service is unlawful, independently depriving the Commission of access to Section 222 as a means of regulating ISPs' provision of broadband service. And finally, the *Open Internet Order* was the product of a procedurally flawed rulemaking process, a fact which may itself prevent the Commission from adopting Section 222 rules for ISPs' provision of broadband service until engaging in a further rulemaking process—and which, if nothing else, suggests that the Commission engage in a more cautious, comprehensive approach here.[21]

---

[19] *See* 47 U.S.C. § 222. As CTIA urges below, even if broadband service can be classified a Title II service, the text and legislative history of the provision demonstrate it is unambiguously limited only to voice services, and cannot encompass other telecommunications services.

[20] *In re Protecting and Promoting the Open Internet*, Report and Order on Remand, 30 FCC Rcd 5601 (2015) ("*Open Internet Order*").

[21] *See generally* Joint Brief for Petitioners Alamo Broadband, Inc. and Daniel Berninger, *United States Telecom Ass'n v. FCC* (D.C. Cir. July 30, 2015) (No. 15-1063).

B. Even If the Commission Has Authority to Classify Broadband Service as a Telecommunications Service, It Lacks Authority To Extend Section 222 to ISPs' Provision of Broadband Service.

Even if the D.C. Circuit upholds the Commission's authority to classify broadband services as a "telecommunications service" under Title II, Section 222 of the Communications Act nonetheless unambiguously does not apply to broadband service. Both the plain language of Section 222 and the legislative history make clear that Congress drafted this section to protect certain information that carriers obtain solely by providing *voice* services to customers in a concentrated, closed market. The Proposed Rules exceed this limited scope by protecting information obtained by carriers by virtue of providing broadband service in a vast and competitive mobile broadband market; the Rules therefore are impermissible, even before a reviewing court could proceed to *Chevron*'s deferential second step of review.[22]

1. The Text of Section 222, as Enacted and Subsequently Amended, Unambiguously Forecloses Application to Broadband Service.

Section 222 is unambiguously about voice service, as Congress made clear through its numerous references throughout the provision to "*call*[*s*],"[23] "*call* location information,"[24] "*local exchange* carrier[s],"[25] "IP-enabled *voice* service[s],"[26] "*telephone exchange* service[s],"[27] *telephone toll* service[s],"[28] "*telemarketing*,"[29] and "subscriber list information"—a term defined

---

[22] *See Chevron U.S.A. Inc. v. Nat. Res. Def. Council, Inc.*, 467 U.S. 837 (1984); *Petit v. U.S. Dep't of Educ.*, 675 F.3d 769, 781 (D.C. Cir. 2012) ("Moreover, at [*Chevron*] step one, a court must exhaust the traditional tools of statutory construction to determine whether Congress has spoken to the precise question at issue. The traditional tools include examination of the statute's text, legislative history, and structure, as well as its purpose." (quotation marks omitted)).

[23] 47 U.S.C. § 222(d)(3), (d)(4), (f)(1) (emphasis added).

[24] *Id.* § 222(d)(4) (emphasis added).

[25] *Id.* § 222(c)(3) (emphasis added).

[26] *Id.* § 222(d)(4) (emphasis added).

[27] *Id.* § 222(e), (g), (h)(1)(B) (emphasis added).

[28] *Id.* § 222(h)(1)(B) (emphasis added).

in the statute as the "listed names of subscribers of a carrier and such subscribers' *telephone numbers*, addresses, or primary advertising classifications."[30]

Furthermore, in its revisions to the Communications Act in 1996, Congress made clear when it sought to regulate voice telephony services, on the one hand, and other kinds of services, on the other. For example, Congress expressly distinguished Internet-related services from services supported by circuit-switched telephone networks to make clear that Section 230 of the Act applied to Internet-related services, and not to telephony. Section 230, which limits the liability of providers and users of "interactive computer services,"[31] expressly applies to Internet content delivered over "packet switched data networks," as opposed to telephone exchange services.[32] Moreover, Section 230 defines "interactive computer services" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides *access to the Internet*."[33] Thus, Congress understood the technological distinctions between Internet access services and voice telephony, and it was careful to make clear precisely what kind of service it intended to regulate. Accordingly, had Congress intended Section 222 to apply to services that provided "access to the Internet" instead of, or in addition to, "telephone exchange services," it knew how to do so, but chose not to, deliberately limiting the application of Section 222 to telephone voice services.

---

[29] *Id.* § 222(d)(3) (emphasis added).

[30] *Id.* § 222(e), (h)(3).

[31] *Id.* § 230(a), (b).

[32] *Id.* § 230(f)(1).

[33] *Id.* § 230(f)(2) (emphasis added).

Indeed, the only references to any Internet-related services in Section 222 are to Internet Protocol ("IP")–enabled *voice service*, further underscoring that Congress never intended this particular provision of Title II to reach broadband service. Specifically, Section 222(d)(4), excludes "*call* location information concerning the user . . . of an *IP-enabled voice service*" from the general prohibitions in the statute relating to the use and disclosure of CPNI.[34] Congress enacted this provision in 2008 to ensure that first responders could receive information necessary to locate callers who use IP-enabled voice services.[35] It is clear from the legislative history that Congress recognized this revision was necessary because, as drafted in 1996, Section 222 applied *only* to wireline and wireless telephony services, not IP-enabled voice services.[36] Congress did not further amend Section 222 to capture other Internet-related services or data.

Section 222 therefore does not apply to broadband services, other than to Internet-enabled *voice* service, and even there, it merely operates to permit carriers to disclose "call location information" relating to subscribers of VoIP services under the circumstances enumerated in Section 222(d)(4). The scope and purpose of the subsequent amendments to Section 222 foreclose any interpretation that would extend Section 222's ambit to cover ISPs or bring Internet-related communications under the definition of CPNI, other than the small subset

[34] *Id.* § 222(d)(4) (emphasis added).

[35] *See* New and Emerging Technologies 911 Improvement Act of 2008, Pub. L. No. 110-283, § 301, 122 Stat. 2620, 2625; *see also* H.R. Rep. 110-442, at 18 (2007), *as reprinted in* 2008 U.S.C.C.A.N. 1011, 1023 (explaining that Section 301 was necessary "so that VoIP providers may give customer information, including location information, to the appropriate PSAP").

[36] H.R. Rep. 110-442, at 7, *as reprinted in* 2008 U.S.C.C.A.N. at 1013 ("The provision of E-911 service by VoIP providers also implicates section 222 of the Communications Act of 1934, which governs the protection of [CPNI]. Section 222 includes exceptions to its protections to allow wireline and wireless carriers to provide customer information to PSAPs in emergency situations. There is no similar provision governing or granting exceptions for VoIP service.").

of call location information generated through VoIP services.[37] *American Library Association v. FCC* is instructive: there, the D.C. Circuit held that subsequent legislation confirmed that the Commission's proffered interpretation of the Communications Act exceeded the Commission's ancillary jurisdiction; so too here, "Congress's principal purpose" in enacting Section 222(d)(4) "was clearly to" clarify how Section 222 covered a specific IP-enabled service, and that purpose "is inconsistent with the FCC's current view that it always has had" authority to regulate IP-related services under Section 222.[38]

2. The Legislative History of Section 222 Likewise Demonstrates That Application to Broadband Service Is Impermissible.

Commission orders and reports repeatedly have acknowledged that Congress drafted Section 222 for two primary reasons: (1) to protect the confidentiality of a certain, narrow category of information to which carriers had unique access by virtue of providing *telephone services* to their customers (*i.e.*, customer proprietary network information ("CPNI")), and (2) to foster competition in the *telephone services market*.[39] The Commission's proposal to extend Section 222 to ISPs' provision of broadband service would not achieve either of these goals. In fact, the Proposed Rules seek to regulate not just CPNI, but a brand new, broad category of customer information, and they would inhibit, rather than promote competition in the market

[37] *See Am. Library Ass'n v. FCC*, 406 F.3d 689, 706 (D.C. Cir. 2005) ("It is enough here for us to find that the Communications Act of 1934 does not indicate a legislative intent to delegate authority to the Commission to regulate consumer electronic devices that can be used for receipt of wire or radio communications when those devices are not engaged in the process of radio or wire transmission. That is the end of the matter. It turns out, however, that subsequent legislation by Congress *confirms* the limited scope of the agency's ancillary jurisdiction and makes it clear that the broadcast flag regulations exceed the agency's delegated authority under the statute.").

[38] *Id.* at 707.

[39] *See, e.g.*, *In re Implementation of the Telecommunications Act of 1996*, Clarification Order and Second Further *NPRM*, 16 FCC Rcd 16,506, 16,514-15 ¶ 17 (2001); *In re Implementation of the Telecommunications Act of 1996*, Second Report and Order and Further *NPRM*, 13 FCC Rcd 8061, 8068-70, 8073-74 ¶¶ 7, 14 (1998) ("*CPNI Second Report and Order*") (describing legacy CPNI rules and Section 222 as reflecting principles of protecting customer privacy and promoting competition among CLECs).

relevant to the Commission here—the online advertising market. The Commission's Proposed Rules thus do not further, and in some respects contradict, the intent of Congress and therefore exceed the Commission's statutory authority.[40]

First, under the clear language of Section 222, CPNI is a discrete category of information that includes, among other things, the type of service a customer subscribes to and a customer's telephone call detail records. By definition, it is information that customers make available to telephone companies "*solely* by virtue of the carrier-customer relationship."[41] Congress deemed CPNI to be sensitive in part because it is "proprietary" information (*i.e.*, information that, at the time, gave its holder a competitive advantage in the burgeoning market for local and long distance voice services), and because it includes information, such as call detail records, that at the time was not available to anyone outside of the customer-carrier relationship. In other words, in the voice context, Congress viewed CPNI as valuable and sensitive because, at the time, it was not available to anyone *other than* the carrier and the carrier's telephone services customer (or other limited entities for the sole purpose of providing the telephone service).[42]

---

[40] *See* cases cited, *supra* note 22; *see also Gen. Dynamics Land Sys., Inc. v. Cline*, 540 U.S. 581, 600 (2004) (confirming that *Chevron* step one inquiry permits recourse to "text, structure, purpose, and history").

[41] 47 U.S.C. § 222(h)(1)(A) (emphasis added). Section 222(h)(1) states that CPNI means "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is *made available to the carrier by the customer solely by virtue of the carrier-customer relationship*; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service *received by a customer of a carrier*." *Id.* (emphases added.) Although only subsection (A) uses the phrase "made available to the carrier by the customer *solely by virtue* of the carrier-customer relationship," both subsections (A) and (B) describe information that is uniquely available to the carrier because of the carrier-customer relationship. Unlike the information listed in subsection (A), bills pertaining to telephone service are generated *by* the carrier; therefore, telephone bills are not made available *to* the carrier "by the customer" but instead are, as the statute states, "*received by* [*the*] *customer of* [*the*] *carrier*." The critical point is that CPNI—*both* the bills *and* the information listed in subsection (A)—is available to the carrier "solely by virtue of the carrier-customer relationship."

[42] As discussed at greater length below in Part V.A.3, intervening changes in the voice market call into serious question whether this information that customers make available to carriers can still be considered "proprietary."

This description will sound foreign to anyone familiar with the broadband ecosystem, where customers' data are necessarily and constantly available to a host of entities that use the data for a variety of purposes, including delivering broadband services to customers, managing broadband networks, and providing ad-supported content and online services.[43] Some of these entities have relationships with consumers, but many do not. Indeed, numerous non-consumer facing companies, such as online advertising networks and data analytics companies, collect a wide range of data about consumers' online activities (*e.g.*, web browsing history), personal characteristics (*e.g.*, gender and age), and network connection (*e.g.*, browser and operating system type, and physical location). Some of these companies combine this data with other data, including data about consumers' offline activities and from public or third-party databases, and sell the combined data to other third parties for use in targeted marketing.[44] Thus, numerous third parties regularly obtain much of the same data to which ISPs have access by virtue of the carrier-customer relationship. This information is *not* uniquely available to ISPs in the Internet context in the way that CPNI, at least at one time, was uniquely available to carriers in the voice services context. Moreover, because there is an actual market for this data in the Internet ecosystem, any company, including ISPs, can obtain this information about their customers from third parties, irrespective of the ISPs' relationships with their customers. Thus, unlike in the traditional voice services context, much of this information is widely available to ISPs and other entities in the marketplace.

Second, Congress recognized that CPNI is a valuable marketing asset for telephone companies, and sought to regulate it, in part, to promote competition in the telephone services

[43] *See Swire Report* at 6-14.

[44] *See infra* Part V.A.2 (discussing open nature of broadband data ecosystem and other entities' extensive access to and use of customer information available to ISPs).

market in the wake of the Bell divestiture. Congress was concerned that, due to their unique access to CPNI by virtue of providing voice service, "[incumbent c]arriers already in possession of CPNI could leverage their control of CPNI in one market to perpetuate their dominance as they enter other service markets."[45]

Here too, Congress's interest has no recognizable application in the Internet ecosystem, where multiple entities have access to, and use for commercial purposes, the data that consumers generate online. Indeed, as discussed in more detail below, the free flow of digital information is the lifeblood of the Internet economy and the means by which many online consumers obtain access to content for which they otherwise would have to pay a subscription (or access) fee. This critical difference distinguishes the open Internet ecosystem from the closed telephone voice services market, where traditional voice and VoIP carriers have not used subscribers' call detail records and telephone usage information to target advertising to support access to services.[46]

Moreover, when Congress enacted Section 222, incumbent local exchange carriers in the voice services market held a competitive advantage, in part because they could use their customers' CPNI to identify potential customers for new services. In the Internet ecosystem, however, the situation is reversed. Here, the ISPs are the new entrants to the market for many online products and services, while the edge providers (search engines, social media platforms, advertising networks, and others) are the incumbent, dominant players. Thus, subjecting ISPs to more restrictive rules than those that apply to edge providers would inhibit, rather than promote, competition for online products and services.

---

[45] *CPNI Second Report and Order*, 13 FCC Rcd at 8089-90 ¶ 37.

[46] As discussed at greater length below, even voice CPNI has, in critical respects, lost its "proprietary" characteristics, as new entrants (*e.g.*, Skype) have disrupted the voice services market, and as new types of entities (*e.g.*, Operating Systems and App providers) have gained access to call logs. *See infra* Part V.A.3.

3. The Commission Implicitly Acknowledged Section 222's Inapplicability to ISPs' Provision of Broadband Service by Forbearing from Applying Its CPNI Rules in the *Open Internet Order*.

For the foregoing reasons, applying Section 222 to ISPs would flout the intent of Congress to protect CPNI in the voice services market, given the closed nature of voice services information flows from customer to carrier, and to foster competition among the various carriers that offered telephony services to consumers.

The Commission recently acknowledged as much in the *Open Internet Order*. There, the Commission expressly forbore from applying its voice CPNI rules to ISPs, because the rules "appear[ed] to be focused on addressing the problems that historically arise regarding voice service."[47] As the plain language and legislative history of Section 222 make clear, however, the same is true of Section 222 itself. Congress drafted Section 222 to regulate carriers of voice services, not ISPs. And, as noted, in 2008, Congress passed legislation to amend the statute to cover a small subset of IP-enabled voice services because the statute, as written, otherwise covered only traditional telephony voice services. Congress appropriately recognized that the Commission would be unable to address this VoIP gap through rulemaking because the statute is not interstitial on this point: any such regulations would have been unambiguously foreclosed by Section 222's text and history. The same is true of the Commission's Proposed Rules here.

C. Regardless Whether Section 222 Could Be Extended to Broadband Service, the Proposed Rules Exceed Other Limitations in Section 222.

Even if Section 222 could be construed to encompass ISPs' provision of broadband service, which it cannot, any corresponding rules regulating ISPs otherwise must accord with

[47] *Open Internet Order*, 30 FCC Rcd at 5823-24 ¶ 467.

Section 222's structural and textual limitations.[48] The Proposed Rules exceed these limits in multiple ways.

Most significantly, the Commission proposes to protect an entirely new, made-up category of information that the Commission calls "customer proprietary information," which includes broadband CPNI elements as well as "personally identifiable information (PII)."[49] To make matters worse, the NPRM routinely abbreviates "customer proprietary information" as "customer PI"—an abbreviation that seems almost intended to invite confusion, as "PI" generally is understood in the privacy context to mean "Personal Information," not "Proprietary Information."[50] The term "customer proprietary information" appears nowhere in the Communications Act, and the Commission lacks authority to create it: Section 222(a) is not an independent grant of rulemaking authority, and the structure of Section 222 unambiguously forecloses rules protecting any category of customer information other than CPNI in any event.

Beyond this category-level error, the Proposed Rules and alternatives also exceed Section 222 in other ways: by failing to exclude de-identified data; by defining CPNI more broadly than the statutorily defined term will bear; by potentially restricting ISPs from using, disclosing, or permitting access to information even with customer approval; by potentially imposing restrictions on ISPs' uses of information obtained by means other than providing broadband service; and by potentially prohibiting or restricting ISPs' use of arbitration.

---

[48] *See supra* note 22.

[49] *See NPRM*, 31 FCC Rcd at 2518-20 ¶¶ 56-60.

[50] Notwithstanding its statutory and policy objections, CTIA uses the phrase "customer proprietary information" as necessary in these Comments to address the merits of the NPRM proposals.

1. Read Holistically, Section 222 Does Not Permit the Commission to Interpret Section 222(a) to Protect Any Category of Customer Information Beyond CPNI.

The Proposed Rules would encompass not just CPNI, but also a new, made up category of information dubbed "customer proprietary information."[51] The Commission's atomistic interpretation of Section 222(a) to identify the scope of customer information that the statute covers is untenable when Section 222 is interpreted holistically.[52] The text and structure of Section 222, as well as its legislative history, make clear that CPNI is the *only* customer data that Section 222 protects. Indeed, the statute is coherent and internally consistent only if "proprietary information," as it relates to customers in Section 222(a), is interpreted to be coterminous with CPNI. Any interpretation of Section 222(a) that expands the scope of customer data protected beyond CPNI is therefore impermissible.

The analysis starts with Section 222's structure. Section 222(a), which is titled "In General," articulates a general requirement that carriers protect the confidentiality of "proprietary information," not only of customers, but also of other carriers and of equipment manufacturers.[53] Section 222(c) explains how this general prohibition operates with respect to customers. And

---

[51] *See NPRM*, 31 FCC Rcd at 2518-20 ¶¶ 56-59.

[52] *See, e.g.*, *Petit*, 675 F.3d at 781-82; *County of Los Angeles v. Shalala*, 192 F.3d 1005, 1014 (D.C. Cir. 1999) ("[T]o prevent statutory interpretation from degenerating into an exercise in solipsism, we must not be guided by a single sentence or member of a sentence, but look to the provisions of the whole law. Under *Chevron* step one, we consider not only the language of the particular statutory provision under scrutiny, but also the structure and context of the statutory scheme of which it is a part." (citations and internal quotation marks omitted)).

[53] Section 222(b) explains how this general prohibition operates with regard to *carriers' information*. The reference to the "proprietary information" of *equipment manufacturers* in Section 222(a) reflects Congress's intent to foster competition in the telephone services market. Specifically, Congress imposed certain conditions on Bell operating companies ("BOCs") that sought to engage in the manufacturing of equipment. The Act permitted them to do so, provided that they comply with a number of safeguards, including restrictions on self-dealing. (Section 273(d)(2) of the Act outlines these restrictions.) As Congress explained, "the BOC must make procurement decisions and award all supply contracts using open, competitive bidding procedures, must permit any person to participate in establishing standards and certifying equipment used in the network, may not restrict sales or equipment to other local exchange carriers, *and must protect proprietary information concerning standards and certification of equipment unless specifically authorized*." S. Rep. No. 104-23, at 6 (1995) (emphasis added).

Section 222(c) expressly limits the type of customer information to which the statute applies to CPNI, which is defined in Section 222(h) to mean *only* information related to the (1) quantity; (2) technical configuration; (3) type; (4) destination; (5) location; and (6) amount of use of a telecommunications service; and (7) information contained in bills pertaining to telephone exchange service or telephone toll service.[54] In short, the most natural reading of Section 222 is that subsection (a)'s general mandate is specifically set forth for customers in subsection (c), which uses a term that is precisely defined in subsection (h). It is not an independent basis for the Commission's proposed privacy notice requirements, choice mechanisms, or data security standards because it does not provide the Commission with freestanding regulatory authority. Instead, it identifies which entities have responsibility to protect information, and informs the reading of the subsequent subsections, which articulate how these entities must protect information.[55]

There is, of course, no requirement that an agency adopt the most natural interpretation of an ambiguous statute,[56] but the interpretation proffered by the Commission is impermissible for a variety of reasons. At the outset, the mere fact that Section 222(a) contains a general requirement and a seemingly vague term (*i.e.*, "proprietary information") is not enough, without

[54] 47 U.S.C. § 222(c), (h). The scope of these seven categories is discussed below. The definition of CPNI does not include customers' names, addresses, and phone numbers. *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14,409, 14,487 ¶ 146 (1999) ("*1999 CPNI Order*").

[55] The Commission's authority to regulate the security of CPNI is found in Section 222(c)(1), which imposes restrictions on carriers' ability to "permit access to individually identifiable [CPNI]." Section 222(c)(1) thus provides the Commission with a specific grant of authority to regulate data security. A more expansive reading of the statute that gave the Commission authority to regulate the security of CPNI under Section 222(a) impermissibly would render Section 222(c)(1) redundant. *See infra*, cases cited, note 58.

[56] *See Pauley v. BethEnergy Mines, Inc.*, 501 U.S. 680, 702 (1991) (explaining that agency interpretation "need not be the best or most natural one by grammatical or other standards" if it is permissible and reasonable).

more, to render the provision ambiguous as to the scope of customer information that is subject to protections.[57]

More important, if Section 222(a) covered customer information other than the categories listed in Section 222(h), other provisions in Section 222 would make no sense. For example, under the Commission's interpretation of Section 222(a), Sections 222(e) and (g) effectively would be rendered null. Section 222(e) mandates carriers disclose "subscriber list information" (*i.e.*, customers' name, address, and phone numbers) to third-party directory publishers when such information has been published by the carrier itself. Similarly, Section 222(g) mandates carrier disclosure of subscriber information to first responders. If Section 222(a) imposed a separate requirement on carriers to protect that information, then Congress would have added subsection (a) to the list of subsections—(b), (c), and (d)—that are trumped by Section 222(e)'s and Section (g)'s disclosure requirements. Congress did not do so. The Commission's interpretation of Section 222(a) effectively would remove the "subscriber list" disclosure requirements in subsections (e) and (g) entirely out of the statute. Thus, under the Commission's interpretation of Section 222(a), a carrier's compliance with the disclosure requirements of subsections (e) and (g) would constitute a violation of subsection (a). Obviously, the Commission's interpretation of Section 222(a) cannot stand.[58]

---

[57] A court would not let the "general language" of Section 222(a) "create an ambiguity" in the specific application of Section 222(c). *See Jogi v. Voges*, 480 F.3d 822, 834 (7th Cir. 2007) ("It is a mistake to allow general language of a preamble to create an ambiguity in specific statutory . . . text where none exists."); *cf. Bhd. of R.R. Trainmen v. Balt. & Ohio R.R. Co.*, 331 U.S. 519, 528-29 (1947) (explaining that "title" and "headings" of a statute are "of use only when they shed light on some ambiguous word or phrase" but "cannot undo or limit that which the text makes plain").

[58] *Indep. Ins. Agents of Am., Inc. v. Hawke*, 211 F.3d 638, 644-45 (D.C. Cir. 2000) (rejecting agency's interpretation at *Chevron* step one based, in part, on canon "of avoiding surplusage"); *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)).

Similarly, if Section 222(a) were read to impose an independent duty on carriers to protect customer information other than CPNI, the exceptions Congress set forth in Section 222(d) would not make sense. Section 222(d) provides exceptions to the general prohibition on the use and disclosure of CPNI for purposes such as billing, deterring fraud, and assisting emergency health, law enforcement, and fire personnel. These exceptions apply only to CPNI and do not extend to any other customer information, such as the broader category of "customer proprietary information" that the Commission suggests might be protected under Section 222(a). If, therefore, Section 222(a) allowed the Commission to protect a category of information beyond CPNI, the statute would permit a carrier to share CPNI with first responders in the event of a threat to life or property but, in those same potentially life-or-death circumstances, would prohibit the carrier from disclosing to first responders some other category of "customer proprietary information," such as the names of other users associated with an account.[59] Congress cannot have contemplated this absurdity.[60]

Further, the legislative history shows that Congress intended to limit the scope of "proprietary" information covered by Section 222 to CPNI, as defined in Section 222(h)(1), and not some broader category of customer "proprietary" information that it did not bother to define. For instance, the Conference Report described Section 222 as "striv[ing] to balance both competitive and consumer privacy interests with respect to *CPNI*."[61] To that end, the final bill

[59] 47 U.S.C. § 222(d).

[60] *See Mova Pharm. Corp. v. Shalala*, 140 F.3d 1060, 1068 (D.C. Cir. 1998) (invoking canon against absurdity at *Chevron* step one and noting that "[i]n deciding whether a result is absurd, we consider not only whether that result is contrary to common sense, but also whether it is inconsistent with the clear intentions of the statute's drafters").

[61] H.R. Rep. No. 104-458, at 205 (1996) (Conf. Rep.) (Joint Explanatory Statement of the Committee of Conference) (emphasis added); *see also In re TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture ("*TerraCom/YourTel NAL*"), 29 FCC Rcd 13,325, 13,352-53, Dissenting Statement of Commissioner Michael O'Rielly (2014) (quoting Conf. Rep.).

circumscribed the customer information that the statute would cover by limiting such information to the precise categories listed in Section 222(h)(1). The House version of the bill had included a catch-all category: in addition to the information currently listed in Section 222(h), the House bill also defined as CPNI "such other information concerning the customer as is available to the local exchange carrier by virtue of the customer's use of the carrier's telephone exchange service or telephone toll services, and specified as within the definition of such term by such rules as the Commission shall prescribe consistent with the public interest."[62] In addition, the Senate version of the bill defined the customer information covered by this section broadly as "customer-specific proprietary information," with no limiting language.[63] Congress ultimately deleted these open-ended and residual categories, however, indicating that Congress did not want to create a category of "customer proprietary information" that was broader than CPNI. The legislative history thus confirms that Congress did not intend for the Commission to regulate privacy generally, and instead intended to limit the Commission's authority to the *narrow* and *expressly defined* categories of telephone-centric information listed in Section 222(h). In short, the Commission always has lacked *carte blanche* authority to expand the scope of customer information to which the statute applies.

In the NPRM, the Commission cites a recent Notice of Apparent Liability and Consent Order ("NAL") in *TerraCom/YourTel* for the proposition that Section 222(a) encompasses "customer proprietary information," a new, non-statutorily defined category of information.[64]

---

[62] H.R. Rep. No. 104-204(I), at 23 (1995).

[63] S. Rep. No. 104-23, at 24.

[64] *NPRM* , 31 FCC Rcd at 2518-19 ¶ 56; *see also In re TerraCom, Inc. and YourTel America, Inc.*, Order, 30 FCC Rcd 7075, 7079 ¶ 2 (2014) (defining "proprietary information" under Section 222(a) to include "all types of customer information that should not be exposed widely to the public, whether because that information is sensitive for economic reasons or for reasons of personal privacy; including but not limited to such confidential information as privileged information, trade secrets, and personally identifiable information—information that can be used on its

The Commission's reliance on the *TerraCom/YourTel* NAL fails. In the *TerraCom/YourTel* NAL, the Commission ignored its previous longstanding position—*viz.*, Section 222 covers only three categories of customer information: (1) individually identifiable CPNI; (2) aggregate customer information; and (3) subscriber list information,[65]—and relied on two sentences from two previous Commission orders to assert that Section 222(a) imposes a broader obligation. But in cherry-picking those two sentences, the NAL mischaracterized those orders.

Specifically, the NAL cited a 2007 Commission Order that established the Commission's pretexting rules (the "*2007 CPNI Order*") for the proposition that it "expect[s] carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information."[66] The next two sentences of the *2007 CPNI Order*, however, make clear that the Commission was talking about CPNI, not some broader category of proprietary information: "Of course, we require carriers to implement the specific minimum requirements set forth in the Commission's new pretexting rules. We further expect carriers to take additional steps to protect the privacy of CPNI to the extent such additional measures are feasible for a particular carrier."[67]

---

own or with other information to identify, contact, or locate a single person, or to identify an individual in context"); *In re AT&T Services, Inc.*, Order, 30 FCC Rcd 2808 (2015) (finding that Section 201(b) applies to carriers' practices for protecting both customers' personally identifiable information *and* CPNI).

[65] *See, e.g.*, *CPNI Second Report and Order*, 13 FCC Rcd at 8064 ¶ 2; *In re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended*, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14,860, 14,864 ¶ 6 (2002); *see also U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1228 n.1 (10th Cir. 1999). Indeed, the Commission previously denied a "request that the Commission hold that section 222 controls all issues involving customer information, rather than issues pertaining to CPNI." *See In re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14,409, 14,888 ¶ 147 (1999).

[66] *In re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further NPRM, 22 FCC Rcd 6927, 6959 ¶ 64 (2007) ("*2007 CPNI Order*"); *TerraCom/YourTel NAL*, 29 FCC Rcd at 13,330 ¶ 13 n.30.

[67] *2007 CPNI Order*, 22 FCC Rcd at 6959 ¶ 64.

The references to CPNI are also pervasive in the surrounding paragraphs.[68] The Commission went on in the same paragraph to mention its expectation that carriers take "reasonable measures" to prevent pretexting,[69] referring back to an earlier section of the *2007 CPNI Order* that indicated that, under Section 222(a), the Commission was codifying a requirement to take "reasonable measures" against pretexting.[70] Notably, the rule the Commission adopted to codify this "reasonable measures" requirement under Section 222(a) applies only to CPNI: "Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[71] The preceding reference to "personal customer information" necessarily reflects Section 222's requirement that carriers protect "individually identifiable" *CPNI* (*i.e.*, the personal information that renders CPNI "individually identifiable").

The NAL additionally cites a sentence in the Commission's *2013 Mobile Device CPNI Ruling*: "We also note that subsection (a)'s obligation to protect customer information is not limited to CPNI that the carrier has obtained or received."[72] But in context, it is clear that this sentence does not suggest that Section 222(a) covers customer information beyond CPNI (or aggregate customer information or subscriber list information). Rather, this sentence explains that Section 222(a) obliges carriers to protect *CPNI* that they have not yet "obtained or received": "[t]he fact that *CPNI* is on a device and *has not yet been transmitted to the carrier's*

[68] *See generally id.* at 6959-60 ¶¶ 63, 65.

[69] *See id.* at 6959 ¶ 64.

[70] *Id.* at 6945-46 ¶¶ 33-34 & n.106.

[71] 47 C.F.R. § 64.2010(a).

[72] *In re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Declaratory Ruling, 28 FCC Rcd 9609, 9618 ¶ 27 (2013) ("*2013 Mobile Device CPNI Ruling*").

own servers also does not remove the data from the definition of *CPNI*."[73] This sentence thus confirms that Section 222(a) applies only to CPNI, not a broader category of information.

Even if the NAL followed from prior Commission orders, which it does not, the Proposed Rules still would not comprise a permissible interpretation of Section 222—regardless of the merits of the NAL, or the policy interests the Commission has since identified in support of protecting a broader category of information than CPNI.

Moreover, Congress drafted Section 222 to cover "proprietary information," not "personal information" or "personally identifiable information" ("PII"), the latter of which are the kinds of information that privacy laws typically protect.[74] Congress generally has defined "personal information" and "PII" to mean information that identifies an individual (or that, when linked to other information, can identify an individual). Congress chose to draft Section 222 in a different manner from privacy laws that protect "personal information" or "personally identifiable information," *including privacy laws that amended the Communications Act.* Indeed, Congress used the term "personally identifiable information" elsewhere in the Communications Act, both before and after Congress drafted Section 222 in 1996. For example, in 1984, Congress imposed certain duties on cable operators to protect the privacy of "personally identifiable information concerning any subscriber."[75] Likewise, in 2004, Congress imposed similar duties on satellite operators to protect the privacy of "personally identifiable information"

[73] *Id*. (emphases added).

[74] *See infra* note 78.

[75] Cable Communications Policy Act of 1984, Pub. L. No. 98-549, § 631, 98 Stat. 2779, 2794-95 (establishing Section 631 of the Communications Act, codified at 47 U.S.C. § 551, to protect the privacy of cable subscribers' "personally identifiable information").

of satellite subscribers.[76] If Congress similarly had wanted Section 222 to cover "personally identifiable information" and not just CPNI, it knew how to do so and would have done so.[77] In addition to the privacy laws that amended the Communications Act, Congress also passed a number of other privacy laws that protect "personal information" or "personally identifiable information" (but not "proprietary information") around the same time that it passed Section 222.[78]

The Commission must give Congress's deliberate usage effect in its regulations. Congress used the term "proprietary information" in Section 222, as opposed to "personal information" or "personally identifiable information," because it intended Section 222 to serve a different purpose. Specifically, because CPNI was available only to carriers and their customers, Congress was concerned that "[incumbent c]arriers already in possession of CPNI could leverage their control of CPNI in one market to perpetuate their dominance as they enter other service markets."[79] Unlike "personal information" and "personally identifiable information," which can be held by multiple persons and commercial entities without losing its character as "personal

---

[76] Satellite Home Viewer and Reauthorization Act of 2004, Pub. L. No. 108-447, § 206, 118 Stat. 2809, 3393, 3425-26 (establishing Section 338(i) of the Communications Act, codified at 47 U.S.C. § 338(i), to protect the privacy of satellite subscribers' "personally identifiable information").

[77] Just as it did in the Communications Act, Congress has distinguished the terms "proprietary information" and "personally identifiable information" from one another elsewhere when they appeared together in the same statutes. For example, Congress directed the Director of the Federal Housing Finance Agency, which is required to collect and make public certain mortgage-related information from Federal Home Loan Banks, to protect information "that the Director determines is proprietary *or* that would provide personally identifiable information." 12 U.S.C. § 1430(k)(2)(B) (emphasis added).

[78] These privacy statutes include the Children's Online Privacy Protection Act ("COPPA"), the Gramm-Leach-Bliley Act, and the Video Privacy Protection Act, to name a few. *See* Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681, 2681-728 (codifying definition of children's "personal information" at 15 U.S.C. § 6501(8)); Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codifying definition of "nonpublic personal information" at 15 U.S.C. § 6809(4)); Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (codifying definition of "personally identifiable information" at 18 U.S.C. § 2710); *see also, e.g.*, Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380 § 513, 88 Stat. 484 (codifying at 20 U.S.C. § 1232g(b)(2) certain protections for students' "personally identifiable information").

[79] *CPNI Second Report and Order*, 13 FCC Rcd at 8089-90 ¶ 37.

information" or "PII," "proprietary information" is information that a person or entity owns to the exclusion of others.[80] Put another way, a person cannot claim that information is "proprietary" if other individuals or entities can access the information and use it for their own commercial purposes.[81] Indeed, Congress has passed numerous laws that recognize the commercial value of *proprietary information* and that protect such information for *that* reason.[82]

In the *Open Internet Order*, the Commission *also* uses the term "proprietary" to refer to information that is sensitive because it has commercial value, not because it reveals information about an individual. For instance, the Open Internet rules allow parties to request that information they submit in a proceeding be designated as "proprietary" and therefore withheld under exceptions to the Freedom of Information Act disclosure provisions. These include an exception for "trade secrets and commercial or financial information obtained from a person and privileged or confidential."[83] As the 2010 *Open Internet Order* explained in announcing this provision (which the 2015 Order retained), "[t]he rule does not require public disclosure of

---

[80] *Proprietary*, Merriam-Webster Dictionary, http://www.merriam-webster.com/dictionary/proprietary (last visited May 6, 2016) (held as property; used, made, or marketed by one having the exclusive legal right).

[81] *See Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh*, 691 F.3d 821, 833 (6th Cir. 2012) (upholding district court decision regarding insurance coverage for loss resulting from theft of electronically stored customer information and finding that that loss of *proprietary information* would mean the loss of information "to which Plaintiffs own or hold single or sole right" but the "stolen customer information was not 'proprietary information' at all, since the information is owned or held by many, including the customer, the financial institution, and the merchants to whom the information is provided in the ordinary stream of commerce" and therefore "would not come within the plain and ordinary meaning of 'proprietary information'").

[82] *See* 25 U.S.C. § 2103(c) (requiring the Department of the Interior to protect the "*proprietary information*" of Indian tribes that submit to the Department "projections, studies, data or other information…regarding…the extent, nature, value or disposition of the Indian mineral resources, or the production, products, or proceeds thereof" in connection with Minerals Agreements (emphasis added)); 7 U.S.C. § 8783(f) (requiring the Secretary of Agriculture to protect "*proprietary information*" submitted to the Department by oilseed producers in connection with proposals for quality incentive payments distributed by the Department (emphasis added)); Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, § 232(c), 128 Stat. 3292, 3333 (requiring individuals who participate in research and development pilot programs run by the Department of Defense to agree to the "nondisclosure of any trade secrets or other nonpublic or *proprietary information* which is of *commercial value* to the covered entity" (emphases added)).

[83] *Open Internet Order*, 30 FCC Rcd at 5887-88 App. A, Final Rules, § 8.16(a); 5 U.S.C. § 552(b)(4).

competitively sensitive information."[84] The Commission even distinguishes "personal" from "proprietary" information in its discussion about applying Section 222 to ISPs, where it asserts that broadband providers can obtain "personal *and* proprietary information about their customers."[85]

2. Regardless Whether 222(a) Could Be Construed to Vest the Commission with Authority to Define "Proprietary Information" Beyond CPNI, That Category Cannot and Should Not Be Extended to De-Identified Data.

The Commission has acted beyond the scope of its authority by proposing to define "customer proprietary information" as "any information that is linked or linkable to an individual."[86] This definition could be interpreted to capture virtually any information that an ISP acquires in connection with its provision of broadband service. This definition has no basis in law, has no limiting principle (other than that the ISP obtained the information by providing service), would be unworkable in practice, would not protect consumers, and would severely limit the consumer and societal benefits derived from such data. It therefore fails at both steps of *Chevron* review.

a. Section 222(c)(1) Unambiguously Excludes De-Identified Data.

CTIA has previously addressed in a separate filing whether Section 222 can be interpreted to encompass de-identified data; the answer is unequivocally no.[87] Nothing has

[84] *In re Preserving the Open Internet Broadband Industry Practices*, Report and Order, 25 FCC Rcd 17,905, 17,937 ¶ 55 (2010) ("*2010 Open Internet Order*").

[85] *See Open Internet Order*, 30 FCC Rcd at 5821 ¶ 463.

[86] *NPRM*, 31 FCC Rcd at 2519-20 ¶¶ 57, 60.

[87] *See In re Petition of Public Knowledge et al. for Declaratory Ruling Stating that the Sale of Non-Aggregate Call Records by Telecommunications Providers Without Customers' Consent Violates Section 222 of the Communications Act*, Comments of CTIA, WC Docket No. 13-306 (Jan. 17, 2014) ("*CTIA Comments on PK Petition*").

changed in the intervening thirty months—including the reclassification of broadband service as a telecommunications service, which is irrelevant to this question—that would compel otherwise.

Any rules the Commission adopts must exclude uses and disclosures of de-identified CPNI—*i.e.*, CPNI that is not reasonably linkable to a particular customer. As discussed above, Section 222 encompasses the use and disclosure of only three kinds of customer information: (i) "individually identifiable" CPNI; (ii) "aggregate customer information"; and (iii) "subscriber list information."[88] Congress underscored the importance of information that is specifically linkable to a customer by using the phrase "individually identifiable" as a compound modifier of CPNI in Section 222(c)(1)—the provision that governs use and disclosure of CPNI—even though it did not use that modifier in other provisions in Section 222. Moreover, this distinction makes sense: individually identifiable CPNI "includes information that is extremely personal to customers . . . such as to whom, where and when a customer places a call, as well as the types of service offerings to which the customer subscribes and the extent the service is used."[89] In contrast, there is nothing in the statute or CPNI rules that suggests CPNI stripped of individually identifiable characteristics is, or should be, subject to the same limitations as information possessing such characteristics.

De-identified CPNI, put simply, is not "individually identifiable" CPNI under Section 222(c)(1), and it is not the type of sensitive, personal data for which Congress intended the protections of that section to apply. Rather, if customer information is not individually identifiable and is not aggregate, it falls into a separate category: non-individually identifiable

[88] *See* 47 U.S.C. § 222(c)(1) (governing "individually identifiable" CPNI); *id.* § 222(h)(2) (governing "aggregate customer information"); *id.* § 222(c)(3) (governing "subscriber list information," which means information "(A) identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classification …; and (B) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format").

[89] *CPNI Second Report and Order*, 13 FCC Rcd at 8064 ¶ 2.

CPNI, or de-identified CPNI. ISPs cannot be precluded from using or disclosing such information. If the Commission nonetheless believes it must classify individual, de-identified customer information into a category identified in the statute, the only permissible conclusion is that it becomes "aggregate customer information" because it involves collective data stripped of sensitive information tied to a specific, individual customer.[90]

b. The NPRM Approach to De-Identified Information Unreasonably Departs from the Uniform Approach Taken by Other Agencies and Organizations and Will Cause Public Interest Harms.

The Proposed Rules go beyond the clear limitations Congress expressed in the text and structure of Section 222. But even if the Commission could invoke Section 222(a) to expand the definition of customer information that Section 222 covers, which it cannot, it takes an approach that is at odds with other privacy regimes and is unworkable in practice, rendering its interpretation of Section 222 unreasonable.[91]

Perhaps in tacit acknowledgement that its approach to de-identified data is contrary to the statute, the NPRM purports to ground the concept of "customer proprietary information" in the approach taken by the FTC.[92] Here too, however, the NPRM misses the mark. The FTC—following an extensive process, that lasted two years and involved workshops, careful examination of the online ecosystem, extensive meetings, and over 450 comments from industry

[90] *See CTIA Comments on PK Petition* at 2. This conclusion follows directly from the statutory definition of "aggregate customer information" which includes "data that relates to a group or category of services *or* customers, from which individual customer identities and characteristics have been removed." 47 U.S.C. § 222(h)(2) (emphasis added). The use of the disjunctive means that data do not *have* to be related to a group of customers to qualify as aggregate customer information, so long as the data are de-identified.

[91] 5 U.S.C. § 706(2)(A); *see also, e.g., Motor Vehicle Mgfs Ass'n of the U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 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).

[92] *See NPRM*, 31 FCC Rcd at 2553-56 ¶¶ 154-162.

and consumer groups[93]—published its report on privacy, setting forth a comprehensive, cross-industry framework for consumer protection. At its core, the *FTC Report* distinguishes between sensitive and non-sensitive information—the former requiring heightened protections (a requirement that is common across privacy regimes and is discussed at greater length below).[94] But the *FTC Report* also excludes from its framework *entirely* information that is not *reasonably linkable* to a particular individual or to something specifically associated with an individual.[95] That is so, because the disclosure of information that is not reasonably linkable involves diminished privacy risks. The FTC considers data (whether individual or aggregate) *not* to be *reasonably linkable* if: (1) the data are de-identified, (2) the company holding the data publicly commits not to re-identify them, and (3) the company requires any downstream users to keep the data in de-identified form.[96]

Although the NPRM claims to rely on the FTC's test for de-identified data, it fails to apply the test appropriately. First, the NPRM proposes to apply the FTC's test not to "individually identifiable" CPNI, but instead to "aggregate customer [proprietary] information."[97] For the reasons explained above, however, the Commission lacks authority to

---

[93] *See FTC Report* at i-iii; ; *see also In re Protecting the Privacy of Broadband and Other Telecommunications Services*, Comments of Jon Leibotwitz 1, former FTC Chairman, WC Docket No. 16-106 (May 23, 2015) (describing FTC's experience of bringing over 400 privacy-related enforcement actions, conducing multiple privacy-related rule makings and initiatives, and engaging in multi-year endeavor involving multiple workshops and comments to develop comprehensive privacy regime) ("*Leibowitz Comments*").

[94] *See FTC Report* at 16, 47-48, 58-59. Even the European Union, which is widely recognized as having one of the most rigorous data privacy regimes, distinguishes in the EU General Data Protection Regulation ("EU GDPR") between personal data generally and "special categories of personal data" that require heightened protection. *See* Regulation (EU) 2016/697 of the European Parliament and of the Council Art. 9 (Apr. 27, 2016) ("EU GDPR"), http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

[95] *See FTC Report* at 18.

[96] *Id*. at 22. The Commission's proposal would impose a fourth prong that the FTC *does not* include in its test. Specifically, the Commission would hold ISPs strictly liable when third parties with which ISPs contract re-identify de-identified data. This is an impossible standard for ISPs to meet.

[97] *See NPRM*, 31 FCC Rcd at 2553-54 ¶¶ 154, 156.

expand the scope of data covered under Section 222. Second, even if the Commission did have such authority, which it does not, it appears to have misapprehended how data de-identification works and what "aggregate" information is. For instance, the Commission proposes to "allow [ISPs] to use, disclose, and permit access to aggregate customer [proprietary information] if the provider" applies to such aggregate data the FTC's de-identification test, described above, and the provider monitors any third parties with which it shares such data.[98] It also proposes to put on providers the burden of proving that individual customer identities and characteristics have been removed from aggregate customer proprietary information.[99] But Section 222 preserves ISPs' ability to use aggregate data that has been stripped of personally identifying information without having to meet this new test established by the Commission. Aggregate data by definition is "collective data" that relates to a "group or category of services or customers" and that already has been stripped of identifiers.[100]

Moreover, far from being "consistent with well-developed concepts of what constitutes personally identifiable information in the modern world,"[101] as the Commission asserts, the Commission's proposed definition of PII for the broadband ecosystem is both unique and at odds with the definition used not just by the FTC, but also by other federal agencies, some of which handle particularly sensitive data. Specifically, these other agencies have cabined their definitions by focusing only on sensitive data, by applying a "reasonableness" standard to de-identification, or by requiring a case-by-case assessment of actual privacy risk.

---

[98] *NPRM*, 31 FCC Rcd at 2553-54 ¶ 154; *see also id.* at 2603, 2606-07, App. A §§ 64.7000(a), 64.7002(g).

[99] *Id.* at 2553-54 ¶ 154; *see also id.* at 2603, 2606-07, App. A §§ 64.7000(a), 64.7002(g).

[100] 47 U.S.C. § 222(h)(2). Chairman Leibowitz has described the Commission's application of the FTC approach to de-identified data "contextually inaccurate." *See Leibowitz Comments* at 6-7.

[101] *NPRM*, 31 FCC Rcd at 2519 ¶ 57.

Multiple other U.S. privacy laws and regulations exclude de-identified information from the definitions of "personal information" and "personally identifiable information." These include laws that protect particularly sensitive information, such as health information and student data. For instance, the HIPAA Privacy Rule does not impose any restrictions on the use and disclosure of de-identified health information.[102] Similarly, the Federal Educational Rights and Privacy Act Rule also allows the disclosure of de-identified student information without consent,[103] and other Department of Education regulations define "personally identifiable information" as information that would allow a "reasonable person . . . who does not have knowledge of the relevant circumstances to identify the student with reasonable certainty."[104]

The Commission's purported reliance on the National Institute of Standards and Technology ("NIST") also is misplaced.[105] NIST's work in this area actually supports CTIA's proposal that the Commission adopt a "reasonableness" standard, and is more consistent with the framework articulated in the *FTC Report*, than with the NPRM's approach. In its *Guide to Protecting the Confidentiality of Personally Identifiable Information*, NIST defines "de-identified information" as information that has "had enough PII removed or *obscured* . . . such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual."[106] NIST assigns "de-identified information" a confidentiality impact level of "low" where (1) the re-identification

---

[102] *See, e.g.*, Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936; 45 C.F.R. §§ 164.502(d)(2), 164.514(a) and (b).

[103] 34 C.F.R. § 99.31(b)(1) (allowing the disclosure of student information without consent as long as the school has made a "reasonable determination" a student's identity will not be made personally identifiable by the disclosure).

[104] 34 C.F.R. 99.3(f).

[105] *See NPRM*, 31 FCC Rcd at 2520 ¶ 60.

[106] Erika McCallister, Tim Grance, & Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* 4-4 (NIST, Special Publication 800-122 April 2010), http://www.nist.gov/customcf/get_pdf.cfm?pub_id=904990.

algorithm, code, or pseudonym is maintained in a separate system, with appropriate controls in place to prevent unauthorized access; and (2) the data elements are not linkable, via public records or other reasonably available external records, in order to re-identify the data.[107] In other words, although NIST includes data that are "linked or linkable" to an individual in its definition of PII, it finds "de-identified information" to be "linkable" to an individual only when the key is maintained in the same system as the re-identification algorithm, code, or pseudonym; or that information can be linked using an auxiliary dataset.[108] While the Commission appears to require virtually foolproof de-identification, NIST and the FTC both have recognized that the appropriate way to mitigate the risk of re-identification is not to restrict usage of de-identified information, but to encourage entities to enter into data use agreements with downstream users, to ensure that appropriate controls are in place.[109]

Compounding the problem with the NPRM's definition of PII is the proposal to deem information "linked or linkable" to an individual "if it can be used on its own, in context, or in combination to identify an individual or to logically associate with other information about a specific individual."[110] This proposal ignores how ISPs may routinely handle information that is theoretically "linkable" to individuals but is maintained in a "non-linkable" manner (*e.g.*, as coded or hashed information), while simultaneously maintaining the key in an entirely secure manner.

---

[107] *Id.* at 4-5.

[108] *Id.*

[109] *Id.* ("Although the original dataset contained distinguishable identities for each person, the de-identified and aggregated dataset would not contain linked *or readily identifiable* data for any individual."); *accord FTC Report* at 21 ("The [de-identification] standard is not an absolute one; rather, companies must take reasonable steps to ensure that data is de-identified).

[110] *NPRM*, 31 FCC Rcd at 2520 ¶ 61.

The NPRM thus might prevent companies from engaging in those routine uses of information for a variety of internal purposes—uses that pose no privacy risks to individuals but that may not fall within the narrow category of activities for which consent may be inferred under the Proposed Rules.[111] Such internal uses are generally excluded from privacy regulation, including under the Gramm-Leach-Bliley Act, which regulates uses and disclosures of nonpublic financial information by financial institutions,[112] and under the EU GDPR.[113] The Commission should follow suit, and exclude from its Proposed Rules the use of such information for legitimate internal business purposes.[114]

The Commission fails even to acknowledge, let alone draw from, the thorough research and analysis that the FTC, NIST, and others have done in the area of data de-identification. At the very least, the Commission should engage in further inquiry to examine the actual risks and benefits associated with uses and disclosures of de-identified data before adopting this proposal. Otherwise, the Proposed Rules would eliminate any incentive that companies may have to de-identify data, a methodology that not only benefits consumers and society, but also is widely touted as a data security measure. Specifically, sharing de-identified data can benefit the public interest in a number of significant ways, by enhancing data providers' abilities, among other things, to (1) monitor and contain the spread of infectious diseases; (2) improve medical

[111] *See NPRM*, 31 FCC Rcd at 2606 App. A § 64.7002(a).

[112] *See* 15 U.S.C. § 6802 (restricting financial institutions' disclosures of nonpublic information to unaffiliated third parties without opportunity for opt out, and further restricting unaffiliated third parties' disclosure to any other person); 16 C.F.R. § 313.11(a)(1)(iii) (allowing use and disclosure of information received "in the ordinary course of business to carry out [an exempt] activity").

[113] *See* EU GDPR ¶¶ 47-50.

[114] *See, e.g., Ass'n of Private Sector Colleges & Univs. v. Duncan*, 681 F.3d 427, 448 (D.C. Cir. 2012) (finding that agency's failure, "without some better explanation," to adopt safe harbor for practices that presented no risks in the record was arbitrary and capricious, for want of reasoned decision making). This subject is further addressed in Part V.C, where CTIA discusses a preferable approach to rules implementing Section 222(d).

research; (3) improve traffic flow and transportation infrastructure; (4) analyze disaster recovery efforts; (5) monitor socio-economic conditions; (6) allocate police resources; and (7) improve the dissemination of useful information to consumers in a manner that increases competition and innovation and reduces prices.[115]

In short, the Proposed Rules are unreasonable, because they restrict providers' use of de-identified data and aggregate data. As recognized by the FTC, NIST, the EU, and Congress (in multiple privacy regimes), the use of de-identified and aggregate data poses minimal privacy risk, while yielding substantial benefits. Instead, the Commission should allow providers to use both "aggregate customer information," as that information is defined in Section 222(h)(2), and de-identified CPNI, provided that they have used commercially reasonable techniques to aggregate or de-identify the data. Specifically, the Commission should recognize that customer information is no longer "individually identifiable" when there is no reasonable basis to believe—given the technical and administrative safeguards in place—that the information could be used to identify an individual in the context in which the information will be used.[116]

---

[115] *See FTC Report* at 20-21; Omer Tene and Jules Polonetsky, *Privacy in the Age of Big Data*, 64 Stan. L. Rev. Online 63 (2012) (discussing manifold public interest benefits from big data analytics and arguing that sophisticated re-identification should underscore, rather than undermine, importance of de-identification); Ann Cavoukian & Khaled El Emam, *Dispelling the Myths Surrounding De-Identification* (2011), https://www.ipc.on.ca/images/Resources/anonymization.pdf; *see also In re Petition of Public Knowledge et al. for Declaratory Ruling Stating that the Sale of Non-Aggregate Call Records by Telecommunications Providers Without Customers' Consent Violates Section 222 of the Communications Act*, T-Mobile Reply Comment at 3-7, WC Docket No. 13-306 (Mar. 4, 2014) (addressing studies and concluding that "the risk of privacy harm from re-identification is significantly lower than many risks we take without concern" (internal quotation marks omitted)); *id.* at 7-8 (recounting various uses of de-identified data in the public interest).

[116] *See In re Wireline Competition Bureau Seeks Comment on Petition of Public Knowledge for Declaratory Ruling that Section 222 of the Communications Act Prohibits Telecommunications Providers from Selling Non-Aggregate Call Records Without Customers' Consent*, Comments of the Future of Privacy Forum at 2, WC Docket No. 13-306 (Jan. 17, 2014).

3. CPNI Is a Narrow and Specifically Defined Category Under Section 222(h) and May Not Be Interpreted to Include Other Information.

As stated above, Section 222(h) limits CPNI to the following information: "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship," as well as "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier," but excluding information published in a public directory.[117]

Because Congress designed Section 222 to apply to telephone voice services and to address the unique sensitivity of information obtained by carriers by virtue of providing voice services, the information listed in Section 222(h) cannot be translated to the broadband context. Furthermore, Section 222(h) captures only information that is made available to carriers "solely by virtue of the carrier-customer relationship." As stated above, unlike in the voice services market, where historically only the carrier and the subscriber had access to call detail records and other information about the subscriber's use of the network, in the Internet ecosystem multiple entities have access to subscriber information. At a minimum, therefore, the following elements must be excluded from the Commission's definition of CPNI in the broadband context: (1) Geolocation information other than precise geolocation information to which other companies have no access; (2) Home router MAC addresses; (3) Traffic statistics; (4) Port Information; (5) IP addresses; (6) Domain name information; (7) Application headers; (8) Application usage; and (9) consumer premise equipment ("CPE") information.

[117] 47 U.S.C. § 222(h)(1).

The NPRM requests comment on whether the Commission should "consider adopting a broader definition of CPNI and include additional categories of customer information into CPNI" and whether a "broader definition of CPNI [is] the best way to provide consumers with robust privacy protections."[118] For all of the reasons identified above, the Commission cannot bootstrap what it primarily proposes to define as "customer proprietary information" under section 222(a) into an expanded definition of "CPNI" under section 222(h). In short, that move, too, is unambiguously foreclosed by the structure of Section 222 and by Congress's decision not to use "personal information" or "PII" anywhere in Section 222—and likewise would amount to an unreasonable interpretation, disconnected from any of the animating purposes underlying Section 222. The Commission has previously recognized as much, describing that it is "clear that the definition of CPNI does not include a customer's name, address, and telephone number," and so interpreting CPNI would cause "anomalous result[s]" that are "clearly not intended."[119]

4. Any Rules Under Section 222 Cannot Prohibit Data Practices and Instead Must Allow ISPs to Obtain Customer Approval to Use, Disclose, or Permit Access to CPNI.

Although not part of its primary proposal, the NPRM also identifies certain ISP practices that the Commission suggests could be "prohibited."[120] Specifically, the Commission (1) "propose[s] to prohibit [ISPs] from making service offers contingent on a customer surrendering his or her privacy rights";[121] (2) requests "comment on whether business practices that offer customers financial inducements, such as lower monthly rates, for their consent to use and share

[118] *NPR*, 31 FCC Rcd at 2518 ¶ 54.

[119] *See In re Implementation of the Telecommunications Act of 1996*, Order, 13 FCC Rcd 12,390, 12,395-96 ¶¶ 8-9 (1998), *adopted by 1999 CPNI Order*, 14 FCC Rcd 14,409.

[120] *NPRM*, 31 FCC Rcd at 2581-84 ¶¶ 256-263.

[121] *Id.* at 2582 ¶ 258.

their confidential information, are permitted";[122] (3) requests comment on "whether the use of DPI for purposes other than providing broadband services, and reasonable management thereof, should be prohibited";[123] and (4) requests comment on "whether the use of persistent tracking technologies should be prohibited."[124]

The Commission lacks authority to prohibit any of these practices. The opening clause of Section 222(c)(1) sets forth that "[e]xcept as required by law *or with the approval of the customer*," a telecommunications carrier may not engage in certain practices involving CPNI.[125] Each of the four proposed prohibitions would be inconsistent with this savings clause.

The first two practices that the NPRM considers prohibiting are methods of obtaining customer approval—*i.e.*, either offering service on a take-it-or-leave-it basis, or offering incentives in favor of approval. The Commission seeks comment on prohibiting these practices on the theory that a customer's "approval" is not "meaningful," either where the ISP has offered a take-it-or-leave-it service or is tipping the scales in favor of approval through incentives.[126] This assumption, in turn, is based on further false assumptions regarding the purported lack of competition among ISPs, and the purported high switching costs of changing providers—neither of which is accurate.[127] Moreover, the potential prohibitions would be at odds with standard industry practice (as the Commission itself appears to recognize[128]) and without clear limits.

---

[122] *NPRM*, 31 FCC Rcd at 2582 ¶ 259.

[123] *Id.* at 2584 ¶ 264.

[124] *Id.* at 2585 ¶ 268.

[125] 47 U.S.C. § 222(c)(1) (emphasis added).

[126] *NPRM*, 31 FCC Rcd at 2582 ¶¶ 258-259.

[127] *See infra* notes 351-363 and accompanying text.

[128] *NPRM*, 31 FCC Rcd at 2582-83 ¶ 260.

Equally problematic, such a prohibition would be contrary to settled principles of contract law. Courts long have held that form contracts are enforceable, notwithstanding a lack of negotiation between the parties, as long as they are not unconscionable.[129] Thus, because Congress allowed carriers to use, disclose, or permit access to CPNI with customers' "approval," it would be unreasonable to conclude that Congress meant to exclude certain kinds of "approval" (*i.e.,* a decision to enter into a form contract that allowed the carrier to use, disclose, or permit access to CPNI) that long have been held valid under contract law.[130] Section 222 therefore must be interpreted to reflect this general contract law rule of "unconscionability." In contract law terms, the Commission is *sub silentio* proposing to find that both take-it-or-leave-it offers and offers with incentives are "unconscionable," without doing any of the requisite work to support such a finding. Unconscionability, however, requires a finding of both procedural *and substantive* unfairness—the latter being reserved for contract terms that are so "outrageously unfair as to shock the judicial conscience."[131] Even the Commission does not suggest that take-it-or-leave-it offers shock the conscience because they include specific privacy provisions, nor is it at all apparent how the Commission could cabin this finding with a coherent limiting principle.

---

[129] *Lake Roosevelt Vacations Inc. v. Norton*, No. 02-5203, 2002 WL 31898183, at *1 (D.C. Cir. Dec. 23, 2002) (per curiam) (noting that contracts of adhesion are enforceable unless unconscionable); *see also Dillard v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, 961 F.2d 1148, 1154 (5th Cir. 1992) ("Adhesion contracts are not automatically void. Instead, the party seeking to avoid the contract generally must show that it is unconscionable."); *Int'l Harvester Credit Corp. v. Leaders*, 818 F.2d 655, 659 (8th Cir. 1987) ("We conclude that the agreement, although a contract of adhesion, was not unconscionable . . . .").

[130] *See, e.g., United States v. Texas*, 507 U.S. 529, 534 (1993) ("In order to abrogate a common-law principle, [a] statute must 'speak directly' to the question addressed by the common law." (citations omitted)); *Astoria Fed. Sav. & Loan Ass'n v. Solimino*, 501 U.S. 104, 108 (1991) ("Congress is understood to legislate against a background of common-law . . . principles. Thus, where a common-law principle is well established . . . the courts may take it as a given that Congress has legislated with an expectation that the principle will apply except when a statutory purpose to the contrary is evident." (citations and internal quotation marks omitted)); *Heiser v. Islamic Republic of Iran*, 735 F.3d 934, 938 (D.C. Cir. 2013) ("[S]tatutes should be interpreted consistently with the common law. Congress can abrogate [a] traditional common-law principle[] . . ., but to do so it must speak directly to the question addressed by the common law." (citations and internal quotation marks omitted)).

[131] *Song fi, Inc. v. Google Inc.*, 72 F. Supp. 3d 53, 62 (D.D.C. 2014); *see also Pappas v. Kerzner Int'l Bahamas Ltd.*, 585 F. App'x 962, 966 n.4 (11th Cir. 2014); *Harrington v. Atl. Sounding Co.*, 602 F.3d 113, 125 (2d Cir. 2010).

The third and fourth practices that the NPRM suggests prohibiting are not methods of obtaining consent, but instead involve the use of particular technologies: DPI and persistent tracking. Like the prohibitions discussed above, outright prohibitions on these practices also would fail as a statutory matter. First, DPI does not involve the "use, disclos[ure], or permit[ting] access to [CPNI]";[132] it is a technology used to analyze online activity, which Section 222 does not in any way restrict. Second, even if Section 222 reached these practices, prohibiting ISPs from using DPI and persistent tracking technology, *even if* ISPs obtain customer approval, would read the opening clause of Section 221(c)(1) out of the statute entirely. To give this clause effect, a carrier that obtains "approval of the customer" to engage in the practice must be able to do so, because the plain meaning of "approval" is "permission to do something."[133]

Section 705 does not save these prohibitions.[134] As will be discussed at greater length below, Section 705 does not extend to ISPs' uses of data in the ordinary course of business,[135] and, in any event, the Commission cannot interpret Section 705 to prohibit that which Section 222 unambiguously permits.[136]

5. Any Rules Under Section 222 Must Permit ISPs to Use, Disclose, or Permit Access to Information They Receive or Obtain Other Than by Providing Service.

The Commission also seeks comment on whether to require ISPs to obtain some form of approval before combining data acquired from third parties with information obtained by virtue

---

[132] *See* 47 U.S.C. § 222(c)(1).

[133] *Approval*, Merriam-Webster Dictionary, http://www.merriam-webster.com/dictionary/approval (last visited May 6, 2016).

[134] *See, e.g.*, *See NPRM*, 31 FCC Rcd at 2585 ¶ 267.

[135] *See infra* Part I.D.2.

[136] *Cf. 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.").

of providing broadband service.[137] The Commission is wholly without authority to regulate uses of information that ISPs acquire from third parties. The statute provides that a telecommunications carrier is restricted from using, disclosing, or permitting access to CPNI that it obtains "*by virtue* of its provision of a telecommunications service."[138] The plain meaning of "by virtue of" is "on account of" or "by reason of."[139] Information that an ISP obtains from a third party is not obtained on account of its provision of service, and therefore the Commission cannot prevent an ISP from using, disclosing, or permitting access to such information. Further, CPNI is specifically defined to include information "that is made available to the carrier by the customer *solely by virtue of the carrier-customer relationship*."[140] Data acquired from third parties falls wholly outside of this definition. Indeed, information about a customer acquired outside of the carrier-customer relationship is not "*proprietary*" information at all.[141] The NPRM even tacitly admits as much; although CTIA does not otherwise endorse this definition, the NPRM defines "customer proprietary information" to include PII "the [ISP] acquires *in connection with its provision of* [*service*]."[142] This definition, if adopted, excludes information that is acquired for other purposes and in connection with other services.

---

[137] *NPRM*, 31 FCC Rcd at 2549 ¶ 138.

[138] 47 U.S.C. § 222(c)(1) (added).

[139] *By Virtue Of*, Dictionary.com, http://www.dictionary.com/browse/by--virtue--of?s=t (last visited May 6, 2016); *By Virtue Of*, Thesaurus.com, http://www.thesaurus.com/browse/by%20virtue%20of%20?s=t (last visited May 24, 2016).

[140] 47 U.S.C. § 222(h)(1)(A) (emphasis added).

[141] *Proprietary*, Merriam-Webster Dictionary, http://www.merriam-webster.com/dictionary/proprietary (last visited May 6, 2016) ("proprietary" means held as property; used, made, or marketed by one having the exclusive legal right). Because the Commission cannot regulate ISPs' use of information acquired from third parties, the Proposed Rules both are not appropriately tailored from a First Amendment perspective and are arbitrary and capricious for APA purposes. Moreover, from achieving their intended purpose, the Proposed Rules will increase the leverage of data brokers and other entities in the Internet ecosystem.

[142] *NPRM*, 31 FCC Rcd at 2519 ¶ 57 (emphasis added).

6. The Commission Cannot and Should Not Adopt Prohibitions or Restrictions on ISPs' Use of Arbitration.

a. Arbitration Benefits Wireless Consumers

Even if the Commission had the legal authority to prohibit arbitration (which, as we explain below, it does not), it should not do so, because arbitration provides wireless customers with significant benefits.[143]

1) Arbitration provides a fair and effective remedy for the many injured consumers for whom the judicial system is not a realistic option.

Arbitration is more accessible to consumers than courts; it is faster, simpler, more flexible, and less costly. As the Supreme Court has observed, arbitration is "usually cheaper and faster than litigation; it can have simpler procedural and evidentiary rules; it normally minimizes hostility and is less disruptive of ongoing and future business dealings among the parties; [and] it is often more flexible in regard to scheduling of times and places of hearings and discovery devices."[144]

The reality of arbitration today supports that conclusion. Studies have long found, for example, that, in practice, a large percentage of individuals who bring claims in arbitration pay

[143] It appears that the Commission proposes to prohibit the use of arbitration clauses only for resolving complaints with respect to the collection, use, and disclosure of customer information pursuant to Section 222 of the Communications Act. *See NPRM*, 31 FCC Rcd at 2586-87 ¶ 273. To the extent the Commission proposes any broader prohibition on the use of arbitration clauses, such a prohibition would cause additional difficulties for wireless customers. Most wrongs suffered by wireless consumers are relatively small and individualized, involving excess charges on a bill, a defective piece of equipment, or the like. These claims are simply too small to justify paying a lawyer to handle the matter and, in any event, most consumers do not have the resources to do so—and a lawyer is needed to navigate the complicated procedures that apply in court. And claims of this sort cannot be brought as class actions because they involve facts specific to an individual consumer's situation. Thus, as Justice Breyer has recognized, without arbitration, "the typical consumer who has only a small damages claim" would be left "without any remedy but a court remedy, *the costs and delays of which could eat up the value of an eventual small recovery*." *Allied-Bruce Terminix Cos. v. Dobson*, 513 U.S. 265, 281 (1995) (emphasis added). For this large category of consumer claims, arbitration provides the only realistic option for obtaining a fair resolution of the dispute.

[144] *Allied-Bruce*, 513 U.S. at 280 (quotation marks omitted).

exactly *nothing* in fees to pursue their claim.[145] The practical costs of presenting a claim in arbitration, moreover, are typically far lower than litigating in court. Arbitration does not require a personal appearance to secure a judgment; claims can be adjudicated on the papers or on the basis of a telephone conference.[146] Consumers need not wait in line at night court or miss work, only to be forced to return another day if the court is unable to get through its docket. In most instances, arbitration claimants can initiate arbitrations online, submit the relevant documents and a common sense statement of why they are entitled to relief, and proceed without a lawyer.[147]

Arbitration also provides a fair forum for consumers. The American Arbitration Association, for example, has adopted a Consumer Due Process Protocol, to which arbitration provisions must adhere: "The AAA will accept a case for administration only after the AAA reviews the parties' arbitration agreement and if the AAA determines that the agreement substantially and materially complies with the due process standards of the Rules and the Consumer Due Process Protocol."[148] Similarly, JAMS—another leading arbitration provider—"will administer arbitrations pursuant to mandatory pre-dispute arbitration clauses between

---

[145] Elizabeth Hill, *Due Process at Low Cost: An Empirical Study of Employment Arbitration Under the Auspices of the American Arbitration Association*, 18 Ohio St. J. on Disp. Resol. 777, 802 (2003) (lower-income employees "paid no forum fees" in 61% of the cases studied; employees also paid no attorneys' fees in 32% of the cases).

[146] AAA, *Consumer-Related Disputes Supplementary Procedures* 6, Mar. 1, 2013, https://www.adr.org/cs/idcplg?IdcService=GET_FILE&dDocName=ADRSTAGE2009997&RevisionSelectionMethod=LatestReleased.

[147] Jason Scott Johnston & Todd Zywicki, *The Consumer Financial Protection Bureau's Arbitration Study: A Summary and Critique* 25-26 (Mercatus Ctr., George Mason Univ., Working Paper, Aug. 2015) (observing that "self-represented plaintiffs were seven times *more* likely than represented plaintiffs to get an AAA arbitrator's decision in their favor" and commenting that it appears that in arbitration, "hiring an attorney offers little value to a consumer and is often unnecessary" (emphasis added)).

[148] AAA, *Consumer Arbitration Fact Sheet*, http://info.adr.org/consumer-arbitration/.

companies and consumers only if the contract arbitration clause and specified applicable rules comply with [JAMS's] minimum standards of fairness."[149]

With these protections in place, consumers prevail in arbitration at least as frequently as—and often more frequently than—they do in court. A recent study by scholars Christopher Drahozal and Samantha Zyontz of claims filed with the American Arbitration Association found that consumers win relief 53.3% of the time.[150] This compares favorably with the success rate of plaintiffs in court, who prevail roughly 50% of the time.[151]

Indeed, companies are increasingly adopting consumer-friendly arbitration agreements. The wireless industry, in particular, is noted for leading this trend and making arbitration easy for, and accessible to, all consumers. Wireless companies' arbitration provisions contain numerous consumer-friendly features:

- Many wireless providers (including Verizon Wireless,[152] AT&T,[153] T-Mobile,[154] Sprint,[155] Boost Mobile,[156] MetroPCS,[157] Straight Talk,[158] U.S. Cellular,[159] and

[149] JAMS, *Consumer Minimum Standards* (footnote omitted), http://www.jamsadr.com/rules-consumer-minimum-standards/.

[150] Christopher R. Drahozal & Samantha Zyontz, *An Empirical Study of AAA Consumer Arbitrations*, 25 Ohio St. J. on Disp. Resol. 843, 896-904 (2010).

[151] *See, e.g.*, 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).

[152] *See* Verizon, *Customer Agreement*, http://www.verizonwireless.com/b2c/support/customer-agreement.

[153] *See* AT&T, *Wireless Customer Agreement*, https://www.att.com/legal/terms.wirelessCustomerAgreement.html#disputeResolutionByBindingArb.

[154] *See* T-Mobile, *Terms & Conditions* (Mar. 17, 2016) http://www.t-mobile.com/Templates/Popup.aspx?PAsset=Ftr_Ftr_TermsAndConditions&print=true.

[155] *See* Sprint, *Terms & Conditions* (July 1, 2013), https://shop2.sprint.com/en/legal/os_general_terms_conditions_popup.shtml.

[156] *See* Boost Mobile, *General Terms & Conditions* (July 1, 2013), https://www.boostmobile.com/#!/about/legal/terms-conditions/general-terms-conditions/.

[157] *See* MetroPCS, *Terms and Conditions of Service*, https://www.metropcs.com/terms-conditions/terms-conditions-service.html.

[158] *See* Straight Talk Wireless, *Terms and Conditions*, https://www.straighttalk.com/wps/portal/home/h/legal/terms-and-conditions/.

Virgin Mobile[160]) agree to make arbitration cost-free for customers by paying all administrative and arbitrator fees and reimbursing the customer for any filing fee. Given their obligation to pay all arbitration fees in every case (which can be thousands of dollars or more), wireless providers have an incentive to settle most nonfrivolous customer disputes before arbitration ever begins. Indeed, Verizon offers customers a free mediation program that helps resolve claims more quickly and avoid the need for any arbitration.

- Verizon, AT&T, and Straight Talk's arbitration agreements feature incentive payment systems, which provide that if a customer does not receive a settlement offer and then prevails in arbitration, or rejects a settlement offer and then wins more than that amount in arbitration, the company will pay the customer a guaranteed minimum award ($5,000 for Verizon and Straight Talk and $10,000 for AT&T) and their attorneys' fees and expenses (sometimes including expert witness or discovery costs). AT&T and Straight Talk agree to pay *double* the amount of the customer's attorneys' fees. Meanwhile, T-Mobile, MetroPCS, and U.S. Cellular agree to pay attorneys' fees to *any* customer who prevails in arbitration, irrespective of whether a settlement offer was made. The companies provide for this cost-shifting even though *the underlying law often does not provide for such cost-shifting and cost-shifting therefore would not be available in court*.

  Indeed, because AT&T's arbitration system provides for incentive payments and cost-shifting, the Supreme Court noted in *AT&T Mobility LLC v. Concepcion* that consumers were likely better off under that arbitration system than they were as members of a class action that "could take months, if not years, and . . . may merely yield an opportunity to submit a claim for recovery of a small percentage of a few dollars."[161]

- Verizon, AT&T, and Straight Talk give customers the choice of whether to resolve a dispute via written submissions, telephone hearings, or in-person proceedings, allowing customers to decide what method of decision works best for their schedules. And all of the companies named above specify that the venue for arbitration is the county in which the customer resides, in order to make it easier for the customer to access the arbitral forum.

---

[159] *See* U.S. Cellular, *Terms and Conditions of Agreement*, https://www.uscellular.com/site/legal/customer-service-agreement.html.

[160] *See* Virgin Mobile, *Terms & Conditions* (Aug. 1, 2013), https://www.virginmobileusa.com/#!/legal/general-terms-and-conditions-no-annual-contract/.

[161] 563 U.S. 333, 352 (2011) (quotation marks omitted).

2) Class-action lawsuits provide little benefit to consumers.

The principal attack on arbitration—largely driven by the plaintiffs' class action bar—stems from the fact that virtually all arbitration agreements require that arbitration proceed on an individual basis and bar class procedures in arbitration and in court. But as the Supreme Court recognized, proceeding on a class basis "sacrifices the principal advantage of arbitration — its informality — and makes the process slower, more costly, and more likely to generate procedural morass than final judgment."[162]

Proponents of class actions nonetheless defend the class mechanism, asserting that the use of that procedure allows the vindication of small claims that (according to those advocates) would be too expensive for plaintiffs to arbitrate individually.

That argument ignores the reality of class actions, which generally deliver little relief to consumers. A study published last year by the Consumer Financial Protection Bureau ("CFPB"), demonstrates the inefficacy of class actions.[163] Among other things, the study revealed that 87% of class actions brought in federal court do not lead to final approval of a federal class settlement; instead, most were voluntarily dismissed by or settled with the named plaintiff only.[164] And even in the 13% of federal court class actions that do yield a classwide settlement, an average of only 4% of class members even bother to file a claim for relief[165]—demonstrating that only a tiny percentage of the members of potential classes recover from class actions.

The principal beneficiaries of class action lawsuits are plaintiff's and defense lawyers, who are far more likely to be enriched by such cases. The CFPB study showed that the average

[162] *Id.* at 348.

[163] Consumer Fin. Protection Bureau, *Arbitration Study: Report to Congress* § 6, at 48-49 (Mar. 1, 2015) ("*CFPB Study*"), http://files.consumerfinance.gov/f/201503_cfpb_arbitration-study-report-to-congress-2015.pdf.

[164] *Id.* § 6, at 37.

[165] *Id.* § 8, at 30.

fee paid to plaintiffs' lawyers in class actions—as a percentage of the announced settlement (not the smaller amount actually distributed to class members)—was 41%, with a median of 46%. The total fees awarded to plaintiffs' lawyers in the cases studied by the CFPB added up to $424 million for 419 cases,[166] which works out to an average of *more than $1 million per case*. It is no wonder that plaintiffs' lawyers are the most vocal advocates for eliminating fair, efficient arbitration and replacing it with more class actions. Wireless customers, as the Supreme Court noted in *Concepcion*, are likely better off in arbitration, given that wireless providers' arbitration systems are set up to give them relief faster and more complete than what they would get in a class action.

b. In Any Event, The Commission Lacks Authority To Prohibit Or Regulate Arbitration.

Any attempt by the Commission to prohibit the use of arbitration in wireless service agreements would not only be bad policy, but also would be contrary to law.

1) Under the Federal Arbitration Act ("FAA"), arbitration provisions are valid and enforceable, unless another federal statute evinces a "contrary congressional command" that overrides the FAA.

The Federal Arbitration Act ("FAA") embodies a "liberal federal policy favoring arbitration agreements, notwithstanding any state substantive or procedural policies to the contrary."[167] The FAA provides that arbitration provisions are "valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract."[168]

---

[166] *Id.* § 8, at 33.

[167] *Moses H. Cone Mem. Hosp. v. Mercury Constr. Corp.*, 460 U.S. 1, 24 (1983).

[168] 9 U.S.C. § 2.

The FAA's mandate applies to all arbitration agreements and to all categories of claims unless Congress overrides the FAA in another federal statute.[169] Congressional intent to circumscribe the FAA can only be demonstrated through a "contrary congressional command" that is "discernible from the text, history, or purposes of the statute."[170] And this congressional command must be explicit: the Supreme Court reiterated that when a federal statute "is silent on whether claims under the Act can proceed in an arbitrable forum, the FAA requires the arbitration agreement to be enforced according to its terms."[171] Unsurprisingly, given the stringency of this test, the Supreme Court *has never held that any federal statute overrides the FAA.*

2) The Communications Act of 1934 does not override the FAA.

The Communications Act of 1934, which presumably would be the statutory authority on which the Commission would rely for any Commission rule purporting to prohibit or limit arbitration, does not override the FAA. The Communications Act's text contains *no* reference to arbitration provisions in agreements for telecommunications services. That fact alone is dispositive: as the Supreme Court explained just a few years ago in *CompuCredit*, when a statute is "silent" on the enforceability of arbitration agreements, that is the end of the matter, and the FAA controls.

Nor does the legislative history of the Communications Act—a factor that the Court has sometimes said is relevant—evince a "contrary congressional command"[172] to override the FAA. Indeed, it does not appear that Congress ever considered the question of arbitration provisions in

[169] *Shearson/Am. Express, Inc. v. McMahon*, 482 U.S. 220, 226 (1987).

[170] *Id.* at 226-27.

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

[172] *McMahon*, 482 U.S. at 226.

telecommunications service agreements. Thus, even assuming that a statute's legislative history could be sufficient to override the FAA where the statute's text is silent, nothing in the legislative history of the Communications Act suggests an intent to override the FAA.

The Supreme Court has also suggested that an "inherent conflict" between arbitration and a federal statute's "underlying purposes" might be enough to override the FAA.[173] But the Court has never found such an "inherent conflict" between the FAA and another statute, and nothing in the Communications Act conflicts with the FAA.

Congress knows how to grant an administrative agency the authority to override the FAA when Congress wishes to do so: In the Dodd-Frank Act, for example, Congress authorized the Securities and Exchange Commission to issue rules "prohibit[ing], or impos[ing] conditions or limitations on the use of" predispute arbitration agreements in agreements between certain broker-dealers and their clients, and between investment advisers and their clients.[174] Congress used similar language in authorizing the CFPB to conduct a study and report to Congress regarding the use of arbitration agreements in consumer financial products and services, and to issue a rule prohibiting or effectively eliminating arbitration if it "finds that . . . [it] is in the public interest and for the protection of consumers."[175] There is no similar language in the Communications Act. Indeed, the Commission's proposal to regulate arbitration closely resembles the National Labor Relations Board's similarly impermissible attempt to use its unfair labor practice authority to regulate arbitration agreements in the employment context, by prohibiting agreements that provide for individualized resolution of disputes and preclude class

[173] *Id.* at 227.

[174] *See* 15 U.S.C. §§ 78o(o), 80b-5(f).

[175] *See* 12 U.S.C. § 5518(b).

proceedings.[176] The NLRB's ruling was set aside by the Court of Appeals for the Fifth Circuit on the ground that the National Labor Relations Act—which also does not mention arbitration—does not override the FAA.[177] Every other appellate court to address the issue has reached the same conclusion.[178] Any attempt by the Commission to regulate or prohibit arbitration would be invalidated on the same grounds.

Finally, arbitration is entirely consistent with the Communications Act's purpose to "secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies."[179] Arbitration benefits both telecommunications providers and their customers by allowing them to resolve customer disputes more quickly and at lower cost, permitting providers to devote more of their resources to providing higher quality service and greater access to consumers.[180] And as explained below, arbitration also directly benefits consumers themselves, by enabling them to obtain relief on claims they could not feasibly bring in court.

3) Any Commission rule regulating arbitration would not receive Chevron deference and would be invalidated.

Any rule addressing arbitration adopted by the Commission would not receive *Chevron* deference—the deference that courts give to agencies' interpretations of the laws they administer. Although the Commission has authority to administer the Communications Act, it

[176] *See In re D.R. Horton, Inc.*, 357 NLRB No. 184 (Jan. 3, 2012).

[177] *D.R. Horton, Inc. v. NLRB*, 737 F.3d 344, 355-62 (5th Cir. 2013).

[178] *See, e.g.*, *Sutherland v. Ernst & Young LLP*, 726 F.3d 290, 297 n.8 (2d Cir. 2013); *Owen v. Bristol Care, Inc.*, 702 F.3d 1050, 1055 (8th Cir. 2013).

[179] *T-Mobile USA, Inc. v. City of Anacortes*, 572 F.3d 987, 991 (9th Cir. 2009) (quotation marks omitted).

[180] *Cf.* Stephen J. Ware, The Case for Enforcing Adhesive Arbitration Agreements—With Particular Consideration Of Class Actions and Arbitration Fees, 5 J. Am. Arbitration 251, 254-57 (2006) (citing, *inter alia*, Richard Posner, *Economic Analysis of Law* (6th ed. 2003)); Rob Berger, *The CFPB Declares War on Arbitration*, Forbes, Oct. 18, 2015, http://www.forbes.com/sites/robertberger/2015/10/18/the-cfpb-declares-war-on-arbitration.

has no special authority with respect to the *FAA*—which governs the question whether arbitration agreements are enforceable. Courts do not give agencies *Chevron* deference on questions controlled by statutes they do not administer.[181]

Indeed, far from deferring to the Commission's rule, a court would invalidate it. "An agency may not reorder federal statutory rights without congressional authorization,"[182] and because it lacks the necessary "contrary congressional command," the Communications Act does not authorize the Commission to eliminate the rights conferred by the FAA with respect to arbitration agreements. The Commission's rule would be struck down as beyond the agency's statutory authority.

In short, arbitration affords individual consumers genuine opportunities to pursue their disputes or otherwise vindicate their rights, in sharp contrast to the false promise of private class actions. The Commission would be exceeding its authority and doing consumers a disservice by attempting to limit consumers' access to this valuable form of dispute resolution.

D. The Alternative Statutory Bases that the Commission Identifies Fail To Provide Authority for Regulating Broadband Customer Privacy.

To the extent that the NPRM asserts legal authority in support of the Proposed Rules, it is largely devoted to Section 222.[183] The Commission's rulemaking authority for privacy is limited to Section 222, and to Section 631 of the Communications Act for cable providers and Section 338 of the Communications Act for satellite providers. Moreover, unlike Sections 631 and 338,

---

[181] *See, e.g.*, *Metro. Stevedore Co. v. Rambo*, 521 U.S. 121, 137 n.9 (1997).

[182] *POM Wonderful LLC v. Coca-Cola Co.*, 134 S. Ct. 2228, 2241 (2014).

[183] In recent testimony before the Senate Judiciary Committee, Chairman Wheeler explained that the Commission is "asserting these rules under Title II"; that this "*is* a Title II proceeding" and that Section 706 has "a bearing on this, but we're doing this under Section 222." *See* Tom Wheeler, Testimony Before the Subcomm. on Privacy, Technology, and the Law, *Examining the Proposed FCC Privacy Rules* at 54:44 -54:10 (May 11, 2016), http://www.judiciary.senate.gov/meetings/examining-the-proposed-fcc-privacy-rules.

which apply broadly to an open-ended category of "personally identifiable information," Section 222 expressly limits the scope of customer data covered to CPNI.[184] Perhaps recognizing that its authority under Section 222 is somewhat tenuous, however, the NPRM also identifies several other provisions of the Communications Act and Telecommunications Act of 1996 as potential fonts for the Proposed Rules. The Commission cannot and should not engage in a scattershot approach to rulemaking. As the Commission has stated previously, Section 222 is a unique creature of the Telecommunications Act of 1996; attempts to bootstrap the Proposed Rules to other provisions would suggest that the Commission is engaged in a results-oriented approach in this rulemaking, and, in any event, the other potential statutory candidates all suffer from fatal shortcomings.

1. Neither Section 201(b) Nor Section 202 Provides a Basis for Regulating the Privacy Practices of Broadband Providers.

The Commission posits that Sections 201 and 202 of the Communications Act might provide statutory authority for the Proposed Rules.[185] In relevant part, Section 201(b) provides that "[a]ll charges, practices, classifications, and regulations for and *in connection with* [interstate or foreign] communication service [by wire or radio], shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful"; and Section 202 provides in relevant part that "[i]t shall be unlawful for any common carrier to make any unjust or unreasonable discrimination in charges[] [or] practices . . .

[184] 47 U.S.C. § 551(a)(2) (requiring cable providers to protect "personally identifiable information" which "does not include any record of aggregate data which does not identify particular persons"); 47 U.S.C. § 338(i)(2)(A) (same with respect to satellite providers).

[185] *NPRM*, 31 FCC Rcd at 2596 ¶¶ 305-306. Any apparent "congruence" between Section 201 of the Communications Act and Section 5 of the Federal Trade Communications Act is not shared by Section 202 of the Communications Act, which prohibits "discrimination." Nor is it at all clear how ISPs' facially neutral uses and disclosures of customer information—whether CPNI or otherwise—could be regulated as a form of "discrimination" under Section 202.

for or *in connection* with like communication service."[186] Although the Commission generally is entitled to deference regarding its interpretation of "just," "unjust," "reasonable," and "unreasonable," and "practices . . . in connection with" communication services, the Proposed Rules stretch these phrases past the breaking point.

Most important, data privacy and security practices related to non-CPNI customer information are not practices "in connection with" broadband service, and thus cannot be governed under Sections 201(b) and 202. Indeed, in enacting Section 222, Congress defined the appropriate scope of consumer privacy protections under the Act, and the Commission cannot expand that protection through a more general section of the Act. The Commission has recognized as much, previously stating when it adopted CPNI rules that it was "persuaded that Congress established a comprehensive new framework *in Section 222*, which balances principles of privacy and competition in connection with the use and disclosure of CPNI and other customer information."[187] In this new comprehensive framework, Congress set forth protections for CPNI and the other categories of customer information described in Section 222, but declined to set forth protections for a broader set of customer information, including PII. Therefore, it follows that Congress unambiguously intended the Commission's privacy authority to be limited to the categories of information set forth in Section 222.[188]

The Commission recognized this principle in the *Open Internet Order*. In opting not to find jurisdiction over privacy issues in Section 706, the Commission wrote:

> We also note, for example, that this approach obviates the need to determine whether or to what extent section 222 is more specific than section 706 of the 1996 Act in relevant respects, and thus could be seen as exclusively governing

[186] 47 U.S.C. §§ 201(b), 202(a) (emphases added).

[187] *CPNI Second Report and Order*, 13 FCC Rcd at 8073, ¶ 14.

[188] *Hawke*, 211 F.3d at 644-45.

> over the provisions of section 706 of the 1996 Act as to some set of privacy issues.[[189]] The approach we take avoids this potential uncertainty, and we thus need not and do not address this question.[190]

Indeed, until the *TerraCom/YourTel NAL*, the Commission had never before in the 80-year history of Section 201(b) asserted that 201(b) gave it authority to regulate data security.[191] Rather than address these fundamental challenges to its interpretation of Section 201(b), the Commission in the *TerraCom/YourTel NAL* did not provide any statutory analysis regarding Section 201(b) or cite any Commission or judicial precedent for its reading of Section 201(b).[192]

In addition, Section 222 limits the scope of customers' personal information that is "for and in connection with" telecommunications service to CPNI and other categories of information described in Section 222(h). Limiting the definition of CPNI to specific types of information "made available to the carrier by the customer solely by virtue of the carrier-customer relationship" reflected Congress's determination that while carriers may collect other non-CPNI

---

[189] [*Cf. Bloate v. U.S.*, 559 U.S. 196, 208 (2010) ("'[g]eneral language of a statutory provision, although broad enough to include it, will not be held to apply to a matter specifically dealt with in another part of the same enactment'" (citation omitted))].

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

[191] The Commission's failure to find such authority to regulate data security practices under Section 201(b) previously is itself evidence that such authority does not exist. *See Util. Air. Regulatory Grp. v. EPA*, 134 S. Ct., 2427, 2444 (2014) ("When an agency claims to discover in a long-extant statute an unheralded power to regulate 'a significant portion of the American economy,' we typically greet its announcement with a measure of skepticism. We expect Congress to speak clearly if it wishes to assign to an agency decisions of vast 'economic and political significance." (citation omitted)).

[192] The *TerraCom/YourTel NAL* provides a source for only one aspect of its novel interpretations of Section 201(b): its finding that misrepresentations of data security practices in privacy policies violate Section 201(b). *See TerraCom/YourTel NAL*, 29 FCC Rcd at 13,339 ¶ 38 n.83 (citing *In re Joint FCC/FTC Policy Statement for the Advertising of Dial-Around and Other Long-Distance Services to Consumers*, Policy Statement, 15 FCC Rcd 8654, 8654 ¶ 4 (FCC/FTC 2000)). But even that precedent supports at most only a finding that carriers' *misrepresentations* about their practices regarding data security *or some other activity*, and not the underlying practices or activities themselves, can violate Section 201(b). The precedent is otherwise inapposite: it neither provides justification to create a new data security regime under Section 201(b) from whole cloth, nor does it answer questions regarding how Commission regulation of carriers' data security practices under Section 201(b) is consistent with Section 222. It did not, and could not, because there is no such support for the Commission's novel approach. Indeed, any analysis or citation to precedent necessarily would confirm that the Commission's assertion of data security authority under Section 201(b) ignores and upsets the balance Congress intended to establish under Section 222.

information as part of their business operations, such information is not collected "for and in connection with" telecommunications service, as it is not collected "solely by virtue of the carrier-customer relationship."[193]

2. Section 705 Does Not Provide Authority for Regulating the Privacy Practices of Broadband Providers.

The Commission suggests that Congress provided authority to adopt some of the proposed rules via Section 705,[194] but misstates the scope of the section. While Section 705 does provide a statutory basis on which to impose liability for unlawful misuses of communications, it *does not* provide the Commission with authority to impose privacy rules relating to information gathered and used in the ordinary course of business. In addition, because the proposed broadband privacy rules apply only to ISPs, they cannot plausibly be based on authority found in Section 705, which Congress clearly drafted to apply to "all persons."[195]

It is untenable to claim that Section 705 authorizes regulations governing the use of data in the ordinary course of business. Rather, Congress intended Section 705 to enable the imposition of penalties on rogue actors—*e.g.*, employees of communications companies who breach their duties by misappropriating messages,[196] satellite signal thieves,[197] customers

---

[193] As CTIA recommended in its proposal to the Commission, if the Commission proceeds under Section 201(b), it should harmonize its regulatory approach with the FTC's approach to regulating data in the Internet ecosystem.

[194] *See, e.g.*, *NPRM*, 31 FCC Rcd at 2523, 2585, 2593, 2597 ¶¶ 67, 267, 294, 307.

[195] *See* 47 U.S.C. § 605(a).

[196] *See Nardone v. United States*, 302 U.S. 379, 380-81 (1937) (explaining that Section 705 "provides that no person who, as an employe [sic], has to do with the sending or receiving of any interstate communication by wire shall divulge or publish it or its substance to anyone other than the addressee or his authorized representative or to authorized fellow employes [sic], save in response to a subpoena . . . or on demand of other lawful authority").

[197] *See DirecTV, Inc. v. Barczewski*, 604 F.3d 1004, 1006, 1009 (7th Cir. 2010) (noting that someone who watches pirated TV violates Section 705(a)).

operating illegal descramblers[198]—whose actions require prohibition and deterrence, not governance or regulation.[199] Those actions are categorically distinct from the routine business uses of technical data that the Proposed Rules would govern (but not prohibit). Additionally, the *data types* protected by Section 705—the "existence, contents, substance, purport, effect, or meaning" of a communication[200]—bear scant resemblance to many of the elements of "customer proprietary information" that the Proposed Rules seek to cover—*e.g.*, device identifiers, IP addresses, and so forth.[201] These incongruities demonstrate that Section 705 does not provide authority for the Proposed Rules.[202]

The Proposed Rules also amount to an unreasonable interpretation of Section 705. While the Proposed Rules would apply to ISPs alone, the plain text of Section 705 states that "*no* person" shall engage in the prohibited activities.[203] This disconnect is fatal. The Commission has no grounds on which to distinguish between ISPs and all other "persons" who make use of the exact same data covered by the Proposed Rules, in the exact same ways. The Commission cannot have it both ways: it cannot, on the one hand, claim not to be regulating other entities in the ecosystem, and on the other, propose to rely for privacy rulemaking authority on a provision that, on its face, mandates broad application to all such entities.

---

[198] *See Cmty. Television Sys., Inc. v. Caruso*, 284 F.3d 430, 435 (2d Cir. 2002) (holding that Section 705 "applies in cases involving the sale of descrambling devices").

[199] *Cf.* 47 U.S.C. § 605(e) (enabling the imposition of civil penalties on violators). The inclusion of a private right of action in Section 705 provides further evidence that Congress designed it to impose penalties for malfeasance. *See DirecTV Inc. v. Seijas*, 508 F.3d 123, 125-26 (3d Cir. 2007) (holding that Section 705(a) creates a private right of action to sue over stolen TV signals).

[200] 47 U.S.C. § 605(a).

[201] *See NPRM*, 31 FCC Rcd at 2514-18 ¶¶ 41-53.

[202] *See Sanofi-Aventis U.S. LLC v. FDA*, 842 F. Supp. 2d 195, 208 (D.D.C. 2012) ("The Chevron step I exercise also involves a consideration of the provisions at issue in light of the statute's purpose.").

[203] 47 U.S.C. § 605(a) (emphasis added).

3. The Proposed Rules Are Inconsistent with Section 706.

Section 706 does not provide a legal basis for the Proposed Rules, because the Commission cannot show that the Rules are tailored to promote the acceleration of broadband deployment and adoption. To the contrary, the Proposed Rules will significantly inhibit deployment of network infrastructure by ISPs, without allaying privacy concerns that may depress broadband adoption, while simultaneously increasing consumer confusion and frustration.

As interpreted by the D.C. Circuit in *Verizon v. FCC*,[204] Section 706 authorizes the Commission to promulgate regulations that are tailored to "drive[] end-user demand for more and better broadband technologies, which in turn stimulates competition among broadband providers to further invest in broadband."[205] The Commission bears the burden of demonstrating that any rules adopted to achieve this purpose are "reasonable and grounded in substantial evidence."[206] Although a reviewing court would give some deference "to predictive judgments that necessarily involve the expertise and experience of the agency,"[207] this standard of review is not a rubberstamp.[208]

Here, the Proposed Rules are directly at odds with Section 706's broadband-deployment purpose. As set forth more fully below, the Proposed Rules would impose tremendous costs on providers while simultaneously depriving them of innovative uses of information, which otherwise would become a significant new source of revenue, some of which would be passed on

[204] 740 F.3d 623 (D.C. Cir. 2014).

[205] *Id.* at 642.

[206] *Id.* at 644.

[207] *NCTA v. FCC*, 567 F.3d 659, 669 (D.C. Cir. 2009).

[208] *See Verizon*, 740 F.3d at 639-40; *see also, e.g.*, *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).

to customers in the form of lower prices or improved broadband coverage and capacity. What's more, ISPs are the new entrants to the Internet advertising market and have thus far lagged behind other entities in this ecosystem in their uses of information for advertising and marketing purposes. The Proposed Rules will lock in advantages for these other entities, to the detriment of ISPs.[209] As Moody's Investor Services has stated, these effects will be particularly pronounced for CTIA's members:

> The FCC's proposal also has the potential to derail efforts by wireless carriers to cultivate mobile video advertising revenues. Wireless carriers have the potential to generate significant advertising revenues due to their ability to precisely target ads to wireless subscribers. But, if the FCC restricts the carriers' ability to collect this data, the advertising revenue opportunity will be reduced. Without a robust mobile video advertising market, the product could lose relevance due to its higher cost to consumers and a potential for fewer content choices.[210]

There is thus already evidence that the Proposed Rules will have deleterious effects on ISPs' abilities to make capital-intensive investments in expanding broadband deployment. That is the end of the inquiry.

The Commission approaches the Section 706 analysis more obliquely, focusing not on ISPs' incentives and resources to deploy network infrastructure, but instead on the theory that consumers' privacy concerns have undermined broadband adoption.[211] But even if there were

---

[209] *See* 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 ("[T]he ability [of fixed and mobile broadband providers] to compete with digital advertisers such as Facebook and Google . . . who are able to collect the same type of data from consumers who access their websites and those of others, will be severely handicapped in the future as the old guard ecosystem evolves to become more competitive."); *see also In re Protecting the Privacy of Customers of Broadband and Other Telecommunications* Services, Thomas Leonard & Scott Wallsten, *An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking* 3 (May 25, 2016) ("*Lenard & Wallsten Comments*") (describing how asymmetric regulation would prevent ISPs from developing new business models and competing in online advertising market, depriving ISPs of new revenue and increasing likelihood of higher costs of service for consumers).

[210] *Id.* at 2.

[211] A Pew Study published in December 2015 lists non-broadband users' top five reasons for not having a broadband connection. Concern about online privacy was not listed among the reasons. John B. Horrigan & Maeve Duggan,

substantial evidence *both* supporting the notion that privacy concerns undermine adoption *and* showing that the Proposed Rules would address those privacy concerns (which there is not, as discussed immediately below), the Proposed Rules would still fail, because further network investment will not take place if ISPs lack the incentives or resources to continue to deploy broadband infrastructure. Likewise, to the extent that the regulations would impose costs on ISPs, there is an increased risk those costs would be passed on to consumers, which also would risk depressing demand for, and adoption of, broadband.

Moreover, the NPRM fails to cite "substantial evidence" to support the theory that concerns about privacy inhibit demand for edge services or otherwise deter broadband adoption. Indeed, the Commission has carefully avoided ever expressly reaching such a finding, at best suggesting the existence of a *correlation* between privacy concerns and non-adoption of broadband.[212] And even this correlation cannot withstand scrutiny; the dominance that Google and Facebook enjoy in their respective markets, and in the broadband ecosystem more generally, belies any notion that consumers' concerns about privacy have inhibited the use of online services that collect, use, and share massive amounts of consumers' personal data. To the contrary: even a recent study that purportedly showed that privacy concerns were "separating

---

Pew Research Center, *Home Broadband 2015: The share of Americans with broadband at home has plateaued, and more rely only on their smartphones for online access,* 16 (Dec. 21, 2015) at p. 16, http://www.pewinternet.org/files/2015/12/Broadband-adoption-full.pdf.

[212] *See Lenard & Wallsten Comments* at 19 (noting that the Commission has never found a causal connection between privacy concerns and broadband non-adoption and that more powerful factors are cost, digital literacy, and relevancy of online access); *see also, e.g.*, *In re Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act*, 2016 Broadband Progress Report 31 FCC Rcd 699, 751-52 ¶ 126 & n.351 (2016) ("*2016 Broadband Progress Report*"); *In re Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act*, 2015 Broadband Progress Report and Notice of Inquiry on Immediate Action to Accelerate Deployment 30 FCC Rcd 1375, 1438 ¶ 104 (2015).

consumers from the Internet," in fact showed the opposite: on a year-to-year basis from 2011 to 2015, "the use of online activities, even ones involving sensitive information, continues to *increase*," and, "despite their privacy concerns, people *increasingly* engage in online activities that might involve sensitive information, like financial transactions and shopping."[213] What's more, the tremendous growth of Google and Facebook and the development and adoption of other online platforms and services have occurred under the flexible privacy framework that the FTC has administered and that applied to mobile broadband providers until February 2015.

Furthermore, even assuming that the Commission could establish, by substantial evidence, that privacy concerns inhibit broadband adoption, that would not be enough to satisfy Section 706. Indeed, the Commission would not sustain its burden even if it could show, by substantial evidence, that *some* privacy protections would promote broadband adoption. Instead, to satisfy the requirements of Section 706, the Commission must establish by substantial evidence that *these specific protections* would promote broadband adoption (or remove barriers to such adoption). This articulation of the test follows from the D.C. Circuit's holding in *Verizon*. Specifically, the Open Internet protections at issue there were "binary": absent the blocking and paid prioritization rules, the Commission reasoned, there would have been no protections for the Open Internet. Further, according to the D.C. Circuit, there was evidence in the record that certain ISPs would engage in, for example, paid prioritization.[214] Here, by contrast, possible privacy protections exist on a continuum—from finding implied consent to outright prohibition of certain practices. The Commission therefore must show that there is

[213] Scott J. Wallsten, *No, the NTIA's Survey Data Do Not Show a "Tipping Point" in Behavior Due to Privacy Concerns*, TPI Blog (May 15, 2016), https://techpolicyinstitute.org/2016/05/15/no-the-ntias-survey-data-do-not-show-a-tipping-point-in-behavior-due-to-privacy-concerns/ (emphases added).

[214] *Verizon*, 740 F.3d at 646.

substantial evidence that the *additional increment* of protection provided by requiring opt-in approval for first-party marketing of non-communications-related services and third-party information sharing would facilitate broadband deployment.

Verizon shows that this distinction is significant: "Equally important" to the *Verizon* Court's finding that the rules were reasonable and supported by substantial evidence was its holding that "the Commission ha[d] adequately supported and explained its conclusion that, absent rules such as those set forth in the *Open Internet Order*, broadband providers" would have represented "a threat to Internet openness and could [have] act[ed] in ways that would [have] ultimately inhibit[ed] the speed and extent of future broadband deployment."[215] Further, *Verizon* depended in part on the finding that broadband customers had no recourse in the event that ISPs engaged in conduct that threatened Internet openness, such as paid prioritization or blocking.[216] Here, by contrast, if the Commission were to adopt a regime modeled on the FTC's framework, allowing opt out (but not requiring opt in) for most first-party and affiliate marketing, it would provide privacy-conscious customers—whose adoption of broadband might reasonably be expected to turn, in part, on the privacy practices of ISPs—with the necessary means to protect themselves from disfavored activities.

For the reasons explained throughout these comments, the Proposed Rules are not reasonably related to protecting customer privacy and will not drive further broadband adoption—nor is there substantial evidence showing that the Proposed Rules would enhance customer confidence, furthering adoption, demand, and so forth.

---

[215] *Id.* at 645.

[216] *Id.* at 646 (noting end users' inability "immediately [to] respond to any given broadband provider's attempt to impose restrictions on edge providers").

Two examples illustrate why. *First*, there is, and can be, *no evidence* that consumer concerns about privacy primarily relate to the practices of ISPs, as opposed to other entities in the broadband ecosystem. The evidence suggests that such concerns relate to practices of search, social media, retail entities, and third-party advertising networks.[217] The Proposed Rules cover none of these activities, rendering them unreasonable under Section 706.[218] Nor can the Commission rely on language from *Verizon*, in which the court appeared to find comfort from the fact that the challenged regulations "appl[ied] directly to broadband providers, the precise entities to which section 706 authority to encourage broadband deployment presumably extends."[219] In addition to being quintessential dicta (made clear by the use of the word "presumably"), this analysis addressed whether the rules were too attenuated from Section 706—which the D.C. Circuit acknowledged was an entirely separate *legal* question from the *record-*

[217] *See Lenard & Wallsten Comments* at 3 (concluding that there is "little, if any, link between privacy concerns and broadband adoption" and that any such connection would not be specific to ISPs vis-à-vis edge providers). The Pew Center obtained its results—on which the NPRM places significant weight—by conducting a survey that presented respondents with six scenarios where privacy could be traded for a benefit. The scenarios involved tracking by a variety of entities to approximate routine privacy transactions faced by consumers; not one of the scenarios involved an ISP. Instead, the scenarios involved your place of employment, a website being utilized by your doctor, a loyalty program being administered by your grocery store, a monitoring program being offered by your insurance company, a social media platform being used by your high school, and a smart thermostat sensor being sold by a "new technology company." *See, e.g.*, Lee Rainie & Maeve Duggan, Pew Research Center, *Privacy and Information Sharing* 3-4 (Jan. 14, 2016), http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf; *see also id.* at 9 (describing common privacy problems ranging "[f]rom retail stores that track customers' shopping behavior in exchange for discounts to online applications that offer free service in exchange for serving personalized ads"). Likewise, a recent analysis by the National Telecommunications and Information Administration, in addition to showing that people are *increasingly* engaging in online activities that involve the exchange of sensitive data, *see supra* note 213 and accompanying text, also shows that the activities that generate the most privacy-related concern do not primarily (or at all) involve ISPs. *See* Rafi Goldberg, NTIA, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

[218] *See Burlington N. & Santa Fe Ry. Co. v. Surface Transp. Bd.*, 403 F.3d 771, 776-77 (D.C. Cir. 2005) ("An agency must provide an adequate explanation to justify treating similarly situated parties differently. Where an agency applies different standards to similarly situated entities and fails to support this disparate treatment with a reasoned explanation and substantial evidence in the record, its action is arbitrary and capricious and cannot be upheld." (citations omitted)).

[219] *Verizon*, 740 F.3d at 643.

based question of whether the regulations would meaningfully promote broadband deployment. In other words, even if the Proposed Rules conform to the limiting principle suggested by the *Verizon* court by reaching ISPs only, the Proposed Rules nonetheless fail under *Verizon* unless there is substantial record evidence that they would achieve Section 706's goal of broadband deployment; as the foregoing makes clear, there is not.

Second and relatedly, there is evidence that far from protecting consumers, these Proposed Rules would be counterproductive. As discussed at greater length below, by imposing opt-in approval requirements on ISPs for most use cases, but leaving edge providers under the FTC's regulatory regime (which generally has resulted in opt-out opportunities for the same use cases), the Proposed Rules would create considerable customer confusion about who may do what, with what information, and when. Available evidence indicates that such confusion generates frustration, which in turn can inhibit demand for, and use of, broadband services.[220]

In short, absent granular data distinguishing customer concerns about the privacy practices of ISPs specifically from the privacy practices of other entities in the ecosystem, the Commission's theory that privacy concerns inhibit broadband adoption, if credited, would require the Commission to regulate not just ISPs' privacy practices, but those at the edge as well.

4. Title III Does Not Provide Authority To Promulgate the Proposed Rules for Wireless ISPs.

Finally, the Commission asserts that Sections 303(b), 303(r), and 316 may provide it with "additional source[s] of authority" to impose the Proposed Rules on wireless providers.[221] None of these provisions gives the Commission the authority it seeks, however.

---

[220] *See infra* note 364 and accompanying text.

[221] *NPRM*, 31 FCC Rcd at 2596 ¶ 304; *see also id.* at 2598 ¶ 310; *id.* at 2591 ¶ 286 (noting that Public Knowledge proposed Section 303(b) as a source of authority "to ensure that protections based in Section 222 can be equally applied" to wireless carriers).

Section 303(b) gives the Commission authority to "[p]rescribe the nature of the service to be rendered by each class of licensed [radio] stations and each station within any class."[222] By its plain language, this provision does not authorize adoption of the broadband privacy rules. As multiple court decisions demonstrate, only rules that "define[] the form" of radio services for given license-classes fall within Section 303(b)'s ambit.[223] While courts have interpreted Section 303(b) as enabling the Commission to regulate the actual services delivered over airwaves—*e.g.*, by excluding air passenger communications from certain frequencies, requiring the carriage of data roaming traffic, or requiring the broadcast of independent programming—303(b) does not amount to a roving warrant to regulate any aspect of the provider-subscriber relationship.[224] Because the proposed rules would govern the treatment of customer data, they fall outside of that limited grant of authority.

Section 303(r) likewise fails to support the Proposed Rules. It enables the Commission to "[m]ake such rules and regulations . . . as may be necessary to carry out the provisions" of the Communications Act, but it does not amount to a delegation to regulate by whim. Rules emanating from Section 303(r) must be tethered to the use of otherwise-delegated authority.[225] Thus, the Commission cannot rely on Section 303(r) because there is no plausible way its rules

---

[222] 47 U.S.C. § 303(b).

[223] *Cellco P'ship v. FCC*, 700 F.3d 534, 543 (D.C. Cir. 2012) (upholding the FCC's data roaming rule, which "define[d] the form mobile-internet service must take for those who seek a license to offer it").

[224] *See id.* (upholding the FCC's data roaming rule, which "define[d] the form mobile-internet service must take for those who seek a license to offer it"); *Aeronautical Radio, Inc. v. FCC*, 928 F.2d 428, 441-42 (D.C. Cir. 1991) (holding that Section 303(b) enabled the FCC to exclude air passenger communications from certain frequencies); *MCI Telecomms. Corp. v. FCC*, 561 F.2d 365, 373 (D.C. Cir. 1977) (noting that Section 303(b) enables the FCC to "set[] out limitations on services to be offered over radio facilities"); *Nat'l Ass'n of Indep. Television Producers & Distribs. v. FCC*, 516 F.2d 526, 534-35 (D.C. Cir. 1975) (upholding the FCC's prime time access rule and citing Section 303(b) as a source of FCC regulatory authority).

[225] *See Motion Picture Ass'n of Am., Inc. v. FCC*, 309 F.3d 796, 803 (D.C. Cir. 2002).

are "necessary" to carry out Section 222's mandates, let alone those of any other Communications Act provision.[226]

Finally, Section 316 does nothing more than grant the Commission authority to modify the actual terms of radio station licenses—permissible frequencies, geographic scope, and the like—via the procedural methods outlined in the section itself.[227] Here, the NPRM does not propose to "modify" anything having to do with the features of service governed by licenses. Rather, it proposes to regulate business practices far removed from the actual provision of licensed service. Characterizing the Proposed Rules as "license modifications" would render that term, and the Commission's authority under Section 316, limitless.

II. The Proposed Rules Restricting ISPs' Uses and Disclosures of Information Collected from and About Customers in the Ordinary Course of Business Are Unconstitutional.

Although this proceeding purports to be about protecting the privacy of broadband customers, the gravamen of the Proposed Rules is to restrict ISPs' uses of customer information for marketing purposes. This is clear from the Commission's primary "choice" framework, discussed in detail below, which imposes graduated consent obligations depending on the nature of the service an ISP is marketing. The Commission tacitly admits that imposing restrictions on

[226] *Cf. Fisher v. Univ. of Tex. at Austin*, 133 S. Ct. 2411, 2414 (2013) (explaining that "necessary" implies that "no workable . . . alternatives" to a regulatory scheme are available).

[227] *See* 47 U.S.C. § 316(a)(1) (providing that "[a]ny station license . . . may be modified by the Commission . . . if in the judgment of the Commission such action will promote the public interest, convenience, and necessity, or the provisions of this chapter or of any treaty ratified by the United States will be more fully complied with," and delineating procedures for protests regarding license modifications); *see also, e.g.*, *Cal. Metro Mobile Commc'ns, Inc. v. FCC*, 365 F.3d 38 (D.C. Cir. 2004) (upholding the removal of a frequency from a licensee's operational control pursuant to Section 316); *Cmty. Television, Inc. v. FCC*, 216 F.3d 1133, 1140-41 (D.C. Cir. 2000) (upholding allocation of digital broadcasting channels to certain broadcasters pursuant to Section 316).

ISPs' marketing practices implicates First Amendment interests,[228] but fails to appreciate the magnitude of the constitutional infirmities from which the Proposed Rules suffer.

First, by subjecting ISPs to differentiated treatment from other providers in the ecosystem with respect to how information may be used for speech purposes, the Commission has proposed a framework of paradigmatic speaker-based discrimination. The regulations are therefore presumptively invalid and must survive strict scrutiny, which they cannot do.

Second, even assuming that it would need to survive only intermediate scrutiny, the Commission's proposed scheme is still fatally flawed. ISPs collect and use customer information using a variety of different methods and for a variety of different commercial purposes. For example, an ISP might use information it collects in the ordinary course of business, like a customer's name and home address, to send promotional materials and offerings to the customer (whether related to the broadband service to which the customer subscribes, or not). An ISP also might attempt to target its marketing to the customer based on a more sophisticated customer profile, for example by understanding the customer's online activity. Alternatively, an ISP might use information that it assigns to a customer, like an IP address, to deliver an advertisement on behalf of an unaffiliated third party when the customer visits a website, without sharing the customer's information with either the website or the third-party ad-provider. And an ISP might economically leverage its access to customer information by selling that information to third parties. Each of these use cases is entitled to robust First Amendment protections: most obviously, an ISP's delivery of both first-party and third-party marketing is protected First Amendment speech,[229] but so too is the ISP's selling of information for

[228] *See NPRM*, 31 FCC Rcd at 2544, 2595 ¶¶ 126, 302.

[229] *See, e.g., Edenfield, v. Fane*, 507 U.S. 761, 766 (1993) (first-party marketing qualifies for First Amendment protection); *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1234-35 (10th Cir. 1999) (same).

commercial purpose.[230] Each use case also involves different potential privacy interests that the Commission may assert an interest in protecting. But it is only by analyzing each use case that the Commission even plausibly would be able to develop a record allowing it to impose restrictions. Moreover, CTIA respectfully submits that once each use case is separately analyzed, it becomes clear that there is no set of circumstances where application of the proposed restrictions would survive review.

Third, even if the record develops such that the Proposed Rules are not *conclusively* unconstitutional, the substantial First Amendment questions identified in the proceeding analysis deprive the Commission of the judicial deference that would normally attach to an agency interpretation of an ambiguous statute.[231] In other words, even if a reviewing court found (incorrectly, in all cases) that Section 222 is ambiguous with respect to any of the operative questions—whether it encompasses the provision of broadband service by ISPs; whether it encompasses information beyond CPNI; whether CPNI can encompass information beyond what is specifically enumerated; whether Section 222 authorizes outright prohibitions on certain uses of information; or whether Section 222 extends to any uses of information obtained otherwise than by virtue of providing service—the court nonetheless would be obligated to invalidate the rules in favor of a permissible alternative that avoids the constitutional problems caused by imposing discriminatory, opt-in requirements on ISPs.[232]

---

[230] *See Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653, 2667 (2011) (finding a "strong argument that prescriber-identifying information [itself] is speech for First Amendment purposes").

[231] *See Nat'l Mining Ass'n v. Kempthorne*, 512 F.3d 702, 711 (D.C. Cir. 2008) (explaining that where serious constitutional problems are presented, the "canon of constitutional avoidance trumps *Chevron* deference"); *West*, 182 F.3d at 1231 ("[D]eference to an agency interpretation is inappropriate not only when it is conclusively unconstitutional, but also when it raises serious constitutional questions.").

[232] *See AFL CIO v. FEC*, 333 F.3d 168, 179 (D.C. Cir. 2003) ("[A]n agency acts unreasonably if, instead of choosing among constitutionally permissible alternatives, it interprets ambiguous statutory language as indicating that Congress intended to authorize infringements on constitutional rights.").

Finally, one such alternative that suffers from no constitutional problems is the industry proposal.[233] Specifically, CTIA and others have urged that the Commission adopt rules that subject ISPs to the same restrictions as other entities in the ecosystem with access to, and control over, customer information. While such restrictions also would implicate ISPs' First Amendment rights, they would not be tantamount to ineffectual, speaker-based discrimination, nor would they regulate more speech than is absolutely necessary to protect consumers.

A. The Proposed Use Restrictions Are Speaker-Based and Fail To Survive Strict Scrutiny Under *Sorrell v. IMS Health, Inc.*

The Commission acknowledges that its proposed choice rules implicate ISPs' First Amendment rights, and asks whether various consent requirements satisfy the Supreme Court's test for restrictions on commercial speech, as articulated in *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*.[234] But the controlling precedent is not *Central Hudson*; it is *Sorrell v. IMS Health, Inc.*[235] That case involved a First Amendment challenge to a Vermont law that, among other things, "prohibit[ed] pharmacies, health insurers, and similar entities from selling prescriber-identifying information, subject to [certain] statutory exceptions."[236] According to the Supreme Court, the provision was problematic as both content- and speaker-based discrimination:

> [The statute] disfavors marketing, that is, speech with a particular content. More than that, the statute disfavors specific speakers, namely pharmaceutical manufacturers. As a result of these content- and speaker-based rules, detailers cannot obtain prescriber-identifying information, even though the information may be purchased or acquired by other speakers with diverse purposes and viewpoints [e.g., academic organizations]. Detailers are likewise barred from using the information for marketing, even though the information may be used by

[233] *See supra* note 7; Ex. A.

[234] *See, e.g., NPRM*, 31 FCC Rcd at 2595 ¶ 302 n.470 (citing 447 U.S. 557 (1980)).

[235] 131 S. Ct. 2653.

[236] *Id.* at 2662.

> a wide range of other speakers. . . . The law on its face burdens disfavored speech by disfavored speakers.[237]

Such restrictions are presumptively invalid.[238] That is so because "[c]hief amongst the evils the First Amendment prohibits are government restrictions distinguishing among different speakers, allowing speech by some but not others."[239]

The Proposed Rules are no different. The Commission is proposing to burden speech the Commission disfavors (*i.e.*, marketing based on information obtained from customers), about subjects the Commission disfavors (*i.e.*, non-broadband-related products and services), by speakers the Commission disfavors (*i.e.*, ISPs), while allowing a wide range of other speakers (*e.g.*, Google, Facebook) to use the same information for diverse commercial and noncommercial purposes. Accordingly, the Proposed Rules are presumptively invalid, and, held to strict scrutiny, they clearly fail. As discussed at greater length below, the Proposed Rules fail to satisfy even intermediate scrutiny, and here, it is sufficient merely to note that the requirement that ISPs obtain opt-in approval, as opposed to opt-out consent (or implied consent), is not the narrowest means of advancing the state's interest (assuming, *arguendo*, that interest is *compelling*) in protecting customer privacy—an interest that is not implicated by many use cases that the Commission has swept within the scope of the Proposed Rules.

---

[237] *Id.* at 2663.

[238] *Id.* at 2667 ("In the ordinary case it is all but dispositive to conclude that a law is content-based and, in practice, viewpoint-discriminatory."); *see also Time Warner Cable, Inc. v. Hudson*, 667 F.3d 630, 639-40 (5th Cir. 2012) ("[A] law that targets a small handful of speakers for discriminatory treatment suggests that the goal of the regulation is not unrelated to suppression of expression, and such a goal is presumptively unconstitutional. Therefore, we cannot countenance such treatment unless the State asserts a counterbalancing interest of compelling importance . . . .").

[239] *ACLU of N.C. v. Tennyson*, 815 F.3d 183, 186 (4th Cir. 2016) (internal quotation marks omitted).

B. Even Under *Central Hudson*'s Intermediate Scrutiny Test, the Proposed Rules Fail at Every Step.

The Proposed Rules regarding the use and disclosure of, and permitting access to, information fare no better under the *Central Hudson* intermediate scrutiny test. At the outset, the NPRM gives short shrift to the well-settled principle that commercial speech, such as the first- and third-party marketing that ISPs engage in, has (and offers) substantial value for customers. It is likewise settled that it is always preferable for individual consumers, rather than government agencies, to judge the merits of speech.[240] For these reasons, the party seeking to restrict commercial speech has the burden of justifying such regulations at every step of the inquiry. While CTIA members believe that customer privacy is an important value (and indeed, have taken substantial steps to protect the privacy of their subscribers' information), the Commission cannot invoke a nebulous (and limitless) interest in protecting privacy to curtail marketing practices; instead, it must create a record that specific marketing practices cause cognizable privacy harms that its speech restrictions will materially redress. The NPRM does not conceptualize use cases in a way that would allow for such a record, creating a framework that is facially invalid, and unconstitutional on an as-applied basis.

1. Because Commercial Speech Promotes the Public Interest, the Commission Bears the Burden of Justifying Restrictions on ISP Speech at Every Step of the Inquiry.

It is a bedrock constitutional principle that speech has considerable value and should not be curtailed. This proposition holds in the commercial context.[241] Even before the advent of

[240] *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).

[241] *Sorrell*, 131 S. Ct. at 2664 ("A consumer's concern for the free flow of commercial speech often may be far keener than his [or her] concern for urgent political dialogue." (internal quotation marks omitted)).

modern, targeted, and sophisticated advertising and marketing practices, the Supreme Court recognized the public interest benefits that would flow from such practices:

> [Commercial] solicitation may have considerable value. . . . [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. . . . Solicitation also enables the seller to direct his [or her] proposals toward those consumers who he [or she] has a reason to believe would be most interested in what he [or she] has to sell.[242]

In the *Sorrell* case, the Supreme Court amplified this analysis, explaining that there was substantial value in facilitating salespersons' access to the "background and purchasing preferences of their clientele"; that is so in the pharmaceutical and medical context, because "[k]nowledge of a physician's prescription practices—called 'prescriber identifying information'—enables a detailer better to ascertain which doctors are likely to be interested in a particular drug and how best to present a particular sales message."[243]

Here too, customers derive substantial benefits from ISPs' commercial speech. An ISP's knowledge of its subscribers can enable the ISP better to anticipate the subscribers' interests and needs, and to avoid delivery of irrelevant or superfluous advertisements. CTIA members have used their access to customer information to market products, such as appropriately sized device cases and screens; proprietary services like cloud storage; and joint promotional offers, such as discounted Spotify or Amazon Prime membership.[244] Additionally, ISP marketing has overall

---

[242] *Edenfield*, 507 U.S. at 766.

[243] *Sorrell*, 131 S. Ct. at 2659-60.

[244] *See, e.g.*, Dante D'Orazio, *AT&T Brings Back Unlimited Data Plans for Its DirecTV and U-Verse Subscribers*, The Verge (Jan. 11, 2016), http://www.theverge.com/2016/1/11/10746516/att-unlimited-data-plan-pricing-directv-uverse; Nick Hardiman, *Verizon's New Cloud Platform*, TechRepublic (Dec. 16, 2013), http://www.techrepublic.com/blog/the-enterprise-cloud/verizons-new-cloud-platform/; Yoni Heisler, *Sprint Offering a Free Year of Amazon Prime If You Buy a Samsung Smartphone*, BGR (Nov. 7, 2015), http://bgr.com/2015/11/07/sprint-offers-free-amazon-prime-samsung/; Greg Kumparak, *T-Mobile Stops Counting*

pro-competitive effects. As consumers become aware of different options and packages, they can change providers,[245] creating overall incentives for ISPs continuously to improve products and services, and to develop innovative packages and bundles.

That is not to say that CTIA members are now—or will ever be—capable of delivering only creative or useful marketing to their subscribers. But the fact that some consumers may find some aspects of ISP marketing to be burdensome, distasteful, or even merely useless cannot by itself justify the government's restricting such marketing. Any argument otherwise has to be based on an assumption that "the public is not sophisticated enough to realize the limitations of advertising, and that the public is better kept in ignorance . . . . [T]he argument rests on an underestimation of the public."[246]

It follows from these principles that the burden will rest with the Commission to justify any restriction on ISPs' commercial speech,[247] under the following intermediate scrutiny test:

> If the communication is neither misleading nor related to unlawful activity,[[248]] . . . [t]he State must assert a substantial interest to be achieved by restrictions on commercial speech. Moreover, the regulatory technique must be in proportion to that interest. The limitation on expression must be designed carefully to achieve the State's goal. Compliance with this requirement may be measured by two criteria. First, the restriction must directly advance the state interest involved; the regulation may not be sustained if it provides only ineffective or remote support for the government's purpose. Second, if the governmental interest could be served as well by a more limited restriction on commercial speech, the excessive restrictions cannot survive.[249]

Data Used with Spotify, Pandora, and Certain Other Music Services, TechCrunch (June 18, 2014), http://techcrunch.com/2014/06/18/t-mobile-stops-counting-data-used-with-spotify-pandora-itunes-radio-and-certain-other-music-services.

[245] *See infra* note 361 and accompanying text (discussing competition among wireless providers and no-cost-switching campaigns).

[246] *See Bate*, 433 U.S. at 374-75.

[247] *Edenfield*, 507 U.S. at 770-71.

[248] It is CTIA's understanding that the proposed rules are not based on any concerns with misleading or otherwise unlawful ISP marketing. If such an interest is advanced, CTIA will address it in Reply Comments.

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

Moreover, "[t]his burden is not satisfied by mere speculation or conjecture; rather, a governmental body seeking to sustain a restriction on commercial speech must demonstrate that the harms it recites are real and that its restriction will in fact alleviate them to a material degree."[250]

2. The Commission Can Invoke an Interest in Protecting "Privacy" Only Insofar as It Identifies a Particularized Privacy Harm Supported by Record Evidence.

Before turning to how the Proposed Rules fare under the *Central Hudson* inquiry as applied to different ISP use cases, it bears emphasizing that the interest on which the Commission is relying here, "protecting privacy," is amorphous.[251] To be sure, courts have described that there is a substantial interest in protecting privacy.[252] And, as discussed below, CTIA members recognize the importance of protecting their customers' privacy; indeed, even a cursory review of the privacy policies of the four largest wireless providers shows the length to which carriers have gone, for example, to protect sensitive data, and to ensure that customers are aware of how their data are being used.[253] But when a government agency asserts a state interest in protecting privacy in order to restrict speech, that interest cannot be invoked in the abstract, and instead must be defined by reference to a *particularized and cognizable* privacy harm.[254]

For example, under D.C. Circuit precedent, the government's interest in protecting privacy can encompass the right of individuals to control the disclosure of their information

---

[250] *Edenfield*, 507 U.S. at 770-71.

[251] In support of various iterations of the CPNI voice regulations adopted under Section 222, the Commission has previously asserted an interest in protecting customer privacy and promoting competition. *See, e.g.*, *NCTA v. FCC*, 555 F.3d at 1001; *U.S. West*, 182 F.3d at 1234-35.

[252] *NCTA*, 555 F.3d at 1001; *Trans Union Corp. v. FTC*, 267 F.3d 1138, 1142 (D.C. Cir. 2001).

[253] *See infra* note 337.

[254] *See, e.g., U.S. West*, 182 F.3d at 1234-35.

outside of a carrier-customer relationship.[255] But the state's interest in protecting privacy does not encompass a customer's desire to prevent collection of personal information in the abstract—or an unsubstantiated risk of breach.[256] Likewise, there *can be* a substantial interest in protecting consumers from vexatious marketing that is tantamount to harassment and intimidation.[257] Many courts have applied that interest to uphold protections of personal injury victims and their loved ones from distressing intrusions in the immediate aftermath of an accident, especially in the home, which is a unique zone of constitutional protection.[258] But to invoke this interest, there must be some record substantiating the intrusiveness of the communications.[259]

Finally, insofar as there are recognized substantial interests in protecting consumers' control of their personal information and protecting consumers from vexatious marketing, that interest extends only to residential, retail clients—*i.e.*, there are no such interests in protecting *commercial* clients. Accordingly, even if the Commission were to adopt the Proposed Rules, CTIA urges the Commission to create carve outs for enterprise and small and medium business ("SMB") customers—as the voice CPNI rules currently do for business customers.[260]

3. The Proposed Rules Are Facially Unconstitutional Because They Lack Any Nexus to Privacy and Are Likely Unconstitutional as Applied to Each ISP Use Case.

Turning now to the Proposed Rules, under *Central Hudson*, the Commission must demonstrate, first, that it has identified a substantial interest and, second, that these rules are

[255] *NCTA*, 555 F.3d at 1001.

[256] *U.S. West*, 182 F.3d at 1235.

[257] *Edenfield*, 507 U.S. at 769.

[258] *See, e.g., Fla. Bar v. Went For It, Inc.*, 515 U.S. 618, 624 (1995).

[259] *See Sorrell*, 131 S. Ct. at 2669-70; *Edenfield*, 507 U.S. at 775-76.

[260] *See* 47 C.F.R. § 64.2010(g).

reasonably tailored to that interest.[261] The Proposed Rules apply Section 222 in a graduated manner, heightening approval requirements depending on (1) whether the product or service the ISP is marketing is part of the service itself, communications-related, or non-communications-related (requiring, respectively, implied consent; notice and opt-out opportunity; and notice and opt-in approval);[262] or (2) whether the ISP shares information with any non-affiliate.[263]

While schematically simple, the structure of the Proposed Rules itself reveals a lack of coherent tailoring: it conflicts with First Amendment values without advancing or reflecting *any* countervailing privacy values. Indeed, on the speech side of the ledger, the Commission primarily distinguishes between speech based on its *content* (*i.e.*, whether the speech relates to broadband service, communications-related services, or non-communications-related services). But burdening speech based on content, like burdening speech based on the identity of the speaker, is presumptively invalid.[264] That the burdened speech is commercial does not excuse the discrimination.[265] On the other side of the ledger, these arbitrary marketing distinctions lack any nexus to identified privacy concerns—*i.e.*, issues that relate to the sensitivity of data or loss of control.[266] Instead, the Commission should have engaged, and must engage, in a more granular use-by-use analysis to determine if any restrictions on ISPs' commercial speech would survive constitutional review. CTIA respectfully submits that, based on the defining

---

[261] *See supra* note 249 and accompanying text.

[262] *NPRM*, 31 FCC Rcd at 2539-45 ¶¶ 111-127.

[263] *Id.*, 31 FCC Rcd at 2545-47 ¶¶ 129-132.

[264] *See Sorrell*, 131 S. Ct. at 2667 ("In the ordinary case, it is all but dispositive to conclude that a law is content-based.").

[265] *See City of Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 417-18, 423-25 (1993) (invalidating restriction on distribution of commercial materials, but not newspapers, on public properties, because the state could not proffer a "[relevant] basis for distinguishing" regulated and unregulated materials).

[266] *See infra* Part V.B.1 (discussing privacy regimes proposed by FTC, White House, and European Union, all of which base protections on sensitivity of data at issue).

characteristics of the broadband ecosystem, it is difficult to imagine how the Commission could develop a record that would allow restriction of any of the following.

a. Rules Restricting First-Party Marketing Based on Information Collected in the Ordinary Course of Business Without Third-Party Disclosure or Access Fail at Every Step of the Central Hudson Analysis.

Requiring anything more than implied consent for an ISP to engage in first-party marketing, irrespective of the nature of the product or service being marketed, fails at every step of the *Central Hudson* inquiry. ISPs routinely engage in first-party marketing, directly to their subscribers, regarding product and service offerings. To deliver this marketing, ISPs use information collected for delivery and billing purposes—*e.g.*, name, e-mail address, and phone number. Such marketing is pro-competition and pro-consumer.[267]

The state lacks any interest in regulating this category of marketing. There can be no plausible claim that regulation of first-party marketing enhances a consumer's ability to control his or her information, where the marketing involves no third-party disclosure or access.[268] Nor is there (or can there be) any reasonable basis to conclude that first-party marketing creates an increased risk of disclosure or access.[269] Restrictions on first-party marketing also cannot be justified based on an interest in protecting consumers from vexatious, burdensome, or harassing marketing, absent some evidence in the record that ISPs' first-party marketing is qualitatively or quantitatively different from first-party marketing by other entities in the Internet ecosystem.

---

[267] *See supra* notes 242-246 and accompanying text.

[268] *Cf. NCTA*, 555 F.3d at 1001.

[269] *Cf. id.* at 999, 1001 n.* (discussing potential harms arising from sharing voice CPNI). The Commission asserts that "[i]ncreasing the number of entities that have access to customer [information] logically increases the risk of unauthorized disclosure by both insiders and computer intrusion," *NPRM*, 31 FCC Rcd at 2545 ¶ 129, but even if this asserted risk is borne out by the record in the broadband context, it would not provide a basis for restricting any use case that does not involve disclosing or permitting access to customer information to third parties.

Moreover, consumers can avail themselves of existing protections that apply equally to all companies to mitigate any burdensome or harassing marketing—*e.g.*, by joining the do-not-call registry or taking advantage of the protections offered in CAN-SPAM concerning e-mail marketing, both of which operate on an opt-out basis.[270]

Imposing an approval requirement beyond implied consent on any first-party marketing by ISPs would fail at the tailoring level for two primary reasons.

First, such restrictions would create a regulatory framework where ISPs are treated differently from other entities in the ecosystem—which largely operate under the framework articulated in the *FTC Report*[271]—without any reasonable basis for doing so that relates to the proffered interest in protecting consumers' control over their information or preventing vexatious marketing. Courts routinely invalidate restrictions imposed on only a particular type of commercial speech or speakers, where the distinctions between regulated and unregulated speakers or speech lack any nexus to the proffered state interest.[272] The obverse is also true:

---

[270] *See* 15 U.S.C. §§ 6101-6108 (codifying Telemarketing and Consumer Fraud and Abuse Prevention Act); 16 C.F.R. § 310.1, *et seq.* (FTC implementing rules); 47 C.F.R. § 64.1200, *et seq.* (Commission implementing rules); *see also* FTC, *National Do Not Call Registry*, https://www.donotcall.gov/register/reg.aspx (last visited May 18, 2016); FTC, *CAN-SPAM Act: A Compliance Guide for Business*, https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business (last visited May 18, 2016).

[271] *See infra* Part V.B.1, especially notes 369 to 377 and accompanying text (discussing the FTC's approach to first-party marketing).

[272] *See Sorrell*, 131 S. Ct. at 2668; *Discovery Network*, 507 U.S. at 417-18, 424-25, 428 (invalidating restriction on distribution of commercial materials, but not newspapers, on public properties, because the state could not proffer a "basis for distinguishing" regulated and unregulated materials "that [was] relevant to an interest asserted by the City"); *Pitt News v. Pappert*, 379 F.3d 96, 107-08 (3d Cir. 2004) (invalidating state restriction banning advertisers from paying for dissemination of alcoholic beverage advertising by communications media affiliated with a university, college, or other educational institution—finding that regulation of "only a narrow sector of the media," would not advance the state's interest in preventing underage drinking, because students who did not see alcoholic beverage ads in a student newspaper still would be "exposed to a torrent of beer ads on television and the radio" and in other publications).

differentiated restrictions are upheld only where there is a meaningful record that supports the discriminatory treatment of certain commercial speech or speakers.[273]

The NPRM does not identify any basis for concluding that first-party marketing by ISPs is uniquely problematic in terms of either consumer control or vexatiousness. Indeed, to the extent that the Commission has identified purported distinctions between ISPs and other entities in the ecosystem, those differences relate to ISPs' unique abilities to *collect* comprehensive customer information.[274] But even if true (which it is not), ISPs' supposed enhanced collection capabilities lack any nexus to the risk of disclosure outside of the customer-carrier relationship or to the vexatious nature of advertising. Nor is there anything in the FTC's *Privacy Report* that expressed concerns about ISPs' first-party marketing practices, further undercutting any claim to appropriate tailoring.[275]

Indeed, the Commission's use of Section 222—a statute that Congress drafted 20 years ago to apply to data related to telephone voice services—suggests that the Proposed Rules are improperly tailored; the Supreme Court has previously held that the tailoring of speech restrictions is inherently suspect where, as here, the government imposes those restrictions in reliance on an "outdated prohibition . . . enacted long before" the motivating concern behind the regulation developed.[276] Further, as discussed at greater length below, there is substantial record evidence that other entities in the broadband ecosystem—which, under the Proposed Rules, will

---

[273] *See Mainstream Mktg. Servs., Inc. v. FTC*, 358 F.3d 1228, 1240 (10th Cir. 2004) (upholding do-not-call registry exclusion of charities and political organizations based on record evidence that most abusive practices were limited to commercial marketers).

[274] *See, e.g.*, *NPRM*, 31 FCC Rcd at 2584-85 ¶ 265.

[275] *Cf. Mainstream Mktg.*, 358 F.3d at 1241 (explaining that because "the type of unsolicited calls that the do-not-call list does prohibit—commercial sales calls—is the type that Congress, the FTC and the FCC have all determined to be most to blame for the problems the government is seeking to address" was probative that the do-not-call registry was properly tailored).

[276] *Cf. Discovery Network, Inc.*, 507 U.S. at 417.

be subject to fewer restrictions on first-party marketing—possess *more power* in the online advertising market than ISPs.[277]

Second, requiring approval beyond implied consent for any first-party marketing would be overly restrictive, even if applied uniformly across the ecosystem. The Commission's proposal to require opt-in consent for first-party marketing of non-communications-related services[278] is particularly problematic (although CTIA also objects to an opt-out requirement for communications-related marketing). It is axiomatic that by setting a default in favor of censorship, an opt-in regime prevents more speech than is necessary (if preventing *any* is necessary) to protect consumers.[279] The Commission cannot justify this increased burden on mere conjecture, but instead must identify a record-based need.[280] Even under intermediate scrutiny, the differences between requiring implied consent, opt-out opportunity, and opt-in approval is doctrinally significant; many courts, including the Supreme Court, have held that to survive a First Amendment challenge, a commercial speech restriction must require that customers who do not want to receive speech affirmatively opt out.[281]

---

[277] *See infra* Part V.A.2.

[278] *NPRM*, 31 FCC Rcd at 2544-45 ¶ 127.

[279] *See U.S. West*, 182 F.3d at 1238-39.

[280] *See id.*

[281] *Mainstream Mktg.*, 358 F.3d at 1242 (affirming restriction that allowed customers to opt out of marketing); *see also Rowan*, 397 U.S. at 737-38 (affirming restriction allowing customers to opt out of receipt of certain mailings, because a customer must be allowed "to erect a wall[] that no advertiser may penetrate without his [or her] acquiescence").

b. *Rules Restricting First-Party Marketing Based on Customer Profiles Developed Through Evaluating Online Activity Without Third-Party Disclosure or Access Fare No Better Under* Central Hudson.

Restrictions on ISP first-party marketing of products and services (regardless of whether communications-related) based on more sophisticated data collection practices by ISPs are not materially different and likewise fail at every step of the *Central Hudson* inquiry.

As technology evolves, ISPs may engage in first-party marketing of products and services using more sophisticated profiles of their customers. ISPs may develop these profiles using a variety of methods, including by evaluating online activity and content consumption. Such practices are already common among popular edge providers, and have become an important part of the consumer experience. For example, Netflix delivers recommendations to users based on what they already have watched and what consumers with similar interests have watched.[282] Amazon, too, monitors what an individual purchases and makes recommendations based on what others with similar tastes have purchased in the past.[283] Indeed, these practices can also improve the delivery of advertisements based on customers' needs and preferences.

Imposing prohibitions or consent-based requirements (*i.e.*, opt-out or opt-in requirements) on ISPs before they may engage in this use case fails at the state interest level. Insofar as ISPs engage in sophisticated marketing without sharing or permitting access to customer information, the practices do not implicate a customer's interest in controlling access to

[282] *See* Ben Popper, *How Netflix Completely Revamped Recommendations for Its New Global Audience*, The Verge (Feb. 17, 2016), http://www.theverge.com/2016/2/17/11030200/netflix-new-recommendation-system-global-regional.

[283] *See* Lutz Finger, *Recommendation Engines: The Reason We Love Big Data*, Forbes (Sept. 2, 2014), http://www.forbes.com/sites/lutzfinger/2014/09/02/recommendation-engines-the-reason-why-we-love-big-data/#3f54881a218e.

information beyond the customer-carrier relationship.[284] Nor would such restrictions survive based on the need to protect customer information from an unsubstantiated risk of breach,[285] especially in light of the robust data security practices that ISPs already have adopted.[286] Moreover, any claim that the effectiveness of sophisticated marketing makes it more "vexatious" would contravene settled First Amendment principles; indeed, the fact that speech is "effective" demonstrates that it is "valuable,"[287] and, in any event, commercial speakers have a First Amendment interest in communicating the most effective and informative speech.[288] Finally, CTIA respectfully urges the Commission to proceed cautiously before articulating a notion of privacy based on perceived public discomfort with information collection and profiling.[289] That some consumers might *prefer* not to have advertising tailored to their interests is a red herring; consumers certainly have come to *expect* these practices, and an opt-out opportunity is more than adequate for those who truly find such advertising vexatious. Additionally, here too, due to the nature of the Internet ecosystem, CTIA believes it is unlikely that a record will develop reflecting that any such concern is uniquely (or even at all) tied to the practices of ISPs. In the absence of such a record, the Commission's Proposed Rules would be constitutionally infirm.

Prohibitions or restrictions on this use case also fail the next step of the inquiry: they are improperly tailored, for the same reasons that restrictions on traditional first-party marketing by

---

[284] *Cf. NCTA*, 555 F.3d at 1001.

[285] *U.S. West*, 182 F.3d at 1235.

[286] *See generally infra* Part VI.B.

[287] *Cf. Thompson v. Western States Med. Ctr.*, 535 U.S. 357, 359 (2002).

[288] *Sorrell*, 131 S. Ct. at 2663 ("Vermont's law thus has the effect of preventing detailers—and only detailers—from communicating with physicians in an *effective and informative manner*" and is suspect because the intent is to "diminish the effectiveness of marketing by manufacturers of brand-name drugs" (emphasis added)).

[289] *See U.S. West*, 182 F.3d at 1234 ("[T]he government cannot satisfy the second prong of the *Central Hudson* test by merely asserting a broad interest in privacy. It must specify the particular notion of privacy and interest served.").

ISPs are deficient—*viz.*, because there is no record-based need to impose such restrictions on ISPs, but not on other entities in the ecosystem,[290] and because, for the reasons explained in the preceding subsection, any requirement beyond implied consent is overly restrictive, even if uniformly applied.[291]

c. Rules Restricting First-Party Delivery of Third-Party Blind Advertising Without Third-Party Disclosure or Access Likewise Fail Central Hudson *at Both the State Interest and Tailoring Steps.*

Restrictions on an ISP's ability to deliver third-party advertising in the context of relationships that do not require the ISP to disclose or share any customer information with the third party also cannot withstand scrutiny. Moreover, by adopting heightened consent requirements before ISPs can engage in this use case, the Commission would risk inadvertently stymieing a nascent and innovative market—a result that does not advance the state's interest in protecting sensitive information or customer control over the disclosure of information.

ISPs are increasingly involved in the business of delivering third-party advertisements to their customers, using information obtained from or assigned to the customer in the provision of service (*e.g.*, IP address), or through more sophisticated practices (*e.g.*, analyzing online activity), but without disclosing any of the customer information to the third-party ad purchaser. For example, a local retail store might request that an ISP deliver 25,000 advertising impressions to customers in the retailer's market. The ISP can do so, using customer IP addresses and billing zip codes, without disclosing any of that information to the third-party retailer. Likewise, a national fashion retailer might purchase delivery of promotional offers to individuals who have previously visited the retailer's website.

[290] *See supra* notes 271-277 and accompanying text.

[291] *See supra* notes 278-281 and accompanying text.

This use case does not present a different constitutional inquiry from the previously discussed scenarios involving ISPs' first-party marketing. Insofar as the delivery of third-party advertising is blind to the third party, the practice does not involve or risk the sharing of information outside of the carrier-customer relationship. Nor does it appear possible that a record will develop that ISP delivery of such advertisements is uniquely problematic or vexatious, relative to delivery of such advertisements by other entities in the ecosystem. For the reasons stated earlier, such restrictions also fail the tailoring prong of the *Central Hudson* test: they do not advance the state's interest due to the commonplace, identical practices by other unregulated entities, and, independently, approval requirements above implied consent are overly restrictive.

d. Rules Indiscriminately Restricting ISP Uses that Involve Disclosing or Permitting Access to Customer Information to Unaffiliated Third Parties Fail in Most Cases to Advance a State Interest and Certainly Are Not Narrowly Tailored.

At various points and for various commercial reasons, an ISP might disclose customer information to an unaffiliated third party, or permit that party to access the customer information—in either case, for specific or more general purposes. For example, a small ISP that lacks the resources and scale to have an internal marketing team may need to establish an ongoing relationship with a vendor to communicate with its customers about existing or new products and services. A mid-sized ISP that wants to send its customers a direct mailing promotional offer has to put customer names and addresses on the mailer, which will be delivered via the U.S. Post Office or a private courier service. Another mid-sized ISP might contract with a retailer to provide ad impressions to customers in a certain geographic area, and might export a set of IP addresses (with no further information) to an ad platform to effectuate actual delivery of the impressions. A large ISP may achieve scale-based efficiencies by

outsourcing some of its customer service functions to a third-party call center, allowing the vendor's employees to access customer information to troubleshoot service-related issues, while another large ISP might decide to leverage its information resources as a data broker by selling customer information to aggregators and other third parties.[292]

All of the above use cases qualify as First Amendment speech.[293] And the Proposed Rules would require each of the above ISPs to obtain opt-in approval.[294] That cannot be correct.

With respect to the state interest inquiry, under *NCTA v. FCC*, the Commission has a cognizable interest in protecting consumers' ability to preserve their information within the customer-carrier relationship.[295] Each of the above use cases implicates that interest *in the abstract*. But a reviewing court also will have to examine the record to ensure that the Commission adequately justifies the assertion of that interest here.[296] Indeed, it is unclear that *NCTA* could be extended to reach *all* sharing of information with third parties, given the Supreme Court's intervening holding in *Sorrell* that the types of information regulated by the Proposed Rules—like the information regulated by the Pretexting Rules—effectively qualify as speech entitled to protection.[297] Instead, the Commission will be required to show the likelihood that, and the mechanism by which, particular types of sharing will result in particular privacy

[292] As noted below, none of the four largest providers currently sell customer information absent customer consent. *See infra* note 337.

[293] *See supra* notes 229-230 and accompanying text.

[294] For example, the Commission proposes permitting a provider to "use," but not to disclose or permit access to, customer information for purpose of providing broadband service, or services necessary to, or used in, the provision of broadband service. *See NPRM*, 31 FCC Rcd at 2540 ¶ 113.

[295] *See* 555 F.3d at 1001.

[296] *U.S. West*, 182 F.3d at 1234-35.

[297] *See supra* note 230.

harms.[298] CTIA respectfully submits that it is unlikely that the record will develop to show that an ISP's sharing of a customer's name and address with the Post Office without prior approval implicates that customer's interest to the same extent as an ISP's selling that customer's data without approval to a data broker.

Moreover, even if a reviewing court were to agree, despite *Sorrell*, that the Commission has a uniform, substantial interest in protecting customers' ability to control the disclosure of, and access to, their information—without regard to the nature of, and privacy risks associated with, the actual disclosure or access involved—the Proposed Rules regarding third parties nonetheless fail the *Central Hudson* inquiry at the tailoring level. To survive review, restrictions on commercial speech must "directly advance the state interest involved; the regulation may not be sustained if it provides only ineffective or remote support for the government's purpose."[299]

Here, the NPRM effectively admits that the Proposed Rules will not in any way advance the Commission's interest in protecting customer control over information: In discussing the risks arising from information sharing, the Commission reiterated its longstanding policy judgment that "in the voice context, once confidential customer information enters the stream of commerce, consumers are without meaningful recourse to limit further access to, or disclosure of, that personal information" and further "anticipate[d] that this is equally true for other forms

[298] *See 2007 CPNI Order*, 22 FCC Rcd at 6947 ¶ 37 (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 6951 ¶ 46 (explaining record evidence, including quantitative evidence, demonstrating mechanisms by which sharing CPNI with joint venture partners and independent contracts "increase[s] the odds of wrongful disclosure of this sensitive information"). Given the amount of time that has passed, and the proposed changes to the types of information subject to protection, the CPNI voice record is insufficient to justify the proposed restrictions on all third party use cases.

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

of customer [proprietary information]."[300] As discussed at greater length in Part IV, the information that the Commission is claiming to protect has already entered the stream of commerce, and is held by numerous entities in the Internet ecosystem, who use it, sell it, analyze it, and share it for a variety of commercial and noncommercial purposes. The Proposed Rules will not alter the practices of any of these entities, which currently dominate the online advertising market relative to ISPs' relatively modest presence. And while the Proposed Rules would regulate ISPs' use of customer information that they obtain by providing broadband service, they cannot prevent ISPs from simply buying that same information and then using and disclosing it pursuant to their own privacy policies.[301]

III. Any Proposed Rules Should Be Based on the Sensitivity of the Data Protected and the Needs for ISPs to Adapt to Changing Technological Developments.

Not only do the Proposed Rules, for the reasons stated above, fail as a matter of statutory and constitutional law, they also fail profoundly as a matter of policy. Privacy rules should be based on the sensitivity of the data and should be flexible enough to allow ISPs to adapt to changing technology. The Parts that follow discuss CTIA's concerns with the four kinds of rules the Commission has proposed: notice, choice, data security, and data breach notification.

The Proposed Rules impose rigid notice requirements on ISPs that risk degrading customers' experience and increasing costs, without enhancing privacy protections for consumers. Regarding choice, the Proposed Rules would create an asymmetric regulatory framework that would impose onerous consent requirements on just one slice of the online data ecosystem, departing radically from established privacy regulation in a way that does not provide

[300] *NPRM*, 31 FCC Rcd at 2546 ¶ 129.

[301] *See supra* Part I.C.5 (discussing Commission's authority to regulate use of information obtained other than by virtue of providing broadband service).

meaningful privacy protections for consumers and that inhibits competition in the marketplace for new online products and services. The proposed choice rules also fail to provide sufficient flexibility for ISPs to use and disclose information for purposes unrelated to marketing, potentially preventing ISPs from taking sufficient action to protect against fraud, abuse, cybersecurity threats, and mismanagement of the network. In the area of data security, the Proposed Rules impose unrealistic and prescriptive requirements on ISPs, which would impede ISPs' ability to respond with adequate flexibility to changes in the online threat environment. Finally, the Proposed Rules regarding data breach notification would hamper companies' responses to breaches and create customer confusion.

All of these problems are compounded by two proposals that broaden the scope of the Proposed Rules: the unlawful and unwarranted coverage of customer data beyond CPNI, discussed at length above,[302] and the definition of "customer," which would include not just current subscribers, as the voice CPNI rules do, but also applicants and former subscribers.[303] The NPRM speculates, but offers no evidence, that absent restrictions on the use of applicant information, prospective customers *may* be reluctant to apply for or switch services. The proposed definition would needlessly complicate ISPs' abilities to sign up prospective subscribers, and would create cumbersome requirements that would confuse and annoy current and prospective customers.

CTIA and other trade associations have encouraged the Commission to adopt an approach to privacy and data security for CPNI that is flexible, harmonized with the well-established and successful FTC unfair and deceptive acts or practices framework, and backed up by strong but fair

[302] *See* supra Part I.C.2.

[303] *NPRM*, 31 FCC Rcd at 2512 ¶ 31.

enforcement.[304] The FTC's well-tested consumer protection approach is consistent with the Commission's privacy recommendations in the 2010 National Broadband Plan, the 2012 *White House Framework*, the *2014 White House Privacy Reports* and 2015 Draft Consumer Privacy Bill of Rights Act, and Chairman Wheeler's 2015 testimony before Congress acknowledging the importance of coordination with the FTC and harmonization with its privacy framework.[305]

The industry consensus framework relies on two key principles derived from FTC enforcement actions and the *FTC Report*: (1) data should be protected based on its sensitivity, and (2) rules should be flexible to allow for changing technology and consumer expectations. The Commission likewise should use data sensitivity and flexibility as its touchstones so that its rules for notice, choice, data security and data breach notification will meet consumer expectations, avoid consumer confusion, and minimize other harms associated with disparate privacy regulation across the ecosystem.

First, any privacy rules that the Commission promulgates should protect data based on their sensitivity, and not on the type of entity using the data or the type of product or services being marketed.[306] As the FTC explained, while the misuse of sensitive data can increase the

---

[304] *See supra* note 7; Ex. A.

[305] *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"); White House, *Administration Discussion Draft Consumer Privacy Bill of Rights* (2015), https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf; Executive Office of the President, President's Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective* (2014) ("*White House Technology Privacy Report*"), https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf; Executive Office of the President, *Big Data: Seizing Opportunities and Preserving Values* (2014) ("*White House Privacy Report*") (collectively "*White House Privacy Reports*"), https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf ; *2012 White House Framework*; *FTC Report* at 26-28; FCC, *Connecting America: The National Broadband Plan* xii, 53-58 (2010), https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf.

[306] *See infra* Part V.B.1 (discussing consensus approach to privacy regulation in, among other things, *FTC Report*, *White House Privacy Reports*, and EU General Data Protection Regulation).

likelihood of "embarrassment, discrimination, or other harms" there are fewer privacy risks associated with the use of non-sensitive data (*i.e.*, data other than Social Security number or financial, health, children's, or precise geolocation information).[307] Therefore, companies should have fewer regulatory obligations when they provide notice and choice regarding non-sensitive information. Moreover, companies should be able to infer consent to use non-sensitive data for first-party marketing and other routine practices. Data sensitivity is an important factor in data security, as well. Indeed, data security programs should be designed to focus more resources on protecting sensitive data. Likewise, most state data breach notification laws are triggered by a likelihood of harm to consumers, which is generally tied to the sensitivity of the data at issue. By tying its rules to the sensitivity of the data, the Commission will ensure that they align with consumer expectations and what consumers know to be fair.

Second, it is essential that the Commission provide for flexibility in its rules. The Commission should identify privacy or security *goals* and give providers flexibility to achieve those goals, rather than dictating particular *methods* for providers. Prescriptive rules quickly become outdated and would prevent ISPs from implementing and updating their practices in ways that meet the privacy and security needs of their customers and address changing developments in this space.

[307] *FTC Report* at 47.

IV. The NPRM Approach to Notice of Privacy Policies Degrades the Customer Experience, Fails to Protect Privacy, and Imposes Substantial Costs.

A. There Is No Need for Expanded Notice Requirements Related to Privacy Policies and Changes Thereto.

The Proposed Rules would impose new requirements on ISPs regarding the type of notice that they must provide concerning their privacy policies and changes thereto ("Proposed Notice Rules"). In addition, the NPRM seeks information about whether to impose additional requirements related to the timing, content, placement, and frequency of such notices. The Commission's Proposed Notice Rules are unnecessary, unduly burdensome, and contrary to well-established industry practices that work well and that consumers have come to expect. Moreover, any additional requirements related to the timing, content, placement or frequency of such notices would degrade customers' experience and risk harming, rather than protecting customers.

Current industry practice with respect to the publication and notice of privacy policies ensures that consumers have access to timely, accurate, and useful information about ISPs' handling of their customers' information. Specifically, ISPs already publish privacy policies, providing their customers with significant information about their data practices, including a description of the type of information they collect, how they use it, with whom (and under what circumstances) they share it, and so forth.[308] Consumers are well aware that providers they interact with in the broadband ecosystem, including ISPs, publish privacy policies describing these practices.

[308] *See* privacy policies cited, *infra*, note 337.

To satisfy consumer expectations and market demand, as well as to comply with the FTC's privacy framework, industry self-regulatory codes,[309] and various state laws,[310] ISPs have developed effective privacy policies and notices of material change. Indeed, in addition to discussing privacy policies generally, the FTC's *Privacy Report* discusses the unique issues affecting wireless providers, and a subsequent mobile-specific privacy report that the FTC issued recommends flexible best practices for wireless providers to implement in the mobile environment.[311] Wireless providers have benefited from the FTC's guidance in this area and indeed have urged the Commission to model its approach to this rulemaking on the FTC's framework.[312] Moreover, prior to the Commission's reclassification of broadband service in the *Open Internet Order*, the threat of an FTC enforcement action served as a backstop to ensure that ISPs would implement and adhere to their privacy policies.[313]

The Proposed Notice Rules, however, would undermine the careful calibration that ISPs undertake in providing notice to customers while ensuring uninterrupted service and a positive user experience. ISPs must ensure customer awareness, without creating consumer confusion

---

[309] For example, the Digital Advertising Alliance ("DAA") has adopted self-regulatory codes of conduct that serve consumers well. Members of the DAA must provide their customers with notice of their privacy practices. *See* Digital Advertising Alliance, Self-Regulatory Principles for Online Behavioral Advertising (July 2009), http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf.

[310] *See, e.g.*, Cal. Bus. & Prof. Code § 22575; *see also* National Conference of State Legislatures, *State Laws Related to Internet Privacy* (Jan. 5, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx ("At least 17 states require government Web sites or state portals to establish privacy policies and procedures, or to incorporate machine-readable privacy policies into their Web sites.").

[311] *See FTC Report* at 63-64; *see also* FTC, *Mobile Privacy Disclosures* 13-14 (2013), *available at* https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf ("The recommendations are intended to be sufficiently flexible to accommodate further innovation and change."); *id.* at 13 n.65 (discussing business models of various types of entities in the ecosystem, including platforms, hardware manufacturers, wireless carriers, and chip manufacturers, and the attendant need to create a framework that allows practices "to evolve").

[312] *NPRM*, 31 FCC Rcd at 2589-90 ¶¶ 280-282.

[313] *See* 15 U.S.C. § 45.

and frustration. Far from informing and empowering consumers, however, the Proposed Notice Rules could require frequent and intrusive notices to consumers, increasing the risk that customers will experience notice fatigue and possibly fail to appreciate the most important notices that impact customer privacy. These predictions are not mere speculation; they find support from scientific studies, which demonstrate that consumers are not served by expansive, untimely, and repetitious privacy notices.[314] Further, data from Europe suggest that providing customers with frequent notices results in customer annoyance and may even deter customers from visiting certain websites.[315]

The Commission thus risks imposing rules that would conflict with its policy goals: requiring carriers to provide extensive, untimely, and repetitious notices would frustrate, rather than advance, the interests of protecting and empowering consumers.[316] Indeed, under the Commission's Proposed Rules, ISPs would have to provide an overwhelming number of notices, even to document small, immaterial changes to privacy policies—risking a "boy who cried wolf"

---

[314] *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S J. L. & Pol'y for the Info. Soc'y 543 (2008) (calculating the high costs of time spent reading privacy notices and suggesting that both the frequency and length of privacy policies are problematic); *cf.* Edith Ramirez, Chairwoman, FTC, *Privacy and the IoT: Navigating Policy Issues* 7, Opening Remarks at International Consumer Electronics Show (Jan. 6, 2015), https://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf (noting that "we risk inundating consumers with too many choices," and advocating a simplified approach); FTC, *Mobile Privacy Disclosures: Building Trust Through Transparency* 18 (Feb. 2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf (noting that the importance of ensuring that information does not become "too complex to be useful to consumers").

[315] *See* Ronald E. Leenes & Eleni Kosta, *Taming the Cookie Monster with Dutch Law—A Tale of Regulatory Failure*, 31 Comp. L. & Sec. Rev. 317, 317 (2015) (describing a Dutch cookie regulation as resulting in "widespread deployment of annoying banners, popup screens, and 'cookie walls'" and amounting to "regulatory failure"); James Hayes, *Cookie Law—Will It Rumble or Crumble?*, Engineering & Technology (Aug. 21, 2012), http://eandt.theiet.org/magazine/2012/08/cookie-law.cfm (noting that the cookie law "may actively deter [people] from 'entering' online stores, or make them suspicious of otherwise legitimate sites").

[316] *Cf. Verizon Nw.t, Inc. v. Showalter*, 282 F. Supp. 2d 1187, 1193 (W.D. Wash. 2003) (holding that Washington state privacy regulations were so "unnecessarily complicated" that they failed to materially advance the state's interest in privacy protection (internal quotation marks omitted)).

response. And for reasons explained below, widespread "notice fatigue" also risks compromising the Commission's goal of increasing broadband adoption and use.

In addition to confusing and frustrating consumers, the Proposed Notice Rules also create complications for ISPs, which already must comply with overlapping self-regulatory and legal requirements governing publication of privacy policies and notice of changes thereto.[317] The proposed additional layer of regulation will generate substantial compliance and other administrative costs, which may ultimately be passed on to consumers as part of the cost of service. This is a separate and fully independent reason that the Proposed Rules could undermine not only the Commission's goal of increasing privacy protection for consumers, but also its goal of increasing broadband adoption.

B. If the Commission Nevertheless Adopts the Proposed Notice Rules, It Should Implement the Following Modifications to Preserve ISP Flexibility.

CTIA urges the Commission not to adopt the Proposed Notice Rules. Nonetheless, CTIA respectfully submits that should the Commission adopt rules regarding privacy policies and changes, it should consider including the following modifications, which are in the public interest.

First, with respect to the "time and place" of notice, the Commission should allow ISPs to provide notice within the governing customer agreement or privacy policy; notice should not be required through a stand-alone document. Periodic updates to customers regarding privacy practices are unnecessary and counterproductive. Indeed, it is precisely such notices that present the greatest risk of desensitizing customers. Instead, CTIA urges the Commission to allow ISPs

[317] *See supra* notes 309-310 and accompanying text.

to make privacy policies and updates available via links on ISPs' websites.[318] In addition (or in the alternative), CTIA urges the Commission to allow ISPs to provide notices electronically. Any broadband customer, by definition, has the capacity to receive electronic notifications.

Second, under no circumstances should the Commission require ISPs to standardize their privacy policies or notices of changes to such policies.[319] ISPs have a wide range of business models and offer different types of service. Some ISPs choose to include in a single policy an explanation of the privacy policies applicable to the full suite of services that they offer. These ISPs need the flexibility to provide comprehensive policies, which benefit consumers by providing all of the necessary information in one place and in a format that best suits the nature of the information the ISP seeks to convey. It would be infeasible to require these ISPs to shoehorn descriptions of different data practices, involving different services and offers, into the same standardized form. A nutrition label model, or any one-size-fits all approach, would not work for all ISPs. Such forms often prevent companies from determining the best way to explain products and services to consumers. For example, the Gramm-Leach-Bliley Act has a model privacy notice form that offers a safe harbor to regulated entities, but many companies have chosen not to use it, determining that the benefits of the safe harbor are offset by the form's rigidity.[320] Likewise, the 2010 Open Internet Order's requirement for standardized notices

[318] *NPRM*, 31 FCC Rcd at 2528-29, 2533-34 ¶¶ 83, 96.

[319] *NPRM*, 31 FCC Rcd at 2528-29, 2533-34 ¶¶ 83, 96.

[320] *See* Letter from Scott Talbott, Senior Vice President for Government Affairs, Electronic Transaction Association, to Monica Jackson, Office of the Executive Secretary, Consumer Financial Protection Bureau, *Amendment to the Annual Privacy Notice Requirement Under the Gramm-Leach-Bliley Act (Regulation P)*, Docket No. CFPB-2014-0010, RIN 3170-AA39 (July 14, 2014), https://www.regulations.gov/#!documentDetail;D=CFPB-2014-0010-0104. For example, the safe-harbor form is geared towards some types of financial institutions and not others, and prevents companies from providing clearer and more transparent notices.

regarding technical data[321] actually led to cumbersome and inaccessible notices, which customers rarely, if ever read. The Commission should not pursue this path again.

The obverse point is equally compelling: in the absence of a substantial, record-based need for uniform practice, providing ISPs with flexibility to publish privacy policies and notices of changes thereto is in the public interest. Flexible rules will facilitate ISP innovation and tailoring to benefit consumers as the marketplace and technology evolve. For instance, ISPs should be able to report general categories of data-sharing partners, rather than listing each and every affiliate, vendor, or contractor with whom the ISP works.[322] Similarly, ISPs should be able to report the types of information collected; uses of information; and consumer information choices in general terms that are intelligible to consumers and that can be adapted as consumer understanding of data practices changes. Moreover, limiting the form of ISPs' notices threatens to tread on First Amendment principles. In particular, ISPs should have the ability to offer customers a clear explanation of the trade-offs at stake in the privacy context. This should be true in initial notices and in notices of material changes to privacy practices.

The Commission further highlights the need for flexibility by noting that a wide range of "Mobile-Specific" considerations might augur in favor of allowing mobile ISPs to deliver privacy policies and notices in a different manner from other ISPs.[323] Rather than trying meticulously to define these considerations and to implement different, corresponding rules—an

---

[321] *2010 Open Internet Order*, 25 FCC Rcd at 17,937 ¶ 54.

[322] This would be consistent with the approach taken under California law. *See, e.g.*, Cal. Bus. & Prof. Code § 22575(b)(1) ("The privacy policy required" of commercial website operators and online service providers that collect personally identifiable information about consumers residing in California shall, among other things "[i]dentify the *categories* of personally identifiable information that the operator collects . . . and the *categories* of third-party persons or entities with whom the operator may share that personally identifiable information." (emphases added)).

[323] *See NPRM*, 31 FCC Rcd at 2536 ¶ 102.

endeavor that, even if feasible, would produce rules that would quickly become obsolete in any event—the Commission would be better served by not imposing a rigid notice requirement at all.[324] Instead, as the FTC has recognized is appropriate, especially in the mobile broadband ecosystem, the Commission should provide ISPs with flexibility to deliver notices to customers in whatever ways best serve the customer given the state of technology at any given time.

Additionally, if the Commission adopts a standard form, it should, at the very least, not *require* use of that form, but instead offer safe harbor protections for ISPs that use it.[325] Furthermore, for the reasons stated above, any standard form should allow *some* variation and flexibility in wording. Otherwise, the form would risk becoming obsolete and irrelevant.[326]

Third and relatedly, the specific prescriptions that the Commission seeks comment on are unworkable, unnecessary, or otherwise undesirable. As noted, the final rules instead should provide flexibility to ISPs, as long as their notices are comprehensible, legible, and make privacy practices readily apparent.[327] For example, the Commission should not require "layered privacy" policies or notices.[328] Even if layering could be useful to consumers in some contexts, it may not make sense in every instance and could become outdated.

Likewise, a requirement that ISPs provide dashboards (either to provide notice or obtain approval) would result in customer confusion and increased costs for ISPs.[329] Record evidence

---

[324] *See supra* note 311.

[325] *Cf. Open Internet Order*, 30 FCC Rcd at 5669-70, 5679-81 ¶¶ 156, 176-181; *Consumer and Governmental Affairs, Wireline Competition, and Wireless Telecommunications Bureaus Approve Open Internet Broadband Consumer Labels*, Public Notice, GN Docket No. 14-28, DA 16-357 (Apr. 4, 2016).

[326] *See supra* note 320.

[327] *See NPRM*, 31 FCC Rcd at 2528-29 ¶ 83.

[328] *See id.* at 2532 ¶ 94.

[329] *See id.* at 2533, 2551 ¶¶ 95, 144.

directly contradicts that customers prefer or would adopt such an interface.[330] Dashboards also are onerous, as they fail to accommodate new business models and web and mobile interfaces. Indeed, technology changes rapidly, and five years from now, a dashboard may seem as outdated as notices coming in the form of paper mailings. This is especially so given the rapid development and deployment of new mobile devices and the Internet of Things, which may render any dashboards developed now soon obsolete. Additionally, dashboards that enable customers to (i) correct their PII and (ii) opt in and out of information-sharing programs would be costly to build, because they involve complex interfaces to allow customer access to information, while also ensuring system security, and their adoption would impose personnel and management costs for ongoing operation. As will be discussed at greater length below, dashboards also can create a security risk and invite attack.[331]

The Commission should not require ISPs, whether through a dashboard or otherwise, to provide information to customers regarding the "categories of entities with whom . . . customer [proprietary information] is shared,"[332]—especially at any level of granularity. ISPs may enter into agreements with third-party agents, independent contractors, and other entities for a variety of different purposes, ranging from one-off transactions to repeat interactions. The proposal could deter some third parties from working with ISPs in the future.[333] Additionally, the very existence or nature of those relationships may involve or implicate sensitive competitive

---

[330] *See id.* at 2533 ¶ 95 n.168 ("Similar dashboards have been voluntarily adopted by online advertising networks; however, their adoption by consumers has been limited, perhaps due to a lack of visibility."). In the NPRM, the Commission cites the *White House Privacy Report* for this proposition, but the *White House Privacy Report* is also consistent with the notion that "privacy fatigue" may make such dashboards unattractive to consumers. *See White House Privacy Report* at 42.

[331] *See infra* Part VI.A.2.a.

[332] *See NPRM*, 31 FCC Rcd at 2533 ¶ 95.

[333] *Cf., e.g., John Doe No. 1 v. Reed*, 130 S. Ct. 2811, 2818 (2010) (explaining that forced disclosure can chill association in First Amendment context).

information. The rules therefore could harm competition. After all, edge providers also disclose customer information to third parties and allow third parties to access such information, and yet, with the exception of specific statutes that apply to all providers notwithstanding the classification of broadband service as a telecommunications service (*e.g.*, COPPA),[334] edge providers now face a very different disclosure regime under the FTC. At the very least, if this proposal is adopted, the Commission should include language clarifying that "categories" refers to broad groups (*e.g.*, suppliers, service providers, etc.) that companies can define by accounting for their own business practices.

V. The NPRM Approaches to Customer Choice Ignore Realities of the Broadband Ecosystem and Are Inconsistent with Established Privacy Regulation, Rendering Them Ineffective and Counterproductive.

The NPRM's approach to customer choice is fundamentally flawed. As described above, the Proposed Rules impose graduated consent requirements on uses of "customer proprietary information" based on the nature of the product or service an ISP is marketing, or whether the ISP is disclosing or permitting access to "customer proprietary information." For many of the same reasons that these restrictions fail at the tailoring level of the First Amendment analysis, they are likewise unreasonable as a matter of policy.

At the outset, the Commission has started from a set of incorrect assumptions about the status quo—*viz.* (1) that ISPs currently provide their customers with no choice protections; (2) that privacy-conscious customers are incapable of (or unsatisfied with) opting out of certain practices, even when presented with the opportunity; (3) that edge providers lack the capability of ISPs to obtain, use, disclose, and permit access to customer information; and (4) that the market for mobile broadband lacks competition and involves high customer switching costs. In

[334] *See* privacy laws cited, *supra*, note 78.

fact, none of these assumptions can withstand scrutiny, leaving the Proposed Rules a solution in need of a problem.

Equally problematic is that the Commission's approach to protecting privacy paradoxically lacks any connection to established privacy concerns: distinguishing between uses of information based on the product or service being marketed reflects neither heightened privacy risk nor customer expectations. The alternative proposals on which the Commission seeks comment fare no better. Neither do the rules proposed in the NPRM to implement the exceptions to Section 222. Specifically, the proposed exceptions need to allow ISPs to use and disclose "customer proprietary information" for beneficial data management and cybersecurity purposes and to defend against and respond to frauds and threats. Finally, overlaid on top of this framework are requirements that ISPs adopt costly, inefficient, and frustrating methods of communicating with customers, which, along with the enhanced requirements for opt-in or even opt-out consent, will degrade the user experience. These flaws suggest not only that the Proposed Rules are not in the public interest, but also that the Commission must reconsider its approach completely as this process continues, in order to satisfy the requirements of the APA.

A. The NPRM Starts from an Improper Baseline Assumption About the Use and Disclosure of, and Access to, Information in the Broadband Ecosystem.

The NPRM is based on two fundamental misunderstandings regarding the uses of customer information by entities in the broadband ecosystem. The Commission's failure properly to frame the problem would jeopardize any final rules adopted.[335]

[335] *See, e.g., Comcast Corp. v. FCC*, 579 F.3d 1, 8 (D.C. Cir. 2009) (invalidating agency rules due to Commission's failure to consider operations of other entities in the market).

1. The NPRM Incorrectly Assumes That Broadband Customers Currently Receive No Choice, and That Opt-In Approval Is the Only Effective Remedy.

The Commission appears to be starting from the premise that ISPs currently offer no choice mechanisms to their customers. In fact, customers already are protected by a variety of state laws,[336] industry self-regulatory regimes, case-by-case enforcement by the Commission, and other market forces. Indeed, ISPs long have successfully protected consumers' privacy through robust choice mechanisms under this framework,[337] with federal and state enforcement as the backstop. Moreover, the fact that the FTC no longer has jurisdiction to take enforcement action against ISPs cannot be a basis for adopting the Proposed Rules, both because that jurisdictional outcome is a problem of the Commission's own making, and because, to the extent there is a need to develop gap-filling regulations, the Commission easily could adopt rules consistent with the FTC's regulatory framework under Section 5 of the Federal Trade Commission Act to govern ISPs' provision of telecommunications service. CTIA has urged the Commission to do exactly that.[338]

---

[336] *See, e.g.*, Cal. Fin. Code §§ 4050-4060.

[337] *See, e.g.*, AT&T, *AT&T Privacy Policy*, https://www.att.com/gen/privacy-policy?pid=2506 (last visited May 2, 2016) ("We will not sell your personal information to anyone, for any purpose. Period. . . . You have choices about how AT&T uses your information for marketing purposes. Customers are in control."); Verizon, *Privacy Policy*, http://www.verizon.com/about/privacy/privacy-policy-summary (last visited May 2, 2016) ("Verizon does not sell, license or share information that individually identifies our customers with others outside of Verizon who are not doing work on Verizon's behalf without your consent."); Sprint, *Legal/Regulatory & Consumer Resources, Privacy Policy* (May 2, 2014), https://www.sprint.com/legal/privacy.html ("We do not share information that identifies you personally with third parties other than as follows: . . . Third Parties with Your Consent. We may share information with other third parties with your consent. For example, you may agree to our sharing your information with other third parties to hear about their products and services. Use of the information you agree to share will be subject to those third parties' separate privacy policies."); T-Mobile, *T-Mobile Privacy Policy Highlights* (Nov. 25, 2015), http://www.t-mobile.com/company/website/privacypolicy.aspx ("We do not sell, license, rent, or otherwise provide your Personal Information to unaffiliated third-parties (parties outside the T-Mobile corporate family) to market their services or products to you without your consent.").

[338] *NPRM*, 31 FCC Rcd at 2589-90 ¶¶ 280-282; Ex. A. In their comments, Thomas Lenard and Scott Wallsten of the Technology Policy Institute likewise argue that the "key question" to answer before the Commission adopts rules that are stricter than those the FTC has applied under its jurisdiction is whether the rules would "yield net incremental benefits"; as Lenard and Wallsten note, the NPRM does not even pose, let alone answer, this question.

Against this backdrop, the Commission has the burden to justify imposing any incrementally greater choice protections than those afforded by the FTC's regime. The NPRM misses this mark. For example, the NPRM states that "customers may object . . . to uses of [their] information for unexpected purposes, such as marketing wholly unrelated services to the customer."[339] Even if true, which, as discussed at greater length below, is unlikely, this is a non-sequitor; it does not address the relevant question, which is whether customers' "object[ions]" to such use require opt-in approval. Indeed, the very use of the phrase "customers *may* object"—not "customers do object" or "customers often object"—suggests that an opt-out approach more closely accords with customer expectations.[340] Likewise, the statement that "customers desire and expect the opportunity to affirmatively choose how their information is used for purposes other than marketing communications-related services by their provider and its affiliates,"[341] even if true, does not support requiring opt-in approval for such marketing. Opting out also entails a "[choice]" by the customer "affirmatively" not to permit certain use, disclosure, and access, and would be stricter than the FTC's current implied-consent approach to most first-party marketing. This approach also would fare better under First Amendment scrutiny.

See Lenard & Wallsten Comments at 3; *see also Leibowitz Comments* at 3 (urging Commission to "take the time necessary to carefully evaluate how [Proposed Rules] would affect business practices, especially where they are in contrast with how those business practices would be treated under the FTC framework" and urging that a "truly consistent approach is vital for the continued growth and economic benefits of the Internet" and "to avoid consumer confusion and misunderstanding").

[339] *NPRM*, 31 FCC Rcd at 2539 ¶ 109.

[340] As set forth more fully below, many consumers would prefer an opt-out regime focused on misuses of sensitive data over a confusing patchwork of opt-in and opt-out requirements that apply depending entirely on the jurisdiction of the agency overseeing the entity providing the relevant service and that generate frequent and lengthy notifications.

[341] *NPRM*, 31 FCC Rcd at 2544-45 ¶ 127.

2. The NPRM Uncritically Extends the Voice CPNI Model, Ignoring Differences Between the Broadband and Traditional Voice Ecosystems That Undermine the Rules.

As discussed above, Congress enacted Section 222 to address harms unique to what once was a closed telecommunications market: the carrier, by virtue of providing service, obtains information from the customer that is valuable to the carrier and that the customer does not otherwise share, and, accordingly, uses of that information implicate the customer's privacy interests and the carrier's competitive interests. In this closed system, it can make sense to impose restrictions on uses, disclosures, and access to customer information on the theory that "once confidential customer information enters the stream of commerce, consumers are without meaningful recourse to limit further access to, or disclosure of, that personal information."[342]

It is entirely another matter, however, to purport to protect privacy by imposing restrictions on information use, disclosure, and access by certain entities in an open ecosystem like the Internet—and yet that is precisely what the NPRM does. The openness of the broadband ecosystem is a fundamental principle—and, indeed, an express priority—of the Commission's *Open Internet Order*.[343] And in reality, many other entities in the ecosystem (including operating systems, browsers, mail platforms, social networks, search engines, and advertising networks) have access to *the same* information as ISPs,[344] and are engaging in various uses and disclosures under regulation by the FTC. Given these realities, it is fatally flawed to assume that

[342] *Id.* at 2545-46 ¶ 129 (internal quotation marks omitted). Certain assumptions and factual findings that justified imposing the current CPNI rules no longer hold in the context of the current voice marketplace, where over-the-top ("OTT") and other services have resulted in increased competition and openness. Whether Section 222's prohibitions on first-party marketing by voice providers remain facially constitutional given these evolving circumstances is better reserved for another proceeding. *See infra* Part V.A.3.

[343] *See, e.g.*, *Open Internet Order*, 30 FCC Rcd at 5877-78 ¶ 569 (explaining that general conduct rule merely "regulate[s] broadband providers' conduct with respect to traffic which currently freely flows over their facilities").

[344] In this respect, too, the Commission misses the mark by claiming that edge providers may have access to "some similar customer [proprietary information]." *NPRM*, 31 FCC Rcd at 2546 ¶ 132. As discussed, there is no basis to think that there is any difference in the information assets of ISPs and edge providers.

the Proposed Rules could keep *any customer information* (whether PII, novel and extra-statutory categories of broadband CPNI, or "customer proprietary information") from entering the stream of commerce by regulating only ISPs. The Commission even appears to acknowledge toward the end of the NPRM that the only way to make such a regime effective would be to deputize ISPs to police edge providers under a framework that otherwise would exceed the Commission's jurisdiction.[345] The NPRM also seeks to get around this problem by identifying certain "mitigat[ing] factors,"[346] but these factors are insufficient to justify discriminatory treatment of ISPs.

The NPRM notes that the FTC "actively enforces the prohibitions in its statute against unfair and deceptive practices against companies in the broadband ecosystem that are within its jurisdiction" and that the FTC "will continue its robust privacy enforcement practice."[347] This statement, far from supporting the Proposed Rules, actually shows a double bind: (1) If the FTC regime is adequate for companies that collect, use, and share *more* personal data in some cases than ISPs, then, as CTIA has proposed, the Commission should adopt the FTC framework whole cloth for ISPs; (2) If, on the other hand, the FTC regime is somehow insufficient, then the open nature of the ecosystem will make the overly restrictive ISP-specific rules ineffective to protect customers who interact online with countless other entities who will have access to the same information.

---

[345] *See NPRM*, 31 FCC Rcd at 2570 ¶¶ 212-213 ("[W]e seek comment on whether we should require [ISPs] to use their contractual relationship with mobile device or mobile operating system (OS) manufacturers that manufacture the devices and hardware that operate on the mobile [ISP's] network to obtain . . . contractual commitments" "[to safeguard . . . data prior to disclosing customer [proprietary information] to . . . third parties."). The answer is no.

[346] *See NPRM*, 31 FCC Rcd at 2546-47 ¶ 132.

[347] *Id.*

The Commission next states that "the industry has developed guidelines recommending obtaining express consent before sharing some sensitive information, particularly geo-location information, with third parties," and that "large edge providers are increasingly adopting opt-in regimes for sharing some types of sensitive information."[348] It is surprising that the NPRM does not examine these "guidelines" and "regimes" more critically. Many requests for "express consent" from search engines, apps, and social networks are actually the routine take-it-or-leave-it offers that are common in the American economy and that the NPRM otherwise characterizes as not affording meaningful choice.[349] Moreover, the Commission's discussion of these "regimes" underscores the argument, discussed below, that the extent of protection afforded should depend on the sensitivity of the data, not the nature of the services to be marketed. And finally, ISPs *also* have adopted similar voluntary guidelines and regimes. As just one example, CTIA has published Best Practices and Guidelines to promote and protect user privacy with respect to geolocation privacy risks. Based on well-established notice and consent principles, these guidelines require a location-based service provider to bear the burden of demonstrating customer consent to use or disclosure of location information.[350] To the extent that the Commission credits the efficacy of such programs for other providers, it should do so for ISPs as well.

---

[348] *Id.*

[349] *See supra* note 126.

[350] *See Best Practices and Guidelines for Location-Based Services*, CTIA (Mar. 2010), http://www.ctia.org/docs/default-source/default-document-library/pdf-version.pdf?sfvrsn=0. In the past, the Commission has expressly declined to adopt rules "to implement the wireless location information privacy amendments to Section 222," recognizing that the better course was "vigorously" to "enforce the law as written, without further clarification of the statutory provisions," given existing industry self-regulation and the "still-developing market for location-based services." *See In re Request by* [*CTIA*] *to Commence Rulemaking to Establish Fair Location Information Practices*, Order, 17 FCC Rcd 14,832, 14,832, 14,835 ¶¶ 1, 8 (2002).

The next purported fact on which the Commission relies is that that "edge providers only have direct access to the information that customers choose to share with them," whereas ISPs "have direct access to potentially *all* customer information, including such information that is not directed at the broadband provider itself to enable use of the service."[351] This distinction is both factually untrue and a red herring. Underlying it are misplaced assumptions about current privacy practices and tracking capabilities, as well as the state of competition and switching costs in different service markets.

First, the NPRM underestimates the amount of information that edge providers—operating systems, content platforms, and non-consumer-facing parties—track, obtain, and sell. Operating systems have access to all or almost all consumer online activity, and operating systems on mobile devices also have access to stored data, like contacts, music files, calls logs, as well as audio recordings, photos, and videos made using the microphone and camera on the device.[352] There are entities in the ecosystem—most prominently, Facebook and Google—that functionally have visibility into the same information as ISPs, through their search functions and by using plug-ins on third-party websites that consumers visit.[353] Likewise, virtually every web page that a consumer visits is serviced by a wide variety of other providers that use cookies and other methods to collect information about the user. Consumers often have little visibility into these collection practices or the third-party provider collecting their data, such that it is

[351] *NPRM*, 31 FCC Rcd at 2546-47 ¶ 132 (footnote omitted).

[352] *Swire Report* at 65-80; *FTC Report* at 56.

[353] *Swire Report* at 43-57; *see also, e.g.*, Tom Simonite, *Largest Study of Online Tracking Proves Google Really Is Watching All of Us*, MIT Technology Review Online (May 18, 2016), https://www.technologyreview.com/s/601488/largest-study-of-online-tracking-proves-google-really-is-watching-us-all/.

inaccurate to say that consumers "choose" to share data with these providers. At best, such collection practices are described in websites' privacy policies.

In contrast, however, ISPs' visibility into information is often limited and is decreasing. This phenomenon is occurring in part because each customer is now connecting to the Internet throughout the day, from a variety of locations and using a variety of devices, which receive service from different ISPs and Wi-Fi providers.[354] For many data users, then, there is not a single ISP capable of seeing all of their online activity. Further limiting ISP visibility is the widespread and increasing use of encryption by the most frequently visited websites, which wholly deprives ISPs of access to any payload information. Moreover, the use of virtual private networks ("VPNs") will further reduce ISPs' ability to collect—let alone use, disclose, or share—certain types of "customer proprietary information."[355]

Second, the NPRM makes passing reference to a purported lack of competition among broadband providers.[356] But, at the very least, there is substantial competition among *wireless* ISPs, and wireless broadband accounts for an increasing percentage of overall usage.[357] In

---

[354] *Swire Report* at 7 ("In the 1990s, a typical user accessed the Internet from a single, stationary home destktop connected by a single ISP. Today, in contrast, the average Internet user has 6.1 connected devices, many of which are mobile and connect from diverse and changing locations that are served by multiple ISPs. By 2014, 46 percent of mobile data traffic was offloaded to WiFi networks, and that figure will grow to 60 percent by 2020. Any one ISP today is therefore the conduit only for a fraction of a typical user's online activity."); *see also Lenard & Wallsten Comments* at 17 (describing that vast majority of Internet users connect via multiple connections over the course of the day, including "a home fixed connection, a mobile cellular network, various WiFi networks, and a work or school connection all the while logged in to the same email account, using the same e-commerce sites, and exploring the world with the same search engine").

[355] *Swire Report* at 23-35; *see also Lenard & Wallsten Comments* at 3 (explaining that encryption prevents ISP access to information, especially to sensitive financial and health information); *see also id.* at 14-16 (discussing increasing use of encryption, especially among companies with access to the most sensitive data); *Leibowitz Comments* at 7 (emphasizing that FTC did not single out ISPs for unique treatment, and describing the "sea change" resulting from the "precipitous rise of encryption and proliferation of networks and devices" which "have limited the scope of customer data available to [ISPs]" since publication of the *FTC Report*).

[356] *See NPRM*, 31 FCC Rcd at 2545-47 ¶¶ 128, 132.

[357] *See, e.g.*, *Eighteenth Report*, 30 FCC Rcd 14,515; CTIA, *The Wireless Difference* (Feb. 10, 2015); *In re Protecting and Promoting the Open Internet*, Comments of CTIA 5-11, GN Docket No. 14-28 (July 18, 2014);

contrast, however, in other service markets that comprise the broadband ecosystem, there is virtually no competition. For example, the market for operating systems comprises only two widely available providers (Android and iOS). In the online search market, one provider (Google) has more than 65% market share.[358] And in the social networking market, Facebook has approximately 44% market share,[359] as well as substantial other legacy advantages.

Third, the NPRM rests on a mistaken assumption about the switching costs that customers face in different service markets.[360] Here too, in the market for *wireless* broadband, providers are adopting practices that actually drive down switching costs—*e.g.*, they are moving away from term-contracts with cancellation penalties, and offering to pay switching costs for new customers.[361] And likewise, here too, the switching costs for consumers of other entities in the ecosystem are dramatically higher. For example, porting allows a customer to keep his or her number when changing providers, but e-mail users cannot keep their domain names when they switch providers. Similarly, network effects as well as inertia make it extremely unlikely that any viable alternative to Facebook will emerge in the social networking market.[362] And it

---

accord Andres V. Lerner & Janusz A. Ordover, *The "Terminating Access Monopoly" Theory and the Provision of Broadband Internet Access* 6-14 (Jan. 14, 2015), https://www.verizon.com/about/sites/default/files/Terminating_Access_Monopoly_Theory_and_the_Provision_of_Broadband_Intern....pdf.

[358] *See* Net Market Share, *Realtime Web Analytics with No Sampling* (Mar. 2016), https://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0.

[359] *See* Statista, *Leading Social Media Websites in the United States in February 2016, Based on Share of Visits* (2016), http://www.statista.com/statistics/265773/market-share-of-the-most-popular-social-media-websites-in-the-us/. YouTube, owned by Alphabet, the parent of Google, owns the second largest share of the social network market with about 22%.

[360] *See NPRM*, 31 FCC Rcd at 2545-47 ¶¶ 128, 132.

[361] *See, e.g.*, Julian Chokkattu, *How to Avoid Early Termination Fees and Switch Phone Carriers Like a Pro*, Digital Trends (Jan. 24, 2016), http://www.digitaltrends.com/mobile/how-to-switch-phone-carriers/; Chris Smith, *How to switch cell phone carriers the easy way*, BGR (Dec. 8, 2015), http://bgr.com/2015/12/08/switch-carriers-att-sprint-t-mobile-verizon/.

[362] *See, e.g.*, Gal Zauberman, *The Intertemporal Dynamics of Consumer Lock-In*, 30 J. Consumer Res. 405, 408-09 (2003) (showing that initial investments in setup costs are sufficient to produce lock-in); David S. Evans & Richard

likewise is not practicable for customers to stop using operating systems—indeed it is more difficult for mobile broadband customers to switch operating systems than it is for them to switch carriers, because in the case of the former, they need to purchase a new device, transfer their data (which may be in a different format), and learn a new set of commands.[363]

Asymmetric regulation of entities in the Internet ecosystem is not just ineffective, however; it is also counterproductive. That is so, because the unique rules for ISPs risk generating customer confusion and frustration—an outcome that would undermine the Commission's purported privacy goals. For example, if customers are required to opt in to ISPs' use and disclosure of "customer proprietary information," they mistakenly could assume that, as a default matter, their data is also unobtainable to, or unusable by, other parties online. Additionally, requiring customers regularly to read new disclosures and frequently exercise their choice preferences also could engender notice fatigue, impeding customers' ability to focus on harmful uses of their data. Finally, requiring customers to provide opt-in consent for services that are currently provided on a basis of implied consent will degrade the customer experience, introducing new transaction costs into previously smooth interactions. Such feelings of futility have been shown to undermine efforts to encourage even privacy-conscious customers to protect their privacy across settings.[364]

Schmalensee, *The Industrial Organization of Markets with Two-Sided Platforms*, 3 Competition Pol'y Int'l 151, 164-65 (2007) (describing the positive-feedback effects associated with increasing network size); *see also* David S. Grewal, *Network Power: The Social Dynamics of Globalization* 17-43 (2008) (describing the way social network size operates to prevent switching even when features of alternative networks are more attractive on the merits).

[363] *See* Vindu Goel, *How to Switch to iPhone from Android: Patience and Persistence*, NYTimes (Apr. 6, 2016), http://www.nytimes.com/2016/04/07/technology/personaltech/how-to-switch-to-iphone-from-android-patience-and-persistence.html; Simon Hill, *Apple Detox*, DigitalTrends (June 4, 2015), http://www.digitaltrends.com/mobile/how-to-switch-from-iphone-to-android.

[364] Lauren E. Willis, *Why Not Privacy by Default*, 29 Berkeley Tech. L.J. 61, 79-80, 88, 90, 114 (2014).

3. Harmonizing Privacy Rules Governing Different Regulated Services Could Reduce ISP Costs, but Final Rules for Each Service Must Reflect Market Conditions.

The NPRM requests comment on whether the Commission should harmonize approval requirements for the use of customer information across telecommunications services and platforms.[365] As an initial matter, the benefits of harmonization should be extended beyond telecommunications services and platforms to include all players in the mobile ecosystem; that is precisely what the FTC attempted to do over the course of a two-year, rigorous process, and that is what industry has proposed here.[366] Nonetheless, CTIA appreciates the Commission's narrower request and agrees in principle that there may be significant advantages to harmonizing regulations to create the *right* regulatory framework for voice, broadband, and cable services—including both the delivery of an improved and simplified customer experience, and the realization of saved administrative costs.

Be that as it may, however, because the restrictions at issue implicate carriers' First Amendment rights, they must reflect market conditions for each service in order to be considered appropriately tailored to achieve a substantial state interest. And the voice market has changed dramatically since Section 222 was enacted: there are many new over-the-top voice providers (*e.g.*, FaceTime, Skype, and Google Hangouts) fostering competition that did not exist in 1996, and data associated with mobile voice services, like call logs, is now widely available to other entities, including operating systems and mobile apps. Likewise, as noted, there has been an evolution in privacy regimes toward a model of implied consent for virtually all first-party marketing. These changes augur in favor of harmonization based on the industry proposal, and

[365] *See NPRM*, 31 FCC Rcd at 2553 ¶¶ 152-153.

[366] *See supra* note 7; Ex. A.

in accordance with the FTC's regime, rather than adoption of stricter requirements for voice and cable services based on the instant NPRM.

Specifically, therefore, in response to the Commission's request for comments regarding harmonization,[367] CTIA advocates at a minimum that the Commission should update its existing voice rules to allow for all or nearly all first-party marketing to occur on a basis of implied consent; to permit flexible customer notices and not require explicit language that consumers do not understand; and to create one set of flexible data security and authentication rules. The Commission also should exclude from any regime the uses and disclosures of information from enterprise and other business customers, for whom the privacy interests underlying Section 222 are inapplicable.

If the Commission instead decides to harmonize the voice CPNI rules to match the Proposed Rules—or if the Commission elects not to harmonize rules for different services—CTIA urges the Commission to extend an existing carve out in the voice CPNI rules for CMRS providers to the Proposed Rules. Specifically, the existing voice CPNI rules allow wireless voice providers to "use, disclose, or permit access to CPNI derived from [their] provision of CMRS, without customer approval, for the provision of CPE and information service(s)."[368] It appears that the Proposed Rules (perhaps inadvertently) would require a wireless ISP to obtain opt-in approval for these same uses. Given that many wireless ISPs provide *both* broadband *and* CMRS service to the same customers—and have long been using this exception to deliver marketing for CPE and information services to those customers—it would frustrate customer expectations and cause considerable confusion if ISPs were abruptly required to request and

[367] *NPRM*, 31 FCC Rcd at 2527 ¶ 80.

[368] 47 C.F.R. § 64.2005(b)(1).

obtain opt-in approval to engage in this same marketing with respect to a customer's broadband service, but not their voice service.

Current practices under this exception also suggest that the Commission should exclude CPE and information services from the definition of broadband CPNI. A CMRS provider currently can use its knowledge of a customer's service to market a device, without approval, under this exception, and can use its knowledge of a customer's device to market accessories to the customer, without approval, because the customer's device is not considered CPNI. The Proposed Rules appear to require the same provider, on a going-forward basis, to obtain opt-in consent to market either the device or the accessories, notwithstanding that customers now expect providers to engage in both types of marketing—and that these practices have, to CTIA's knowledge, never been flagged by the Commission or consumer advocates as problematic.

B. The NPRM Choice Rules Lack Any Nexus to Privacy Concerns and Threaten Innovation, Competition, and Routine Business Operations.

The NPRM choice framework ignores established privacy-related concerns entirely. In its discussion of the choice rules, the NPRM adopts an approach to choice that does not accord with customer expectations; is based on the type of product or service an ISP markets, rather than the sensitivity of the data used or whether and to whom such data is disclosed; and ignores critical differences in third-party relationships, leading to absurd results. The alternative approaches on which the Commission seeks comment fare no better. Rather than doubling down on the Proposed Rules, the Commission would be better served by engaging in further analysis through an ongoing rulemaking process.

1. Under Effective Privacy Regimes, Heightened Protection Is Required Only for Heightened Risk.

Privacy regimes offer heightened protection either where there is deliberate collection and use of *sensitive* data (because such activities increase the privacy impact of unwanted

disclosure), or where information is shared with a third party for its own use or without adequate contractual control, (because such sharing can increase the probability of unwanted use and further disclosure). Put simply, in these regimes, the nature of the protection offered is based on the nature of the privacy risk (measured in terms of probability and impact).

The *FTC Report* is instructive. After spending two years conducting workshops and extensive meetings, and after receiving over 450 comments from industry and consumer groups—addressing subjects including the unique aspects of the online ecosystem, the costs and benefits of regulation, consumers' interests in privacy, and so forth—the FTC determined that the critical policy distinctions for purposes of consumer protection are (1) the nature of the data being collected and used (as well as the knowledge and intent of the provider), on the one hand; and (2) the sharing of data with unaffiliated third parties for their use and/or without appropriate controls, on the other hand.[369] The FTC concluded that companies "do not need to provide choice before collecting and using consumers' data for commonly accepted practices," including most first-party marketing.[370] Instead, in the ordinary course, not only is opt-in consent generally unnecessary for first-party marketing, but approval for such marketing generally is *implied*. In short, the FTC does not regulate first-party marketing based on the *type of entity* doing the marketing or the *type of product* being marketed, but rather on the *sensitivity of the data* or the lack of consumer control over the *sharing of the data*.[371]

---

[369] *See FTC Report* at i-ii (discussing FTC's comments and workshop process); *id.* at 40-41, 47-48 (discussing scenarios that require enhanced notice and/or choice). The *FTC Report* defines as sensitive, at a minimum, "data about children, financial and health information, Social Security numbers, and *certain* geolocation data." *Id.* at 47 (emphasis added).

[370] *Id.* at 36.

[371] *Id.* ; *see also Leibowitz Comments* at 8 (describing Commission's approach to first-party marketing by ISPs as a "baffling departure from FTC guidance" which "ignores the critical context of the interaction between the consumer and the service provider, which would make consumers the losers in this policy choice").

The FTC adopted this approach because "first-party collection and use of non-sensitive data (*e.g.*, data that [are] not a Social Security number or, financial, health, children's, or [precise] geolocation information) creates fewer privacy concerns than practices that involve sensitive data or sharing with third parties."[372] Indeed, while first-party collection and use of *sensitive* data can create privacy risks, these practices trigger different consent requirements *only* when a provider has knowledge of the sensitive nature of the information.[373] The FTC also noted that while first-party marketing generally does not require choice, certain practices, including tracking consumers across other parties' websites, may not be consistent with the context of the consumer's first-party relationship.[374] Many kinds of companies, including ISPs, social networks, advertising networks, and operating systems, have the ability to engage in these practices and thus would need to offer consumers choice in order to use data gleaned from such tracking.[375] Notably, however, after all of its fact-gathering and analysis, including a separate workshop eight months after the *FTC Report* was released, the FTC did not single ISPs out for heightened restrictions;[376] it took a technology-neutral approach. It made clear that entities should provide consumers with choice regardless of whether they tracked consumers through DPI, social plug-ins, cookies, web beacons, or some other technology.[377]

---

[372] *FTC Report* at 15-16.

[373] *See infra* notes 405-412 and accompanying text (discussing FTC approach to deliberate marketing based on sensitive information).

[374] *See FTC Report* at 40-41.

[375] *See id.* at 40-41, 56.

[376] FTC, *The Big Picture: Comprehensive Online Data Collection* (2012), https://www.ftc.gov/news-events/events-calendar/2012/12/big-picture-comprehensive-online-data-collection; *see also 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").

[377] *See FTC Report* at 40-41; *see also* FTC, *The Big Picture: Comprehensive Online Data Collection* (Dec. 6, 2012), https://www.ftc.gov/sites/default/files/documents/public_events/The%20Big%20Picture%3A%20Comprehensive%20Online%20Data%20Collection/bigpicture_transcript_21206ftc.pdf; *id.* at 165 (statements of Paul Ohm, professor

The 2012 *White House Privacy Framework* also recognized that companies could infer consumer consent to first-party marketing, explaining that in today's online environment, "companies may infer consent to use personal data to conduct marketing in the context of most first-party relationships, given the familiarity of this activity in digital and in-person commerce, the visibility of this kind of marketing, the presence of an easily identifiable party to contact to provide feedback, and consumers' opportunity to end their relationship with a company if they are dissatisfied with it."[378]

Even the EU GDPR does not require opt-in approval for the use of customers' personal information for first-party marketing. Indeed, the EU GDPR merely requires that consumers be given "the right to object" to such use, and it recognizes companies use of consumers' personal information for first-party marketing as a "legitimate interest" of the company.[379]

CTIA is not taking the position that opt-in approval should *never* be required. But unlike the Commission, the FTC did the research and outreach to identify those circumstances where opt-in consent may be the better practice, and it determined that those circumstances are reasonably tethered to privacy risk. Moreover, the FTC has established an approach that allows providers the flexibility to determine, in the first instance, the appropriate level of protection to

---

and moderator and Christopher Calebrese, legislative counsel, ACLU, in support of technology-neutral approach); *id.* at 197 (statement of Stuart Ingis, co-lead Venable privacy practice, that "the marketplace [should] pick[] winners or losers . . . and . . . we should be careful not to pick a technology or some means of data collection"); *id.* at 267 (statement of Alissa Cooper, Center for Democracy and Technology, that "[t]here are all kinds of technologies that can be used for essentially very similar purposes [as DPI] and not just on a sector-by-sector basis" and arguing that "we should stay away from trying to evaluate these practices on the basis of which technology is being used"); *see also id.* at 273 (statement of Maneesha Mithal, Associate Director, FTC, describing consensus viewpoint among participants of need for adopting technology neutral approach to comprehensive data collection); *cf.* Center for Democracy and Technology, *Comments for November 2015 Workshop on Cross-Device Tracking* 1 (Oct. 16, 2015), https://cdt.org/files/2015/10/10.16.15-CDT-Cross-Device-Comments.pdf (emphasizing importance of providing "meaningful opt-out system" and identifying multiple technological pathways being developed by multiple types of entities to achieve cross-device tracking).

[378] *2012 White House Privacy Framework* at 17.

[379] EU GDPR, Art. 21; *id.* ¶ 47.

afford, based on the sensitivity of the data and context in which the data was collected and used. Such a determination often must be made on a case-by-case basis, taking into account consumer expectations. Similarly, were the Commission here to adopt opt-in approval requirements, it should do so, only given an appropriate record, where (1) ISP marketing involves the *deliberate*, rather than incidental, collection or use of *sensitive* data; (2) ISP marketing involves sharing individual customer information with unaffiliated third parties for their own uses or uses outside of the context of the relationship; or (3) an ISP makes a material change to its privacy policy that will be applied retroactively to data it collected from customers under a previous policy. Otherwise, like the FTC and the White House, the Commission should establish a default position that ISPs may use customer information based on the customers' implied consent consistent with the context of the transaction and the relationship, or if outside the context of the transaction or relationship, based on opt-out consent.

2. Imposing Different Approval Requirements Based on the Type of Service Being Marketed Is Untethered from Either Privacy Risk or Customer Expectations.

Instead of hewing closely to the FTC's privacy framework, the Commission has primarily proposed that ISPs be required to provide opt-out consent before using its new category of customer information, "customer proprietary information," to market communications-related services, and to obtain opt-in approval before using such information to market non-communications-related services to customers. But whether a service is communications-related or not does not have even an attenuated connection to privacy risk, nor does the Commission attempt to establish such a connection.

Instead, the Commission proposes that this distinction comports with customer "desire[s] and expect[ations]."[380] This move fails for a variety of reasons.

First, although the Commission appears to conflate customer preferences and expectations, the two should be treated as analytically distinct concepts. "Customer preferences" refers to how customers would want an entity to use and share their data in a particular circumstance. "Customer expectations," in contrast, describes what customers understand is common practice by companies with which they interact. The latter is an important concept for purposes of consumer privacy, because it is used by policymakers to frame privacy protections;[381] the former does not *inform* privacy protections, but rather is manifested through the various choice options that companies make available to consumers. In short, consumer preferences may be subjective, but expectations are objective.

Second, drawing a distinction based on the type of service being marketed does not, in fact, reflect consumer expectations. The NPRM has to be based on an assumption that consumers are confused or surprised when their ISP offers and markets them non-communications-related services. It is unlikely that there will be substantial evidence showing that such consumer confusion is common, given consumers' general understanding of the Internet and the services offered by their ISPs, and the prevalence of bundled offerings that extend beyond access services to include value-added content and other features. But even if the record were to suggest that such a response could occur in the abstract, this concern is easily resolved through common branding. At a minimum, therefore, this proposed framework misses the mark by focusing on the nature of the service (and not co-branding). Moreover, if the

[380] *See, e.g., NPRM*, 31 FCC Rcd at 2544-45 ¶ 127.

[381] *See, e.g., FTC Report* at 38-39 (explaining that requiring choice based on "context of the interaction" balances the need to preserve flexibility for providers while honoring "reasonable consumer expectations").

"category of service/product" scheme proposed by the Commission did map onto actual customer expectations, the FTC would have discussed it in the *Privacy Report* and would have included evidence in the record on which the *Privacy Report* is based. For example, the FTC does not subject Google to different rules when it markets its search, maps, mail, operating system, and other unrelated services, nor is there any indication the FTC considered doing so. So too should ISPs be able to engage in marketing of various products and services, on a first-party basis, based on consumers' implied consent.

Nor does the Pew Report, cited by the Commission,[382] show that customers' expectations vary depending on the service being marketed. Indeed, the Pew Report has nowhere near the level of granularity that would support the distinction the Commission has proposed. The NPRM cites the Pew Report for the proposition that "the vast majority of adults deem it important to control who can get information about them."[383] But this uncontroversial finding certainly does not support the fact (or inference) that opt-in consent for first-party marketing is necessary to provide adults with the "control" they desire, or that their desire for control corresponds to the product or service being marketed to them. To the contrary: the Pew Report is *inconsistent* with the idea that uniform opt-in should be imposed for certain categories of products or services, given its recognition that privacy preferences are heavily context and condition dependent.[384]

---

[382] *NPRM*, 31 FCC Rcd at 2539, 2545-46 ¶ 109 & nn.188-89, ¶ 129 & n.226.

[383] *Id.* at 2545 ¶ 129 & n.226.

[384] *See* Rainie and Duggan, *supra* note 217, at 2-3 ("[T]he phrase that best captures Americans' views on the choice between privacy vs. disclosure of personal information is, 'It depends.' People's views on the key tradeoff . . . are shaped by both the conditions of the deal and the circumstances of their lives. . . . [N]otable shares of the public say their consideration of each individual scenario is conditional: Their answer depends on the circumstances of the offer, their trust in those collecting and storing the data, and their sense of what the aftermath of data-sharing might look like.").

Moreover, for methodological reasons, the Pew Report should also be accorded little weight. Studies show there are significant gaps between privacy preferences when measured as "willingness to pay" ("WTP") to protect data and "willingness to accept" ("WTA") a benefit to disclose data.[385] "[A]t an empirical level, [research] findings should caution against the uncritical use of privacy valuations that have used single methods—for example, only WTP or only WTA . . . . [E]stimated valuations of privacy . . . are larger when individuals consider trading personal data for money [*i.e.*, WTA] and smaller when people pay money for privacy [*i.e.*, WTP]." The Pew Report appears to be based on a pure WTA methodology,[386] suggesting that its results overstate customer privacy preferences.[387]

Third, to the extent that customer expectations are shown to vary based on the type of service being marketed to them—which showing, CTIA submits, would need to be granular and detailed, given the novelty of this proposed regime—the Commission should define "communications-related services" broadly and flexibly. The overwhelming trend in the ecosystem is toward cross-service consumption of content (*e.g.*, consuming video on fixed broadband, increasing data flows on mobile) such that it is becoming increasingly difficult to draw precise boundaries between services. Additionally, in any context, customer expectations (and preferences, for that matter) are not static, but evolve given changing circumstances. That is especially so here, where the relevant markets are dynamic, resulting in service and product

---

[385] *See* Alessandro Acquisti, Leslie K. John, & George Lowenstein, *What is Privacy Worth*, 42 J. Legal Stud. 249, 255-57 (2013) (concluding that "[t]he dichotomy between WTP and WTA is just one example of the notion that preference for privacy may be not only context dependent but malleable and uncertain and suggest that ordinary studies investigating privacy valuations may not tell us much about whether, or how much, consumers will actually pay to protect their data").

[386] *See* Rainie & Duggan, *supra* note 217, at 2 ("A new Pew Research Center study based on a survey of 461 U.S. adults and nine online focus groups of 80 people finds that there are a variety of circumstances under which many Americans would *share personal information or permit surveillance in return for getting something of perceived value*." (emphasis added)); *id.* at 23-25 (discussing loyalty card offer in exchange for tracking purchases).

[387] Acquisti, John, & Lowenstein, *supra* note 385, at 268.

innovations and disruptions. Further, the distinction between "communications-related services" and "non-communications-related services" in the voice CPNI context is a vestige of the non-competitive and closed communications landscape that existed before 1996 (but which has since become competitive and open); in contrast, and as discussed above, the market for data services is open, dynamic, and competitive. And finally, a narrow definition of "communications-related services" would limit innovation and competition in the market for advanced broadband-related services.[388] Indeed, restricting companies from expanding to offer new lines or from achieving efficiencies through innovative bundling of products and services would run counter to the principles that underlie the American economy.

In sum, the Proposed Rules are fatally flawed with respect to the distinction between communications-related services and non-communications related services. This is a marketing-based distinction, not a privacy-based distinction.

3. Requiring Opt-In Approval For Any Disclosure of, or Access to, "Customer Proprietary Information" to Any Third Party Leads to Absurd Results Without Commensurately Protecting Privacy.

It appears that the Proposed Rules require ISPs to obtain opt-in approval before disclosing or permitting access to *any* of the information defined as "customer proprietary information" to any unaffiliated third party.[389] In addition to being unconstitutional, this approach fails as a policy matter for two reasons. First, the Commission appears not to have

---

[388] These Comments primarily are intended to demonstrate that the proposed distinction between communications-related and non-communications-related services does not advance the *privacy* interest underlying Section 222. Even if the Commission theoretically could have proposed drawing lines based on the type of service being marketed to advance the *competition* interest underlying Section 222, it did not do so, making any such attempt now procedurally unavailable. The foregoing also demonstrates that the proposed distinction would frustrate, rather than advance, Section 222's competition interest in any event.

[389] *See NPRM*, 31 FCC Rcd at 2545-47 ¶¶ 129-32. Chairman Leibowitz hypothesizes that the Commission "could not possibly" have intended this outcome—*viz.*, that ISPs would be required to obtain opt-in consent before sharing with "appropriate affiliates and service providers." *Leibowitz Comments* at 9.

considered meaningful distinctions between various types of third-party relationships. The application of the rules leads to absurd results and massive disruptions of routine ISP business practices that CTIA believes must have been unintended. At the very least, this is an area where further consideration and rulemaking is in the public interest. And second, given the realities of the broadband ecosystem discussed above, the proposed restrictions would not meaningfully protect individuals from the propagation of their information across the Internet ecosystem.

In the context of voice CPNI, the Commission has, over time, considered, developed, and followed different rules governing carriers' disclosures and permitting access to CPNI to different types of third parties—including affiliates,[390] agents,[391] joint venturers and independent contractors,[392] and entirely unrelated third parties.[393] In each proceeding, the Commission addressed how new facts and changing circumstances required certain heightened protections. For example, in 2007, the "exponential[]" growth of the "black market for CPNI" and "increased market value placed on obtaining this data" had created an increased risk of pretexting, justifying the imposition of an opt-in approval requirement for sharing with joint venture partners and independent contractors (but not agents).[394] Even the imposition of opt-out requirements in this context has not been without costs for customers, who, since 2007, must be given an opportunity to opt out before, for example, a carrier's vendor can review account information even for routine business purposes. But at least the Commission's past processes for identifying issues

[390] *See CPNI Second Report and Order*, 13 FCC Rcd at 8074 ¶ 15.

[391] *See In re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers Use of Customer Proprietary Network Information and Other Customer Information*, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14,860, 14,862-63 ¶ 2 (2002) ("*2002 CPNI Order*").

[392] *See 2007 CPNI Order*, 22 FCC Rcd at 6929 ¶ 3.

[393] *Id.* at 6947-53 ¶¶ 37-49; *2002 CPNI Order*, 17 FCC Rcd at 14,880-90 ¶¶ 45-68.

[394] *See 2007 CPNI Order*, 22 FCC Rcd at 6947-48 ¶ 39.

arising from CPNI disclosure and access have been similar to the FTC's case-by-case approach to issues arising from data disclosure and access more generally.

Moreover, because the definition of voice CPNI always has been limited, even as the Commission has adopted tighter restrictions on third-party disclosure and access, the Commission's rules have never prevented carriers from sharing their customers' names, addresses, and phone numbers with *any* third parties. The Commission's approach over time has thus always provided voice carriers with at least some flexibility to define third-party relationships in different ways, mindful of Section 222's objectives. For example, even after the adoption of the Pretexting Rules in 2007, a voice carrier could, without customer approval, enter into a vendor relationship with, for example, a call center or shipping provider, and provide that third party with customer contact information, but not CPNI. Alternatively, a voice carrier could determine, on a case-by-case basis, to enter into an ongoing agency relationship with a closer third party, and could provide that agent with CPNI, so long as customers had received an opt-out opportunity. This flexibility resulted in cost savings and efficiencies, which ultimately benefitted consumers.

In both of these respects, however, the instant NPRM falls short.

The NPRM does not offer a granular explanation of how ISPs create privacy risks for broadband customers when they disclose information to third parties, or allow third parties to access such information.[395] Specifically, the Commission has failed to identify *what types* of information and disclosure (or access) *to which third parties* presents heightened privacy risks. Instead, it treats all disclosures to, and access by, third parties the same. There is no policy

[395] *See NPRM*, 31 FCC Rcd at 2546 ¶ 130 ("[W]e believe that the threat to broadband customers' privacy interest from having their personal information disclosed to [third parties] without their affirmative approval is a substantial one, and there is a greater need to ensure express consent from an approval mechanism for third party disclosure.").

justification for the Commission's blanket approach. It is beyond cavil that sharing a customer's name with an ISP's longstanding agent (for which the ISP has assumed liability) presents a diminished privacy risk relative to an ISP's selling a customer's web browsing activity to an anonymous data broker, but the NPRM fails to acknowledge that distinction.

There likewise is virtually no analysis of whether restrictions on third-party disclosure and access even remain necessary if the Commission adopts rules specifically addressing data security and misuse by third parties.[396] The Commission has long allowed carriers to disclose to, or permit access by their agents to voice CPNI, with opt-out approval, because the carriers' control and liability for any misuse ensures continued protection of the information. Here, the Commission has effectively proposed that ISPs exert similar control and face liability for all third parties, and yet still requires opt-in approval for disclosure or access, without offering any explanation for why both forms of protection even might be necessary—or why implied consent would not meet customer expectations. Given evolving technologies, this NPRM also presented the Commission an opportunity to distinguish between different privacy concerns that might arise from actually disclosing customer information to third parties (*i.e.*, sharing materials, which involves the surrendering of control) as opposed to permitting third-party access to customer information (*e.g.*, presenting materials through a secure online portal), the latter of which consumers understand is routine in American business operations.

On the other hand, by shoehorning tremendous amounts of relatively anodyne information into the category of "customer proprietary information," the Proposed Rules would cause massive disruptions in routine ISP operations. An ISP's inability, following adoption of the Proposed Rules, to send a promotional mailer to a customer, saluting him or her by name, at

[396] *See id.* at 2569 ¶ 210.

his or her home address, using the U.S. Mail is but one example. The fact that the Proposed Rules even possibly could have such results suggests the need to restart this proceeding.

Finally, for reasons already explained in detail above, these potentially tremendous costs come with very little purchase. Unlike in the old telephone voice services market, here, the nefarious (and enterprising) actors who might misuse "customer proprietary information" have more than one potential supplier: they can hack a retailer's website for credit card information; they can obtain an individual's call list through a mobile operating system; they can purchase customer profiles from data brokers; and so forth. Selectively imposing restrictions on when and with whom ISPs can share information in this open ecosystem would not redress any of these scenarios—all of which would result in actual or potential consumer harm, unlike the benign use cases that the Proposed Rules would regulate.

4. The Alternative Approaches Advanced by the Commission for Comment Are Similarly Flawed.

The NPRM seeks comment on various alternative approaches to the primary framework discussed immediately above. Each suffers from substantial shortcomings.

The Commission requests comment on an alternative proposal that would require ISPs "to obtain customer opt-in approval for the use and sharing of all customer [proprietary information]," except where consent is implied or where there is a codified statutory exemption;[397] this approach fails for all of the above-cited reasons: It does not reflect a heightened privacy risk or customer expectations; it undermines innovation and competition; and it does not materially advance a privacy interest. Additionally, this approach is even more

[397] *Id.* at 2544 ¶ 126.

problematic under the First Amendment than the primary proposal, because it creates a default position of censorship with respect to more speech.

The Commission separately requests comment on whether its rules should treat virtually all affiliates as third parties (and accordingly require opt-in approval for disclosure) except where the relationship is clear to consumers (*e.g.*, co-branding);[398] this approach amounts to a radical departure from the Commission's voice CPNI rules, without any apparent basis for doing so. Moreover, this approach is not practicable for ISPs and would effectively shut down any advertising or marketing based on use of customer data that the provider obtained by virtue of its provision of service. The approach also is inconsistent with customer expectations, because after years of receiving bundled services, customers understand affiliate relationships and expect the same rules to apply to the use of the data within a company—irrespective of which corporate entity is using the data for which marketing campaign. Moreover, this approach to affiliates is expressly based on the concern that ISPs lack adequate incentives to protect the customer-provider relationship with respect to use or disclosure of customer information.[399] This concern, in turn, is based on a failure to acknowledge the robust competition among providers and the low switching costs for customers, addressed above.[400] In any event, ISPs have every incentive to safeguard information obtained from customers, given the importance of maintaining consumer trust and the value of the information, which everyone in the proceeding agrees is high. In the few rural areas where there may be only one or two wireless providers, the providers' privacy

[398] *Id.* at 2544-45 ¶¶ 126, 128.

[399] *Id.* at 2545 ¶ 128.

[400] *See supra* notes 356-363 and accompanying text.

policies are the same as those in markets where there is robust competition.[401] And finally, even if there were insufficient competition in some markets, such circumstances could be remedied by requiring companies to allow customers to opt out of data use. An opt-in requirement would be unnecessary to avoid a perceived and unsubstantiated problem of lack of choice over data use.

The Commission identifies an alternative of requiring "opt-out approval . . . for ISPs' (and their affiliates') use of customer [proprietary information] for purposes other than marketing communications-related services,"[402] which is a moderate improvement vis-à-vis the primary proposal of requiring opt-in approval for such marketing. But here too, with the possible exception of marketing based on persistent tracking or the use of sensitive data, the Commission's rules would be in tension with the FTC's approach that, subject to specifically delineated exceptions, first-party marketing generally is appropriate based on the customer's implied consent.[403] Any such deviation must be based on record evidence distinguishing ISPs' practices from those of other entities in the ecosystem—a distinction that the FTC, after careful and thorough research and analysis, did not find.[404]

The suggestion that the Commission identify "certain types of highly sensitive customer information," which can be used by ISPs, "even for the provision of the service, or shared with their affiliates offering communications-related services, only after receiving opt-in approval from customers"[405] finds a modicum of support from the *FTC Report*, but the FTC's approach is

---

[401] For example, none of the privacy policies of the four national wireless carriers differ based on jurisdiction. *See supra* note 337.

[402] *NPRM*, 31 FCC Rcd at 2547 ¶ 133.

[403] *See FTC Report* at 40.

[404] *See supra* Part V.B.1, especially notes 369-377 and accompanying text.

[405] *NPRM*, 31 FCC Rcd at 2548 ¶ 136.

considerably more tailored on this point.[406] Specifically, according to the FTC, the "requirement of affirmative express consent for first-party marketing using sensitive data should be limited. Certainly, where a company's business model is *designed to target* advertising or other activities to consumers based on sensitive data—including data about children, financial and health information, Social Security numbers, and precise geolocation data—the company should seek affirmative express consent before using or disclosing the data from those consumers. On the other hand, the risks to consumers may not justify the potential burdens on general audience businesses that *incidentally collect* and use sensitive information."[407] The FTC based this conclusion on a cost-benefit analysis, and CTIA urges the Commission to do the same. Additionally, even use of "highly sensitive" customer information by ISPs, or disclosing or permitting access to such information with affiliates offering communications-related services, is still *internal use* by ISPs.

Moreover, there already are laws that protect sensitive information. For example, the Fair Credit Reporting Act regulates the use of personal information for sensitive purposes like credit, employment, and housing. COPPA regulates the collection and use of personal information from children.[408] HIPAA protects health-related information.[409] GLBA imposes privacy and security requirements on financial institutions.[410] And laws designed to protect individuals' safety (such as anti-stalking laws) govern the collection and use of precise geo-

---

[406] *See FTC Report* at 47 ("The [FTC] agrees with the commenters who stated that affirmative express consent is appropriate when a company uses sensitive data for any marketing whether first- or third-party. Although as a general rule, most first-party marketing presents fewer privacy concerns, the calculus changes when the data is sensitive. . . . In light of the heightened privacy risks associated with sensitive data, first parties should provide a consumer choice mechanism at the time of data collection.").

[407] *FTC Report* at 47-48.

[408] *See supra* note 78.

[409] *See supra* note 102.

[410] *See supra* note 112.

location information.[411] Notably, the FTC jurisprudence and guidance and the anti-stalking laws distinguish between precise geolocation information, on the one hand, and other, less granular types of location information, on the other. In general, only the former is deemed sensitive and deserving of heightened protection.[412] The Commission refers to legislation related to "call location information,"[413] but this information is different from the kind of location information typically held by ISPs. CTIA urges the Commission to make clear that its Proposed Rules would cover only precise GPS location information.

Furthermore, this proposal, if adopted, could have the unintended consequence of frustrating the Commission's purported privacy objectives, by requiring ISPs to identify the sensitivity of data crossing their networks to determine the level of consent required. The most viable way to do so would be to use DPI, a technology similar to methods other platform providers use to analyze data and which the Commission otherwise appears to disfavor. Accordingly, if the Commission elects this approach, it should include language making clear that ISPs are not required to proactively analyze customer data to determine what form of choice is appropriate—*i.e.*, the rule should apply *only to the extent an ISP reasonably knows* that information qualifies as highly sensitive.

The Commission's request for comment on whether to require ISPs to obtain consent before combining third-party data with data obtained by virtue of providing the service,[414] too, is

---

[411] *See, e.g.*, N.Y. Penal Law § 250.45(5)(c) ("Jackie's Law").

[412] *See FTC Report* at 59-60 (discussing sensitivity of, among other data, "*precise* geolocation data" (emphasis added)); *The Location Privacy Act of 2014: Hearing Before the Subcomm. for Privacy, Technology, and the Law* (2014) (statement of Jessica Rich, Director, Bureau of Consumer Protection), *available at* https://www.ftc.gov/system/files/documents/public_statements/313671/140604locationprivacyact.pdf (discussing sensitivity of "precise location information").

[413] *NPRM*, 31 FCC Rcd at 2548-49 ¶ 136.

[414] *Id.* at 2549 ¶¶ 138.

a nonstarter as a statutory matter, as addressed above.[415] Moreover, this practice, referred to in the industry as "data appending," is routine for advertising and marketing by all kinds of companies, and there are no regulations or privacy implications that any other governing body has identified with the practice.[416] This proposal in particular also exacerbates the problem that ISPs are already uniquely competitively *disadvantaged* vis-à-vis other entities in the broadband ecosystem in terms of cross-context and cross-device tracking,[417] and imposes further restrictions on ISPs' ability to compete in the online advertising market.

C. The NPRM Rules Implementing Section 222(d)'s Exceptions Should Provide ISPs with Flexibility to Operate Their Businesses, Provide Security, and Protect Against Fraud.

The NPRM queries whether ISPs "need or benefit from using customer [proprietary information] for purposes other than marketing communications-related services" and, if so, asks "what are those uses?"[418] Although asked in the section of the NPRM addressing choice rules under Section 222(c)(1), the question is nonetheless surprising, given (1) that Section 222(d) identifies a number of other non-marketing uses for CPNI that are beneficial to the ISP, other carriers, and indeed, to customers; and (2) that the NPRM also identifies the importance of cybersecurity, which, in order to be effective, requires a flexible approach to data use and

---

[415] *See supra* Part I.C.5 (discussing statutory requirement that carriers be permitted to use, without approval, information not obtained by virtue of providing service).

[416] *See, e.g.*, Experian, *Introducing Consumerview Now*, http://www.experian.com/small-business/data-appending-services.jsp (last visited May11, 2016) (commercial appending provider service for SMBs); Relevate Group, *Services, Data Append & Enhancement*, http://www.relevategroup.com/services/data-enhancement/ (last visited May 11, 2016) ("adding actionable information to your prospect or customer data will provide you with critical insight regarding your customers"); Speedeon Data, *Data Append*, http://www.speedeondata.com/service/category-81763dca-5149-47ef-8949-94ba0460a3b7.aspx (last visited May 11, 2016) ("For the data you need but don't have, data append solutions provide the most up-to-date name, mail and e-mail address, telephone and demographic data on your customers and prospects"); NAICS Association, *Data Append Services*, https://www.naics.com/data-append-services-enhancement/ (last visited May 11, 2016).

[417] *Swire Report* at 13-14, 106-07, 119-21.

[418] *NPRM*, 31 FCC Rcd at 2545 ¶ 128.

sharing. The Proposed Rules give these interests short shrift, both by defining the category of protected information ("customer proprietary information") broadly, and suggesting that the exceptions are rigid and narrow.

Rather than relegate these uses to the backseat, the Commission should allow for a flexible set of exceptions that reflect the role that ISPs can play in protecting not only privacy, but also against fraud, abuse, mismanagement, cybersecurity threats, and more. In this regard, too, it should be emphasized that the FTC has taken a flexible approach, rather than attempting specifically to identify the types of legitimate business practices involving use of customer information that should be permitted without approval.[419] A flexible approach also makes good policy sense for a rapidly evolving ecosystem, where the next generation of beneficial and innovative uses of data are not always immediately apparent. ISPs should not be forced constantly to fight the last war.

1. The Commission Should Adopt Section 222(d) Rules to Facilitate Network Management and Protection of Carriers, Customers, and Other Third Parties.

The Proposed Rules implementing Section 222(d)[420] should be rewritten to ensure that they cover ISPs' routine practices that benefit carriers, customers, and third parties.

For example, the Commission should make clear that the Proposed Rules allow ISPs to use "customer proprietary information" for network management and related purposes, such as to improve the delivery of service. This would follow from the internal carve out in Section 222(c)(1), which allows carriers to use information to provide the service itself or to provide services necessary to, or used in the provision of, the service. Over time, ISPs can track and

[419] *See FTC Report* at 26-27; EU GDPR ¶¶ 47-50.

[420] *NPRM*, 31 FCC Rcd at 2540-41 ¶¶ 115, 117.

utilize individually identifiable, and de-identified, and aggregate data to manage bandwidth needs and identify areas, times of day, and other factors that can result in congestion and related service disruptions. In separate proceedings, the Commission has recognized the importance of such network management to match the exponential growth in demand for data—especially from mobile providers.[421]

Moreover, any adopted rules should make clear that ISPs may use "customer proprietary information" *whenever reasonably necessary* to protect users, providers, *and other entities* from fraudulent, abusive, or unlawful use of, or subscription to, broadband services *or other products and services*.[422] The inclusion of "other entities" in this exception is important. For example, ISPs should be permitted to share data to help financial institutions authenticate users and prevent financial fraud.[423] This will benefit consumers by reducing fraud in the data ecosystem. ISPs also should be entitled to use customer information to protect content creators from digital piracy.

A clarification of this exception will help accommodate the continued growth of Internet use, which will spur new relationships between consumers and various companies in the ecosystem, generating substantial public interest benefits. Companies should be permitted to share consumer data routinely with other kinds of companies to use that data for unobjectionable authentication procedures, which ultimately saves costs and protects consumers. Fraudsters

---

[421] *See, e.g., 2016 Broadband Progress Report*, 31 FCC Rcd at 708 ¶¶ 20-21.

[422] *See NPRM*, 31 FCC Rcd at 2541 ¶ 117.

[423] *See, e.g.*, Chris Johnson, et al., *Guide to Cyber Threat Information Sharing*, (Second Draft NIST Special Publication 800-150 April 2016), http://csrc.nist.gov/publications/drafts/800-150/sp800_150_second_draft.pdf (identifying "scenarios . . . to show how sharing and coordination can increase the efficiency and effectiveness of an organization's cybersecurity capabilities" including where ISPs form part of working group to "assist both the affected companies and law enforcement personnel by helping to identify the upstream and downstream traffic sources, implementing routing changes, and enforcing data rate limits").

increasingly use digital channels to commit identity theft that defrauds consumers, retailers, and financial service providers. Carriers can be part of the solution by providing or giving access to data to authenticate transactions. Furthermore, other statutes explicitly permit disclosure of certain data, including data that may fall within the Commission's proposed category of "customer proprietary information," for these purposes.[424] Moreover, the collaboration between ISPs and financial institutions to enable safe and secure digital transactions is consistent with the Administration's goal to expand the availability of financial services to the unbanked and underbanked.[425] The Commission should clarify that the Act allows these activities, so that the rules do not have the perverse result of contravening Congress's clear intent in enacting Section 222(d)(2) by inhibiting practices that not only do not result in, but actually prevent, consumer harms such as fraud and identity theft.

2. The Commission Should Make Clear That Its Rules Do not Limit Any Sharing of Information for Cybersecurity Purposes.

The NPRM acknowledges that complex rules could stymie cybersecurity information sharing, and proposes to interpret section 222(d)(2) to allow ISPs to protect themselves or others from cybersecurity threats or vulnerabilities.[426] The Commission must make clear that nothing in Section 222, existing voice CPNI rules, or any new rules limits ISPs' ability to share cybersecurity information, whether CPNI or "customer propriety information."

---

[424] *See* Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113, Division N § 104(b)-(d), 129 Stat. 2242, 2936, 2941-42 (allowing "defensive measures" and disclosure of "cyber threat indicators or defensive measures" in certain circumstances and with specific safeguards).

[425] *See* Consumer Financial Protection Bureau, *Mobile Financial Services Report* (Nov. 2015), *available at* http://files.consumerfinance.gov/f/201511_cfpb_mobile-financial-services.pdf (providing information on how mobile financial services can help customers underserved by traditional financial services).

[426] *NPRM*, 31 FCC Rcd at 2541 ¶ 117.

Broad information sharing lets companies improve detection, mitigation, and response. Put simply, "[w]e know sharing threat information is critical to effective cybersecurity."[427] Entities "must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible."[428] The Department of Homeland Security ("DHS") operates a statutorily-based information sharing program, Protected Critical Infrastructure Information, that protects shared information from public disclosure,[429] and its National Cybersecurity & Communications Integration Center ("NCCIC") is a hub of sharing "among public and private sector partners."[430] Moreover, a key part of NIST's Cybersecurity Framework is information sharing.[431] Likewise, the Communications Security, Reliability, and Interoperability Council ("CSRIC") urges industry to "shar[e] more detailed threat intelligence information"[432] and is looking at sharing in the communications sector.[433] In the Cybersecurity

[427] Michael Daniel, *Getting Serious About Information Sharing for Cybersecurity*, White House Blog (Apr. 10, 2014, 1:45 PM), https://www.whitehouse.gov/blog/2014/04/10/getting-serious-about-information-sharing-cybersecurity; *see also Today's Mobile Cybersecurity: Information Sharing*, CTIA—The Wireless Association, at 8, http://www.ctia.org/docs/default-source/default-document-library/ctia_informationsharing.pdf ("[I]t serves as the essential, hidden shield in the ongoing struggle to protect [us] against cyberthreats.").

[428] Exec. Order No. 13691, 80 Fed. Reg. 9349, Promoting Private Sector Cybersecurity Information Sharing (Feb. 13, 2015) https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

[429] *See Protected Critical Infrastructure Information (PCII) Program*¸DHS.gov, https://www.dhs.gov/protected-critical-infrastructure-information-pcii-program (last visited May 24, 2016).

[430] *National Cybersecurity and Communications Integration Center*, DHS.gov, https://www.dhs.gov/national-cybersecurity-and-communications-integration-center.

[431] Framework for Improving Critical Infrastructure Cybersecurity 9, 17, 33, NIST (Feb. 12, 2014) http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf ("NIST Cybersecurity Framework").

[432] Cybersecurity Risk Management and Best Practices Working Group 4: Final Report 10, CSRIC (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf ("CSRIC WG 4 Final Report").

[433] Working Group 5: Cybersecurity Information Sharing: Status Update, CSRIC (Mar. 16, 2016), https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG5_Presentation_031616.pptx.

Information Sharing Act of 2015 ("CISA"),[434] Congress authorized certain information-sharing, "notwithstanding any other provision of law."[435] This was "important," because before CISA, "private and public sectors [could not] fully share cyber threat information."[436]

The Commission should avoid creating legal uncertainty, because any barrier to sharing information will create risk. For example, the Proposed Rules may encompass IP protocol metadata. ISPs may be reluctant to share, and discouraged from sharing, with Information Sharing and Analysis Organizations and Information Sharing and Analysis Centers without having protections to ensure that other parties use data consistent with complex Commission obligations. In addition, ISPs may be discouraged from bundling anti-virus software with services, as anti-virus software stores info on CPE and anti-malware vendors aggregate this information.[437] Uncertainty will cause delay, and less information may be shared.

The Commission proposes to make clear that its approach will allow cybersecurity information sharing of CPNI, and asks whether it should include "customer proprietary information," as well.[438] If the Commission attempts to do so, notwithstanding CTIA's comments to the contrary, it must clarify that the statute and the Commission's rules are not barriers to any information sharing, whether they concern CPNI or "customer proprietary information."

---

[434] Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113, Division N, 129 Stat. 2242, 2936 (codified at 6 U.S.C. §§ 1501-1510).

[435] 6 U.S.C. § 1503(a)(1). This broad authorization would moot any obstacle the Commission might create, but as CISA and other information sharing efforts proceed, the Commission should ensure its rules do not erect barriers.

[436] Press Release, Senator Dianne Feinstein, Debunking Myths about Cybersecurity Information Sharing Act (Oct. 20, 2015), http://www.feinstein.senate.gov/public/index.cfm/2015/10/debunking-myths-about-cybersecurity-information-sharing-act.

[437] *See infra* Part VI.A.2.a.

[438] *NPRM*, 31 FCC Rcd at 2541 ¶ 117.

The Commission asks whether it should provide guidance on what constitutes a cybersecurity threat entitled to this "exception."[439] Any definition offered by the Commission is likely to be under-inclusive and rapidly become obsolete. The threat landscape is evolving, and many agencies and entities are evaluating next steps. DHS is the point through which information is shared under CISA; the Commission should not complicate this with its own approach. The Commission could indicate that permissible activities include, but are not limited to, baseline definitions in CISA, but even codifying existing definitions will lock in approaches. CISA is unlikely to be the last development, so the Commission need make clear only that existing and future rules and duties regarding CPNI, "customer proprietary information," and data and network security are not barriers to information sharing.

3. The Commission Should Adopt Rules Carving Out Uses and Disclosures of Non-Residential Customers' Information.

Furthermore, whether implemented under Section 222(d) or otherwise, the Commission should adopt a specific exemption for ISP use or disclosure of, or permitting access to, the information of non-residential customers (*i.e.*, business customers). As discussed previously, none of the privacy concerns underlying Section 222 or identified in the NPRM apply to non-residential customers.[440] The Commission has previously adopted similar exceptions to its voice CPNI rules.[441]

[439] *Id.*

[440] *See supra* note 260 and accompanying text.

[441] *See* 47 C.F.R.§ 64.2010(g).

D. The Proposed Rules Regarding When and How ISPs Obtain Approval Impose Unreasonable Costs, Without Providing Meaningful Additional Protection.

The Commission proposes and seeks comment on a variety of specific requirements for how ISPs solicit and obtain customer approval. These requirements relate to when and how frequently ISPs must solicit consent, what the approval interface options should be, and ISP retention of approval decisions. The Commission should avoid an overly prescriptive approach, which would impose unnecessary costs on ISPs and squander ISPs' knowledge about how best to interact with particular (or particular types of) customers—forcing every approval transaction down to the lowest common denominator.

The proposal to require ISPs to obtain approval "subsequent to the point of sale" and "when a[n] [ISP] first intends to use or disclose the customer's proprietary information in a manner that requires customer approval"[442] benefits neither carriers nor customers. In some circumstances, it may be more effective for the customer, and more efficient for the ISP, to provide notice and obtain consent at the point of sale, when, for example, an ISP's in-store employee walks the customer through every aspect of service. But a "point of sale" approach may not make sense for all types of data or all types of uses. Moreover, there may be other circumstances where the ISP knows that disclosure and consent at the point of sale would be ineffective. Given the variety of factors that must be considered when determining how to seek consent most effectively, the provider is best positioned to make the ultimate determination, as long as it is not doing so in an unfair or deceptive manner.

This aspect of the Proposed Rules appears to be based on a misapplication of the FTC's sound determination that, as a general matter, choice should be provided "at a time and in a

[442] *NPRM*, 31 FCC Rcd at 2550 ¶ 140.

context that is relevant to consumers."[443] The NPRM fails to recognize, however, that it is often *providers* that can best determine the time and context that will be relevant to *consumers*.[444] The salient point is that there is no one-size-fits-all "time" and "context" that is always "most relevant" to consumers. Instead, often the point of sale will be most effective from both the provider's and consumer's perspective; in other circumstances, another time may be more effective. Nothing in the *FTC Report* is to the contrary.[445]

The NPRM seeks comment on whether ISPs should be required "to notify customers of their privacy choices" and to "solicit customer approval at [many] prominent points of time," such as "just-in-time approval whenever" the relevant information is "collected or each time the [ISP] intends to use or disclose the relevant [information]."[446] CTIA respectfully submits that a mandated just-in-time approach would exacerbate the tendency of the Proposed Notice Rules to desensitize customers, undermining the privacy protection the Rule are intended to advance. This approach also would impose considerable costs on ISPs, especially if adopted in conjunction with a requirement that ISPs provide a sophisticated user interface—the merits of which are questionable as well.[447] Further, as discussed above, frequent notices also will generate customer confusion and frustration, as consumers may not understand why their previously provided "consents" are not being honored. If, however, the Commission pursues this

[443] *Id.* at 2550 ¶ 141 (quotation marks omitted).

[444] *Id.*

[445] *FTC Report* at 35 (emphases added).

[446] *NPRM*, 31 FCC Rcd at 2550-51 ¶ 142.

[447] *See supra* notes 329-333 and accompanying text (addressing dashboard notice alternative).

approach, it should recognize that just-in-time notice of choice provides zero benefit where consent is implied, or where a customer already has been afforded an opportunity to opt out.[448]

The Commission should not require ISPs to accept approval selections by *any* means.[449] This requirement would impose unnecessary costs on ISPs, especially insofar as it encompasses written correspondence. Moreover, the NPRM does not cite any indication that there are customers who prefer these options—let alone require them or otherwise would be unwilling to adopt more efficient practices. In any event, companies should have flexibility to provide choices in the ways that their consumers prefer, which may include many means, but none should be required.[450]

Finally, the NPRM's approach to ISP record retention lacks any support.[451] The fact that the Proposed Rules are based on the rules "governing safeguards on the use and disclosure of customer [proprietary information] for voice telecommunications services"[452] is precisely the problem: no similar compliance and record-keeping rules apply to any other entities in the broadband ecosystem. Moreover, ISPs are in the best position to determine what records they need to keep for compliance purposes, balanced against risk to customer privacy and other business concerns that attach to record retention.[453] Indeed, requiring ISPs to retain records for

---

[448] The *FTC Report* is not to the contrary, insofar as it discusses the value of allowing customers to exercise just-in-time "choice," whereas the NPRM is looser in describing just-in-time notifications triggered by, among other things, collection. *See FTC Report* at 49-50.

[449] *NPRM*, 31 FCC Rcd at 2551 ¶ 145.

[450] *See FTC Report* at 49-50 ("Indeed, the proposed framework was not intended to set forth a 'one size fits all' model for designing consumer choice mechanisms. Staff instead called on companies to offer clear and concise choice mechanisms . . . at a time and in a context that is relevant to the consumer's decision . . . Precisely how companies in different industries achieve these goals may differ . . . .").

[451] *See NPRM*, 31 FCC Rcd at 2552 ¶ 149.

[452] *See id.*

[453] *See, e.g.*, *FTC Report* at 9 ("[T]he framework does not include rigid provisions such as specific disclosures or mandatory data retention and destruction periods.").

non-business and non-customer-facing reasons would be inconsistent with basic data governance principles—*i.e.*, that providers should not retain records longer than necessary.[454] These retention requirements serve only the Commission's regulatory and administrative needs, while creating data security risks for consumers, without any indication that ISPs will not honor customer decisions.

Specifically, requiring ISPs to maintain records on customer information disclosures to third parties for at least one year (whether in the form of records regarding information sharing or records of notices) serves no business or customer-facing function. Similarly, requiring ISPs to retain records of customer notices and approvals for at least one year for customers who have opted out of use and disclosure of their information would frustrate those customers' privacy preferences, without any resulting benefit.

VI. The Proposed Rules Regarding Data Security Are Not in the Public Interest

A. The Commission's Approach Reveals a Fundamental Misunderstanding of Network Security and Threatens to Harm Consumers.

1. The Proposed Rules Reflect a Simplistic and Static View of the Internet Ecosystem, Network Design, and Risk Management.

The Commission's proposed approach to data security is not based on a firm grasp of network security, the complex Internet ecosystem, risk management, or sensitivity analysis. By applying and expanding rules for CPNI to virtually all information that ISPs handle, the Commission risks endangering security and stifling innovation.

[454] *See, e.g., id.* at 28 ("The Commission confirms its conclusion that companies should implement reasonable restrictions on the retention of data and should dispose of it once the data has outlived the legitimate purpose for which it was collected."); *see also id.* at 60 ("For example, all companies should consider shorter retention periods for teens' data.").

a. The Commission's Approach Oversimplifies the Internet ecosystem, Underestimates Cyber Threats, and Ignores the Dynamic Nature of Network Design and Management.

The global Internet ecosystem extends far beyond ISPs to include operating systems, search engines, mail platforms, social networks, and advertising networks, among others.[455] Comprehensive security requires a multilayered approach.[456] This enables the entire ecosystem to adjust to changes in technology and threats. A host of non-governmental standards bodies and associations—like 3GPP[457] and ATIS[458]—are dedicated to security across the network. But the current proposal looks only to ISPs, fragmenting the ecosystem's holistic and flexible approach to adapt to technology and the dynamic threat landscape.

Additionally, the Commission seems to misapprehend the nature of online threats, whose profiles are ever changing, with cybercriminals constantly shifting tactics.[459] Just as "[a] broader and deeper threat landscape greeted 2016 . . . [with] new technologies and attack models from the year before,"[460] each year will bring a different landscape. This evolving challenge cannot be addressed by static rules developed by reference to past and current concerns.

---

[455] *See supra* Part V.A.2.

[456] *See, e.g.*, CTIA, Comments to NIST on Mobile Device Security: Cloud and Hybrid Builds, at 2 (filed Jan. 8, 2016); CTIA, Comments to FTC on Mobile Security Project, No. P145408, at 10 (filed May 30, 2014), http://www.ctia.org/docs/default-source/fcc-filings/ctia-ftc-mobile-security-prose.pdf?sfvrsn=0.

[457] 3GPP: A Global Initiative, The Mobile Broadband Standard—Home , http://www.3gpp.org/specifications-groups/sa-plenary/sa3-security/home (explaining that the working group is "responsible for security and privacy in 3GPP systems, determining the security and privacy requirements, and specifying the security architectures and protocols").

[458] ATIS, Advancing Transformation of the ICT Industry, http://atis.org/about/index.asp (explaining that one of its priorities is to create "solutions and an overall industry framework for addressing cybersecurity threats").

[459] *See* TrendMicro, TrendLabs 1Q 2014 Security Roundup, Cybercrime Hits the Unexpected: Bitcoin- and PoS-System-Related Attacks Trouble Users 9 (2014), http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-cybercrime-hits-the-unexpected.pdf ("Cybercriminals continue[] to find new avenues to commit digital crime and evade countermeasures applied against their creations.").

[460] TrendMicro *Setting the Stage: Landscape Shifts Dictate Future Threat Response Strategies* (Mar. 8, 2016), http://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup.

Likewise, the rules are predicated on treating network design and management as static. This threatens to endanger networks. Network design and configuration is highly complex, varied and fluid. In light of changing technology, industry needs to innovate and move on to better measures as circumstances dictate. Unless tempered by reasonableness and flexibility, mandates will force companies to continue doing what has been done, and outdated expectations will constrain innovation,[461] as resources flow to what is required, not what is best. This seems lost on the Commission, which proposes minimum requirements and asks hundreds of questions about mandating particular procedures, like methods of authentication and network segmentation. This approach is flawed, and inconsistent with the reality of today's threat environment.

b. The Commission Ignores Real-World Risk Management and Wrongly Treats All Data as Equal.

Risk management is different for every organization and changes over time. "Risk management is the process of identifying risk, assessing risk, and taking steps *to reduce risk to an acceptable level*."[462] It is not about *eliminating* risk: "there is not a perfect solution to information security."[463] Many agencies recognize this. "Organizations will continue to have unique risks—different threats, different vulnerabilities, and different risk tolerances—and how

[461] Policymakers' use of DNSSEC to secure the Domain Name System ("DNS") provides a useful example of why it is important to avoid locking in approaches to data security *ex ante*. Early best practices identified DNSSEC as a valuable tool, but making it a broad private industry *requirement* would have been unwise. Not only has technology and the threat landscape changed dramatically since DNSSEC was introduced in 1997, but DNSSEC may have unintended consequences, exacerbating other types of attacks, impacting reliability and cost, harming user experience due to false alarms, and burdening network capacity. Industry is innovating on DNS security. Had the Commission required DNSSEC, innovation would have been stunted, and the DNS would be less secure.

[462] Gary Stoneburner et al., Risk Management Guide for Information Technology Systems 1 (NIST, Special Publication 800-30, July 2002), http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (emphasis added).

[463] Dan Nutkis, CEO of HITRUST Alliance, Cybersecurity: The Evolving Nature of Cyber Threats Facing the Private Sector, Testimony Before the Oversight and Government Reform Committee, Subcommittee on Information Technology (March 18, 2015), https://www.hsdl.org/?view&did=767368.

they implement [various] practices . . . will vary."[464] NIST explains: To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance.[465] The Commission's CSRIC IV Working Group 4 agrees: "[e]fforts to help enterprises manage cybersecurity risk must be continuous and ongoing to adapt to a continually changing ecosystem and threat landscape," and "each enterprise must decide how to utilize and implement the [NIST] Framework or an equivalent risk management construct."[466] The White House says, "[a]t present, provable security exists only in very limited domains, … practical cybersecurity draws on the emerging principles of such research… [and] practical lessons learned."[467] Likewise, the FTC advises companies to "assess their options and make reasonable choices based on the nature of their business and the sensitivity of the information involved."[468]

Despite this, the Commission adopts an unrealistic mandate, proposing to require ISPs to "*ensure* the security, confidentiality, and integrity of all ["customer proprietary information"] the [ISP] receives, maintains, uses, discloses, or permits access to from any unauthorized uses or disclosures, or uses exceeding authorization."[469] And under its proposed risk assessment regulation, the Commission would require complete risk mitigation, requiring an ISP to "promptly address *any weaknesses* in the [ISP]'s data security system identified by . . .

---

[464] NIST Framework, *supra* note 431, at 2.

[465] *Id.* at 5.

[466] CSRIC WG 4 Final Report, *supra* note 432, at 10.

[467] *White House Technology Privacy Report* at 33.

[468] FTC, *Start with Security: A Guide for Business* 1 (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[469] *NPRM*, 31 FCC Rcd at 2608-09 App. A (proposed rule § 64.7005(a)) (emphasis added).

assessments."[470] This turns risk management on its head and will keep companies from dedicating finite resources to real risks and safeguarding truly sensitive information.

Yet another way the Commission proposes to force the mismanagement of finite security resources is by wrongly treating all data that ISPs hold as equal. The Commission's overly broad definitions, as described,[471] do not distinguish sensitive from non-sensitive data. The Commission proposes to include even publicly available information (such as name, address, and phone number) and data that have been de-identified. Therefore, under this proposed regime, the Commission would subject publicly-available data held by ISPs to the same overly burdensome regulations as truly sensitive data. Just as is the case with the risk management mandate, if ISPs are forced to spread their defenses this broadly, overall security will suffer.

c. The Commission Wrongly Assumes ISPs Can Control the Security Practices of Downstream and Upstream Players in the Internet Ecosystem.

The Commission appears to assume that ISPs can control the security practices of other players, given its approach to third-party liability and interactions between ISPs and edge providers.[472] The Commission states that ISPs should "ensure the confidentiality of customer [proprietary information] when shared with third parties"[473] and asks how to achieve this, including whether to dictate contractual commitments between ISPs and mobile device and operating system manufacturers.[474] ISPs do not control the security practices of the ecosystem. ISPs compete with edge providers and deal competitively with suppliers and business partners;

[470] *Id.* (proposed rule § 64.7005(a)(1)) (emphasis added).

[471] *See supra* Part I.C.1.

[472] *See infra* Part VI.C.5.

[473] *NPRM*, 31 FCC Rcd at 2569 ¶ 211.

[474] *See, e.g., id.* at 2570 ¶ 213.

to saddle one part of the ecosystem with burdensome demands that they must impose on business partners will disadvantage them relative to unregulated players. It is unrealistic for the Commission to expect ISPs, many of which are small- to medium-sized entities, to control the security practices of other entities. Even large ISPs do not have such power. Expecting ISPs to enforce requirements upstream and downstream is also unrealistic. Small ISPs in particular depend on large commercial providers for technology, software, and help with network and customer service, including 911 and interoperability for roaming. It is not reasonable to expect them to manage large providers' operations. The proposals' unintended consequences will cause more harm than good, especially to consumers.

2. The Commission's Flawed Regulatory Vision Threatens Serious Unintended Consequences: It Would Create a Less Secure Network, Diminish User Experience, and Burden ISPs.

a. The Commission's Approach Would Worsen Security and Degrade Users' Experience.

The NPRM's approach would make networks less secure. Technical mandates and prescriptive regulations encourage a compliance mindset, rewarding companies that meet minimum standards and discouraging innovation. The Proposed Rules, combined with the incredibly broad definitions of data to be protected, will remove incentives for companies to engage in valuable security measures. Among the unintended consequences, the Commission's approach will:

- **Make it easier for cybercriminals**. Static requirements and standardized security provide a roadmap for hackers.[475]

- **Harm the functioning of the Internet**. The Commission would expand liability and limit ISPs in their use of data, with serious consequences. For example, the

[475] CTIA, *Today's Mobile Cybersecurity: Blueprint for the Future* 24 (Feb. 12, 2013), http://www.ctia.org/docs/default-source/default-document-library/cybersecurity_white_paper.pdf?sfvrsn=2.

restrictions on data usage and sharing may impact migration from IPv4 to IPv6, because under the proposed rules and broad definitions, ISPs may have to ensure IP addresses exiting their network do not contain MAC addresses.[476] It may also limit the use of DPI, which is critical for SPAM filtering and parental controls. And, the rules may limit fraud-detection, which may require use of information that would arguably be covered by the definitions.

- **Discourage early risk detection and mitigation via anti-virus software**. ISPs often bundle services with anti-virus/anti-malware software. Typically, anti-virus software stores information on consumer CPE, and anti-malware vendors aggregate the information. The Proposed Rules' broad definitions of protected data will hinder sharing, and ISPs may be discouraged from bundling anti-virus/anti-malware packages with services. Ultimately, less information will be collected and shared, and incidents will increase due to lack of early detection and mitigation.

- **Discourage beneficial de-identification**.[477] The Commission misapprehends what data needs to be subject to rigorous security. As stated above, the Commission fails to distinguish between sensitive and non-sensitive data, including publicly-available information and data that has been de-identified. Rules that treat de-identified data the same as other sensitive data remove incentives to de-identify.[478] This would be unwise, as de-identification facilitates information sharing[479] and yields security benefits (de-identified data is a less attractive target, and less harmful if accessed). These benefits will not be realized if the incentive to de-identify is reduced or eliminated.

- **Undermine prudent data segregation**. Providing consumers a broad right of access and correction, and a dashboard[480] with all of a customer's information in one place, could be dangerous. It could create a new attack vector for cyberattackers who could be able to obtain massive amounts of data from one place.

The Commission's approach also threatens to degrade the user experience. For example, micromanaging customer-ISP interactions, particularly in areas of authentication, passwords, and

[476] *See, e.g.*, *NPRM*, 31 FCC Rcd at 2514-15 ¶ 41 (treating MAC addresses as CPNI).

[477] *See supra* Part I.C.2.

[478] *See supra* Part I.C.2.

[479] *See supra* notes 111-115 (discussing public interest benefits of de-identification).

[480] *NPRM*, 31 FCC Rcd at 2533 ¶ 95 (setting forth the "dashboard" concept which would, among other things, allow consumers to "request correction of inaccurate customer PI"). *See supra* Part IV.B., notes 329-330 (explaining why consumers may not benefit from dashboards).

access, threatens to slow or complicate access to information and services. ISPs already receive complaints about burdensome steps in place to manage accounts via phone and online.[481] Imposing additional steps, or pushing customers to online dashboards, is likely to frustrate many customers. Likewise, obligations about complex and sensitive issues like software updates and patching can have operational impacts and impact user experience, for better and worse.[482]

b. The Commission's Approach Fragments the Ecosystem by Regulating ISP and Edge Security Differently, and Having Different Rules Based on Service Type.

The Commission's approach introduces two pernicious distortions: different security obligations for ISPs and edge providers, and different rules for the same company depending on whether data relates to voice or data service. Both are harmful. *First*, imposing prescriptive security requirements on ISPs when other players—like edge providers—are subject to the FTC's case-by-case regime will fragment the ecosystem. It is confusing and, at bottom, arbitrary and capricious. There is no reason a consumer would expect that online security or data practices will vary dramatically, with ISPs being subject, for example, to detailed authentication obligations or prohibitions on data collection,[483] while social media companies are not. It will be difficult for consumers to appreciate the difference between ISPs and edge providers enough to understand that one could only hold data for a certain amount of time, while the other has no such limitations.

---

[481] *See supra* Parts V.B.2-V.B.3 (discussing costs for consumers from imposing heightened consent requirements that do not accord with customer expectations).

[482] NIST has explained that there are "challenges that complicate patch management," for example, "installing a patch may 'break' other applications," "forcing application restarts, operating system reboots, and other host state changes [may be] disruptive and could cause loss of data or services," and downloading large patches over certain networks—like mobile networks—"may be technically or financially infeasible." Murugiah Souppaya and Karen Scarfone, *Guide to Enterprise Patch Management Technologies* vi-vii (NIST Special Publication 800-40 Revision 3, July 2013), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf. NIST cautions that "organizations need to balance the need to get patches applied with the need to support operations." *Id.* at vii.

[483] *NPRM*, 31 FCC Rcd at 2572-74 ¶¶ 221–232.

Second, having two sets of rules for different categories of services is problematic. Varying rules for voice and broadband makes little sense, especially in light of the fact that customers purchase both voice and data services, often from the same companies. Customers will not expect different approaches or restrictions based on the type of service about which they are calling. Avoiding fragmentation is critical in data security, as it would be burdensome if not impossible for ISPs—especially small ISPs—to implement one set of security requirements for voice data and another set for broadband data. Small ISPs have limited staff and rely on third party software, which has to be evaluated and managed. Moreover, their customer service operations are lean. They should be focused on their businesses and not managing disparate obligations.

Most troubling, the Commission's approach seems intended to act as a one-way ratchet in favor of *more burdensome* obligations. If the Commission imposes burdensome, different rules on ISPs, it may then invoke interests in harmonization to change and expand voice CPNI rules. By embarking on its own new approach, the Commission will distort other regulatory regimes.

B. The Commission's Prescriptive Approach to Internet Data Security Is Contrary to Established Approaches and Unnecessary.

The Commission's overbroad, overly prescriptive, strict liability approach to security goes against the established body of security frameworks. Not only does the security proposal represent the opposite of the FTC's reasonable and flexible approach, it also directly conflicts with statements from Chairman Wheeler, past Commission approaches, and longstanding Administration efforts to reject heavy-handed data security regulation in favor of flexible and voluntary processes. Importantly, it undermines the efforts that both NIST and DHS have made regarding the NIST Cybersecurity Framework.

1. The Commission's Approach Is Inconsistent with the FTC Model, Which Uses a Reasonableness Standard for Data Security.

The Commission claims that its proposals are "firmly rooted" in the FTC's work and other models. Quite the contrary. The FTC expects companies to "follow commercially reasonable standards of care."[484] To the FTC, the lack of written regulations is not a bug but a feature of its approach. The FTC does not issue specific data security requirements in part because "industries and businesses have a variety of network structures,"[485] so "[t]he touchstone of the FTC's approach to data security is reasonableness: a company's data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities."[486] A case-by-case approach that includes cost-benefit analysis "saves regulated entities . . . from having to comply unnecessarily with data security standards that may be excessive in light of the circumstances."[487] The FTC recognizes there "is no[] such thing as perfect security; that reasonable security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; and that the mere fact that a breach occurred does not mean that a company has violated the law."[488] Rather than imposing the

---

[484] Brief for the Federal Trade Commission at 40, *FTC v. Wyndham Hotels & Resorts, LLC*, 799 F.3d 236 (3d Cir. 2015) (No. 14-3514). The FTC evaluates data security practices under its deceptive practices authority, and of late, its unfairness authority. While the FTC's approach has been controversial, the FTC says it allows the government and industry to evolve and evaluate practices over time, in light of changing circumstances.

[485] Plaintiff's Response in Opposition to Wyndham Hotels & Resorts' Motion to Dismiss at 12, *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 13-CV-1887), ECF No. 45.

[486] FTC, Data Security, https://www.ftc.gov/datasecurity.

[487] Plaintiff's Response in Opposition to Wyndham Hotels & Resorts' Motion to Dismiss at 22, *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 13-CV-1887), ECF No. 110.; *see also* 15 U.S.C. § 45(n). The NPRM's questions about how to modify the proposed prescriptive regime to reduce the burdens on small carriers would not be necessary if the Commission adopted a flexible reasonableness standard.

[488] Jessica Rich, *Data Security: Why It's Important, What the FTC is Doing About It* 4, FTC, National Consumers League, Alliance Against Fraud Coalition (March 24, 2014), https://www.ftc.gov/system/files/documents/public_statements/295751/140324nclremarks.pdf.

prescriptive regulation proposed in the NPRM, the Commission should consider a flexible reasonableness standard for data security, akin to the FTC model.

The Commission cites other models, including Commission and FTC settlements, as well as HIPAA, GLBA, and state laws,[489] but these models are poor fits here.[490] For example, the HIPAA security regime applies to data that Congress has deemed to be uniquely sensitive: health information held by certain entities.[491] Congress has not deemed *all* data that ISPs touch to be uniquely sensitive,[492] yet the Commission proposes to impose security regulations on all such data. Similarly, GLBA mandates that financial institutions protect the security and confidentiality of customers' nonpublic information.[493] Again, Congress has made no such mandate for ISP customer information, nor should it, as not all information handled by ISPs is inherently sensitive. As for Commission and FTC settlements, negotiated consent decree requirements for a few companies do not justify broad restrictions on everyone.

2. The Commission's Approach Is Inconsistent with Longstanding Federal Policy, Including the Prior Commission Position Favoring a Voluntary, Collaborative Approach to Data Security.

Federal policy has long emphasized a non-regulatory model that leverages voluntary, private sector collaboration through multistakeholder processes to improve security.[494] For

[489] *See NPRM*, 31 FCC Rcd at 2557 ¶168. State laws are inapt as they reflect the direction of state legislatures.

[490] In certain instances, these models could be helpful guides to the Commission; however, as discussed throughout these comments, the Commission often fails to take from these models appropriate lessons and approaches.

[491] *See* 42 U.S.C. § 1320d-2(d) (mandating security standards for health information).

[492] *See* 47 U.S.C. § 222(c) (mandating that telecommunications carriers protect a more limited dataset: CPNI).

[493] *See* 15 U.S.C. § 6801 ("It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.").

[494] *See, e.g.*, Exec. Order No. 13636, 78 Fed. Reg. 11,739, *Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2013), https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (creating a "voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and other interested entities").

example, NIST's *Cybersecurity Framework*, which was developed at the direction of the Cybersecurity Executive Order and through the collaboration of government and industry, including CTIA, is a voluntary, risk-based strategy designed to adapt and allow for innovation.[495] Likewise, DHS is the sector specific agency for communications[496] and runs the NCCIC and the Critical Infrastructure Cyber Community (C^3) Voluntary Program to help the sector use the Cybersecurity Framework and "manage their cyber risk[s]."[497]

Chairman Wheeler explained that "[o]ur nation chose" risk management "over a traditional regulatory approach of prescriptive government mandates."[498] This is sensible because "[t]he pace of innovation on the Internet is much, much faster than the pace of a notice-and-comment rulemaking."[499] The Chairman also said that the Commission will only regulate where industry approaches have been unsuccessful.[500] Yet here, the Commission seeks to burden thousands of companies with complex regulations, without any evidence of a failure of the prevailing industry approach. The Commission "recognize[s] that most [ISPs] already have robust data security measures in place."[501] ISPs have cyber security plans, and the ecosystem

---

[495] NIST Cybersecurity Framework, *supra* note 431, at 1. NIST's "voluntary consensus standards … best ensure[] the interoperability, security, and resiliency" of critical infrastructure. Kevin Stine, NIST, Confronting the Challenge of Cybersecurity, Testimony Before the Committee on Commerce, Science and Transportation, 114th Cong. 5 (Sept. 3, 2015), https://www.commerce.senate.gov/public/_cache/files/629b3130-c0d3-44af-adce-88237096a14c/5C76FD0AFAE9345A904E20300AA568F4.mr.-kevin-stine-testimony.pdf.

[496] *Communications Sector*, DHS.GOV, https://www.dhs.gov/communications-sector (last visited May 24, 2016) (laying out plans and resources on communications sector security).

[497] *See Critical Infrastructure Cyber Community Voluntary Program*, US-CERT.GOV, https://www.us-cert.gov/ccubedvp; *see also Using the Cybersecurity Framework*, DHS.GOV, https://www.dhs.gov/using-cybersecurity-framework (describing C^3 as a public-private partnership).

[498] Chairman Tom Wheeler, Remarks at American Enterprise Institute 3 (June 12, 2014), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-327591A1.pdf.

[499] *Id.* at 4.

[500] *Id.* at 1.

[501] *NPRM*, 31 FCC Rcd at 2560 ¶ 177.

has incentives to continue this hard work.[502] Rules are unnecessary, and in any event, cannot keep up with technological change and the dynamic threat landscape.

Regulating cybersecurity in this way undermines other security efforts beyond those of NIST and DHS, including in the CSRIC and the Commission's Technological Advisory Council ("TAC"), which engage the entire ecosystem. CSRIC develops technical recommendations on security[503] and the TAC advises on emerging issues, such as software-defined networks.[504] By validating industry concerns about regulation and enforcement, the NPRM also undermines voluntary cybersecurity dialogue with the Commission.[505] As Chairman Wheeler told Congress, "there is no 'correct' or 'minimum' standard against which companies will be measured" in such discussions.[506] But the Proposed Rules do just that: impose "minimum" requirements.[507]

C. If the Commission Is to Regulate, It Must Change Its Approach to Avoid Disrupting Existing Rigorous ISP Security.

1. The Commission Should Not Impose a Sweeping Security Standard on ISPs.

If the Commission has authority to regulate ISP security and chooses to do so, it should not impose the overbroad standard proposed. The Proposed Rules require ISPs to "ensure the

---

[502] *See, e.g.*, CSRIC WG 4 Final Report, *supra* note 432, at 8 ("[M]any communications companies have long-standing and mature cybersecurity risk management capabilities . . . . Reducing cybersecurity risk by implementing widely recognized standards and guidelines has been a hallmark of communications industry practice, and is supported by exceptionally high levels of service availability.").

[503] *See generally id.* at 4.

[504] *Technological Advisory Council*, FCC.gov, https://www.fcc.gov/general/technological-advisory-council (last visited May 25, 2016) (describing TAC and linking to recent reports).

[505] It appears that cyber assurance meetings would happen outside the protected critical infrastructure information (PCII) construct called for by CSRIC, which recommended that "the FCC, in partnership with DHS, participate in periodic meetings with communication sector members, in accordance with PCII protections" or "another legally sustainable construct." CSRIC WG 4 Final Report, *supra* note 432, at 30, 30 n.37; *see also id.* at 6, 7, and 385. Industry has been willing to work with the Commission on CAMs, but regulation here threatens to chill cooperation.

[506] U.S. Senate Comm. on Commerce, Science, & Transp., Written Question Submitted by Hon. John Thune and Responses by Chairman Tom Wheeler 9, http://www.commerce.senate.gov/public/_cache/files/6d3caac4-4a5c-4614-96b5-5f39eaef1379/8692A68293184CC559A17FFAB736FAB4.wheeler-qfrs.pdf.

[507] *NPRM*, 31 FCC Rcd at 2608-09 App. A (proposed rule § 64.7005(a)).

security, confidentiality, and integrity of all [customer proprietary information]."[508] This is broader than the mandate in Section 222(c), which requires that a telecommunications carrier obtain a customer's approval before using, disclosing, or permitting access to CPNI. Indeed, the Commission cites no authority for its overbroad standard, nor is there such authority. The Commission must remain faithful to the clear intent of Congress, which cabined the scope of Section 222 with respect to customers' information to CPNI and regulated carriers' activities with respect to CPNI under Section 222(c).[509] The Commission should not address the concept of data integrity in its Proposed Rules, because this concept is wholly unrelated to the statutory obligations governing CPNI. Instead, the Commission should focus on data security, which, as with existing CPNI obligations, naturally flows from the requirement to obtain approval before disclosing or permitting access to CPNI.[510]

2. The Commission Should Eschew Strict Liability in Favor of a Reasonableness Standard.

The proposed security rule unrealistically imposes strict liability on ISPs. As proposed, ISPs "must *ensure* the security, confidentiality, and integrity of *all* [*"customer proprietary information"*] the [ISP] receives, maintains, uses, discloses or permits access to from *any* unauthorized uses or disclosures, or uses exceeding authorization."[511] The Commission sets out "minimum" requirements to achieve this expansive standard. The sweeping rule is unrealistic, ignores real risk management, and is a stark departure from the FTC's approach. The

[508] *Id.*

[509] *See supra* Part I.C.

[510] *See* 47 U.S.C. § 222(c)(1) (requiring carriers to obtain customer approval before disclosing or permitting access to CPNI).

[511] *NPRM*, 31 FCC Rcd at 2608-09 App. A (proposed rule § 64.7005(a)) (emphasis added).

Commission should abandon its attempt to prescriptively regulate, or if it does regulate, at least use a reasonableness standard.

A strict liability approach is unrealistic. The Commission's standard, coupled with its proposed broad definitions, would result in nearly every piece of information that ISPs hold or touch being subject to data security, access, and correction obligations—even publicly available information. This turns the existing CPNI security rules—which are not perfect—into a breathtaking obligation to meet an unrealistic standard. The NPRM goes far beyond existing CPNI protection, and improperly imports aggressive compliance efforts developed by the Commission's Enforcement Bureau in data security-related consent decrees.

The strict liability approach also flies in the face of cybersecurity learning. As explained, security is about risk *management*; there is never total risk mitigation, and even reasonable and appropriate measures will not stop all attacks.[512] Additionally, strict liability is antithetical to the FTC's policy and enforcement approach to data security. The FTC expects companies to "take care to *reasonably* secure consumers' data"[513] and uses a case-by-case approach. The FTC guides companies to "make *reasonable* [security] choices based on the nature of their business and the sensitivity of the information involved."[514] The Commission would do better to require entities to take reasonable measures to protect more limited information, as comports with common sense and the superior approach of the FTC. Ultimately, the best approach is to reject prescriptive regulation.[515] CTIA urges the Commission to engage in the productive work of the

---

[512] *See supra* Part VI.A.1.

[513] FTC, *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues* iv (Jan. 2016), *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf (emphasis added).

[514] FTC, *Start with Security*, *supra* note 468.

[515] *NPRM*, 31 FCC Rcd at 2560 ¶ 177.

CSRIC, NIST, DHS and others on security, using the multistakeholder process that has worked well.

3. Any Rules the Commission Adopts Must Provide More Flexibility.

Further, if the Commission is to regulate in this area, CTIA urges it to build more flexibility into its rules. As drafted, the rule lacks flexibility, despite the NPRM's rhetoric. The NPRM purports to propose a security regime that is "calibrated to the nature and scope of the [ISP]'s activities, the sensitivity of the underlying data, and technical feasibility."[516] However, the proposed rule appears to adopt a one-size-fits-all approach. If the Commission is serious about creating flexible rules, then the text of the rule must reflect that commitment.

The Commission should explicitly draft flexibility and scalability into its security rule in two ways: (1) regarding what requirements apply, and (2) regarding how ISPs decide to achieve them. First, the Commission should not impose "minimum" obligations for all ISPs.[517] The Commission should instead give ISPs flexibility regarding the requirements by which they have to abide. Giving ISPs flexibility around what rules apply, based on factors like the ISP's size, is a better approach given the context-specific nature of cybersecurity.[518] The Commission should reject its one-size-fits-all, "minimum" obligation approach, and instead model flexibility and scalability.

Second, the Commission should allow ISPs more flexibility to determine the measures used. As drafted, the Commission's Proposed Rules allow individual ISPs to "employ any

[516] *Id.* at 2558 ¶ 169.

[517] *Id.* at 2608-09 App. A (proposed rule § 64.7005(a) ("At minimum, this requires a[n ISP] to . . . .")).

[518] This approach is also more in line with HIPAA, which the Commission repeatedly claims to be modeling. *See* 45 C.F.R. § 164.306(d). Under the HIPAA regime, some security standards are "required" and some are "addressable," leaving a regulated entity the ability to "[a]ssess whether [the] specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic health information," and act accordingly, maintaining appropriate documentation. *Id.*

security measures that allow the [ISP] to reasonably implement the requirements set forth in [the rule]."[519] This is a good start to building flexibility into the text, and it is in line with other privacy regimes;[520] unfortunately, it is undone by the language in subsection (a) of the rule, which sets out a strict liability approach.

Even if the strict liability approach did not undo the Proposed Rules' built-in flexibility regarding how an ISP can achieve the security obligations, the factors that the Commission proposes to guide this determination are under-inclusive. The Proposed Rules could be improved by explicitly including additional factors. The Commission's proposed factors—(1) "the nature and scope of the [ISP]'s activities" and (2) "the sensitivity of ["]customer proprietary information["] held by the [ISP]"—do not go far enough. Following the HIPAA model,[521] the Commission should expressly permit companies to consider other factors, including (1) the nature of threats and risks they face, (2) the likelihood of actual harm to consumers, and (3) the costs of security measures. A more inclusive list might expand on and make express reference to NIST's "impact levels."[522]

4. The Proposed Risk Management Assessment and Remediation Mandate Is Overly Burdensome and Unrealistic.

The Commission should abandon its risk management assessment and remediation mandate. There is no reason for the Commission to mandate risk assessments. Companies

[519] *NPRM*, 31 FCC Rcd at 2609 App. A (proposed rule § 64.7005(b)).

[520] *See, e.g.*, *FTC Big Data*, *supra* note 513, at iv.

[521] A good model in this regard is HIPAA's Security Rule, which lists the following factors: "(i) The size, complexity, and capabilities of the covered entity or business associate. (ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities. (iii) The costs of security measures. (iv) The probability and criticality of potential risks to electronic protected health information." 45 C.F.R. § 164.306(b)(2)(i)-(iv).

[522] *NPRM*, 31 FCC Rcd at 2571-72 ¶ 220 & n.350 (citing NIST, Special Publication 800-60 Rev. 1 (Volume 1, Volume 2), Guide for Mapping Types of Information and Information Systems to Security Categories, http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf and http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf).

already do appropriate risk assessments and remediation, guided by their needs, supply chains, partnerships, and resources, as well as by changing approaches, like the NIST Cybersecurity Framework.

Even if the Commission decides to impose a mandate, the Proposed Rules are deeply flawed. Under the current proposal, the Commission would require ISPs to "[e]stablish and perform regular risk management assessments and *promptly* address *any weaknesses* in the provider's data security system identified by such assessments"[523] Instead of forcing ISPs to detect and mitigate all weaknesses, the Commission should look to industry best practices and corresponding regimes. As discussed, requiring perfect protection from all weaknesses conflicts with risk management best practices, and may lead to less secure networks.[524] Risk management—including identification and mitigation—is not about perfect protection, as all risks are not equal. Risk management is about identifying real risks, in context, and reducing them to acceptable levels. Best practices call for mitigation to be linked to materiality, and for companies to take into account risk profile and other factors. Other security regimes, like HIPAA and GLBA, recognize this and have reasonableness built into their risk assessment rules.[525]

Further, the Commission's proposal is overly burdensome and unrealistic. The stunning breadth of the proposed risk management assessment and mitigation mandate—which starkly

[523] *NPRM*, 31 FCC Rcd at 2608-09 (proposed rule § 64.7005(a)(1)).

[524] *See supra* Part VI.A.2.

[525] HIPAA requires a risk analysis and risk management. The regulated entity must "implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level" to comply with HIPAA's general requirements. 45 C.F.R. § 164.308(a)(1)(ii)(B). Likewise, GLBA has a reasonableness standard. GLBA requires entities to "identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks." 16 C.F.R. §314.4(b). Entities must "design and implement information safeguards to control the risks . . . . identif[ied] through risk assessment." *Id.* § 314.4(c).

differs from other regimes in that it attempts to regulate virtually all data touched by the regulated entity[526]—will overly burden ISPs. Moreover, mandated assessments are likely to cost millions of dollars and take substantial time. This burden is not justified, especially because it will divert resources from real risks. Moreover, the expansive mandate is not based in reality, as it does not consider potential difficulties of dealing with various other entities in the ecosystem, including software providers, hardware manufacturers, operating system providers, OEMs, and the like.

If the Commission decides to mandate risk assessments, it should leave particulars to industry experts. Technical mandates are generally a bad approach, and risk management is no different.[527] Dictating specifics also may have other unintended, negative consequences. For example, in the NPRM, the Commission considers defining "promptly" as it relates to the timing of mandated remediation.[528] Such a prescriptive approach may result in poor prioritization of remedial measures based on chronological order, rather than risks. Finally, risk management is dynamic and organization specific, so the Commission is not in the best position to dictate specifics. Risk assessments are iterative and focus on understanding the systems in use, attack surface, and vulnerability to known or foreseeable risks. Risk assessments are an ongoing part of providing information and telecommunications services. For example, risk assessments to evaluate possible vulnerabilities would typically take place when a new platform is placed into service or a new service is turned on. The Commission does not have the information necessary to dictate the specifics of such assessments; cybersecurity experts do.

---

[526] *See* 45 C.F.R. § 164.302 (regulating only a confined data set—electronic protected health information).

[527] *See supra* Part VI.B.1.

[528] *NPRM*, 31 FCC Rcd at 2562 ¶ 184.

The Commission should abandon its idea to dictate specifics in assessment and remediation timing, penetration testing, and technical audits, among others.[529] The notion of "regular" assessments, annual or otherwise, reflects a lack of appreciation of the platforms, networks, and services offered by an ISP, as well as the diversity of threats and assessments routinely done throughout ISPs' systems. Dictating the timing of risk assessments makes no sense. In many instances, a new threat is discovered or reported by researchers and a risk assessment is executed to evaluate the vulnerability. This cannot be regularly scheduled. Similarly, penetration testing can be helpful, but the Commission should not require it. Penetration testing is a small part of overall risk management, and tends to be most effective to test new systems prior to launch. Tests involve specific attacks and are expensive, so the decision to perform them is best made by network experts, not by regulators. Likewise, the Commission does not have the expertise or understanding of each ISP's network to vet audit programs.

5. The Commission Should Not Hold ISPs Accountable for Third-Party Actions.

The Commission asks whether it should hold ISPs accountable for the actions of third parties.[530] The answer is no. Though it is important for everyone in the ecosystem to protect sensitive data, both the premise for, and the process of, extending Commission authority by imposing third-party liability on ISPs is unsound. Consistent with the approach in the NPRM, the Commission should not regulate in this area.

Any action to extend the Commission's regulatory authority over ISPs to third-party actors would be based on a flawed premise. The Commission states that "[c]onsumers may be

[529] *Id.* at 2561-62 ¶¶ 181, 184.

[530] *Id.* at 2569-70 ¶¶ 210-214.

apprehensive about disclosing their personal information to [ISPs] if they cannot trust that their data will not be misused downstream."[531] However, this purported problem is not rooted in reality. The Commission has no empirical evidence that this "problem" has impeded broadband adoption or has made consumers scared of ISPs.

Similarly, there is neither authority nor need for the Commission to regulate the behavior of third parties via ISPs. Most important, the Commission's Section 222 authority is limited to telecommunications carriers. Moreover, non-telecommunications providers are already regulated under other regimes. For example, many vendors are regulated by the FTC, state law, and self-regulatory regimes, and are liable for their own conduct under those regimes. Similarly, third parties, just like ISPs, have non-regulatory incentives to secure data, including public relations, consumer and business client confidence, and contractual requirements that would result in large monetary payments by the vendors for breaches. And the Commission itself acknowledges that the existing model of protection based on contractual agreements works.[532] Therefore, the existing model should be left alone.

CTIA agrees that it is important to protect customer data accessed by contractors. However, the process the Commission envisions for protecting this data is problematic. Extending direct or vicarious liability to ISPs for the actions of third parties—for the *entire lifespan* of data—is unrealistic and unworkable, as ISPs lack control over third-party systems and operations.[533] And holding ISPs liable for the acts of third parties will have a disproportionate effect on small ISPs, who have to contract out more often and more extensively. This is especially true if the liability extends to the entire lifespan of the data.

[531] *Id.* at 2569 ¶ 210.

[532] *Id.* at 2569 ¶ 212

[533] *See supra* Part VI.A.1.c

Should the Commission nevertheless elect to regulate, any ISP obligation should be clear and limited.[534] First, any requirement must be general. There are already market incentives for ISPs to utilize contractual provisions in ways that make sense. It is enough for the Commission to expect that ISPs have contracts with third parties to safeguard data; the Commission should not require specific commitments. Second, any requirement should be limited to contractors and not extend to relationships between ISPs, OEMs, application developers, operating system providers, or others in the Internet ecosystem. Wireless ISPs should not be required to use negotiations with others, like device manufacturers and operating system providers, to get commitments on security. The Commission should be careful to limit expectations, lest it end up using ISPs to effectively regulate the edge. ISPs are also not in a position to demand or ensure compliance by entities like device manufacturers and operating system providers. In a world in which the Commission wants consumers to be able to choose their own devices,[535] it is clear that ISPs do not control the design and maintenance of devices, apps, or operating systems. Manufacturers—not ISPs—should be responsible for the security of their own devices, applications and systems.

6. A Right to Access and Correct Customer Data Is Ill-Conceived, Unworkable, and of No Benefit to Consumers.

Likewise, CTIA urges the Commission to abandon its interest in creating a new and broad ability for consumers to access and correct all their "customer proprietary information" held by ISPs.[536] Such an endeavor is ill-conceived. It is akin to the "right to be forgotten" that

---

[534] *NPRM*, 31 FCC Rcd at 2569 ¶ 212

[535] FCC, *Cell Phone Unlocking FAQs*, https://www.fcc.gov/consumers/guides/cell-phone-unlocking-faqs (last visited May 25, 2016).

[536] *NPRM*, 31 FCC Rcd at 2568-69 ¶¶ 205-209.

the EU has pursued and should not be adopted in the United States for any part of the Internet.[537] Among other things, this approach is burdensome and chills speech on the Internet.[538]

Similarly, it makes little sense to put this sweeping requirement on ISPs. The Commission acknowledges that "edge providers, data brokers, and other entities in the Internet ecosystem also collect, process, retain, and distribute large quantities of sensitive consumer data" and asks if it should "consider the restrictions, or lack thereof, that are currently placed on edge providers or other entities in crafting [these right to access/correction] rules for broadband providers."[539] It should. Edge providers do not have this obligation and ISPs should not either. As discussed above, such a broad right is ill-conceived and could have the unintended consequence of endangering—rather than safeguarding—data.[540]

Moreover, the concept is unworkable, as evinced by the numerous complex questions packed into the NPRM.[541] For example, disputes over accuracy and correction of consumer data would be highly complex and create enormous burdens on ISPs, particularly small ISPs. And any requirement that the covered data (meaning virtually all data) should be available to

---

[537] The EU has found that "individuals have the right—under certain conditions—to ask search engines to remove links with personal information about them. This applies where the information is inaccurate, inadequate, irrelevant or excessive for the purposes of the data processing." *See* European Commission, Factsheet on the "Right to be Forgotten" Ruling (C-131/12), http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

[538] *See* Jeffrey Rosen, *The Right to Be Forgotten*, 64 Stan. L. Rev. Online 88 (2012), *available at* http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten; *see also* Jason Wright, *Some Things Should Not Be "Forgotten,"* Wall St. J. (Jan. 19, 2015 12:36 PM), http://www.wsj.com/articles/jason-wright-some-things-should-not-be-forgotten-1421689011 ("As a committee of the British House of Lords recently described it, the newly enforced 'right' is 'misguided in principle and unworkable in practice.' When applied in a business context it hinders openness and availability of information, making it easier for fraud and corruption to flourish.")

[539] *NPRM*, 31 FCC Rcd at 2568 ¶ 206.

[540] *See supra* Part VI.A.2.a.

[541] *NPRM*, 31 FCC Rcd at 2568-69 ¶¶ 205-209.

customers in "useable form" is simply unwieldy.[542] ISP systems are not customer-facing systems, nor should they be. And applying this already complex idea of a sweeping right to access and correction to the sprawling definitions of "customer proprietary information" and "customers" makes it even more unworkable.[543]

Further illustrating the complexities are questions about third-party access.[544] Section 222 requires that "[a] telecommunications carrier shall disclose customer proprietary network information, upon affirmative written request by the customer, to any person designated by the customer."[545] Any broadband model should follow the voice approach, which does not elaborate on how a voice customer can authorize third party access,[546] and be as simple as possible.

It makes little sense to consider imposing such a complex and unworkable obligation on ISPs when the actual right of access and correction will be of dubious utility to consumers. It is unclear what the Commission envisions consumers would be accessing and correcting: URLs, old IP addresses?[547] Based on the type of information held by ISPs, there is no obvious consumer benefit or potential utility, which makes the case for access and correction of data held

---

[542] *Id.* at 2568 ¶ 206.

[543] Other regimes that grant similar rights are more limited. For example, under HIPAA, generally, the right of access and amendment applies to data that is contained in a "designated record set." *See* 45 C.F.R. §§ 164.524(a)(1), 164.526(a)(1). And FCRA applies to data used for specified eligibility decisions—like insurance, credit, and employment decisions. "The regulatory framework created by the legislation established a set of rights and responsibilities for the collection and use of personal information when used for certain specified eligibility decisions. When, in Congress's judgment, information was used in ways that risked substantially affecting a person's life chances in a negative way, it was brought under this regulatory framework. Other uses of information were left outside of this framework." *See* Software & Information Industry Association, *How FCRA Protects the Public*, Software & Information Industry Association (Dec. 2013), https://www.ftc.gov/system/files/documents/public_comments/2014/04/00010-89272.pdf.

[544] *NPRM*, 31 FCC Rcd at 2568-69 ¶ 208.

[545] 47 U.S.C. § 222(c)(2).

[546] *NPRM*, 31 FCC Rcd at 2568-69 ¶ 208.

[547] *See supra* Part I.C.3 (arguing that CPNI in broadband context must exclude, at least (1) Geolocation information other than precise geolocation information to which other companies have no access; (2) Home router MAC addresses; (3) Traffic statistics; (4) Port Information; (5) IP addresses; (6) Domain name information; (7) Application headers; (8) Application usage; and (9) CPE information).

by ISPs different from the case of health or credit information.[548] Worse, the proposed right will create a target for cybercriminals out of customers' newly centralized data.[549]

The Commission therefore should refrain from adopting any regulations that would require ISPs to allow consumers to access and correct all data. However, *if* the Commission wrongly decides to impose such a requirement, it certainly should not require ISPs to give notice of this right to consumers, as proposed in the NPRM.[550] Companies can and should determine on their own reasonable and appropriate notice. And as discussed above, such notices will do little to inform or empower consumers, and instead will simply lead to notice fatigue for consumers and create an enormous burden for companies, with no benefit for either.[551]

7. The Commission Should Avoid Granular Regulation Which Imposes Costs Without Security Benefits and Threatens to Freeze Practices in a Rapidly Changing Area.

Despite the Commission's claim that it is not mandating specific security techniques,[552] it considers and proposes just that. The Commission should not go down this path. The Commission should leave operational issues to the experts: security personnel and engineers in the private sector. The Commission's inquiries raise complex issues, but are insufficiently

---

[548] For example, there can be specific consumer utility in easy access to and correction of health information: "[I]ndividuals with access to their health information are better able to monitor chronic conditions, adhere to treatment plans, find and fix errors in their health records, track progress in wellness or disease management programs, and directly contribute their information to research." *See* Individuals' Right under HIPPA to Access their Health Information 45 C.F.R. §164.524, HHS.gov, http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/ (last visited May 25, 2016). Similarly, accessing credit information has real benefits for consumers. Incorrect information in credit reports may affect whether a consumer can get a loan and how much they will pay to borrow money—so incorrect information can tangibly harm consumers. *See* Consumer Information, Disputing Errors on Credit Reports, Consumer.ftc.gov, https://www.consumer.ftc.gov/articles/0151-disputing-errors-credit-reports (last visited May 25, 2016).

[549] *See supra* Part VI.A.2.a.

[550] *NPRM*, 31 FCC Rcd at 2569 ¶ 209.

[551] *See supra* Part IV.A.

[552] *NPRM*, 31 FCC Rcd at 2560 ¶ 176 ("[W]hile requiring the regulated entities to install protocols and safeguards that are available and economically justified, we propose not to specify technical measures for implementing the data security requirements outlined below.").

formed, so any further Commission action would require more specifics and a new proposal for comment. The Commission should not adopt prescriptive mandates requiring or addressing the following:

- **Network Segmentation.**[553] Network segmentation is complex and evolving.[554] Software defined network (SDN) technology and network function virtualization (NFV) are "very young in terms of technological maturity" so there will be "future work for the FCC and other organizations as SDN and NFV mature and operational standards and best practices are adopted."[555] Traditional understandings of segmentation are not suitable for a Commission mandate.

- **Software updates.**[556] Software lifecycle management is important, but "depend[s] on the complexity of [an entity's] network" and can introduce security risks.[557] A joint Commission-FTC inquiry currently is underway on mobile security and updates, confirming the utility of joint, collaborative efforts.[558] Because the issue is already under review in a collateral, inter-agency process, it need not be addressed here.

- **Encryption.**[559] Encryption is complicated and has tradeoffs. Encrypted data requires more bandwidth to transmit, decreasing speed and capacity. There are other technical challenges: "legacy applications, may also make it extremely difficult, if not impossible, to implement[.]"[560] And policy and consumer expectations are in flux. It

[553] *See NPRM*, 31 FCC Rcd at 2570 ¶ 215.

[554] *Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach* 10 (NIST, Special Publication 800-37, Feb. 2010), http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf ("One of the most challenging problems for information system owners … is identifying appropriate boundaries for organizational information systems.").

[555] *See* FCC, *White Paper: Considerations for Securing SDN/NFV* 63, 65 (Jan. 2016), https://transition.fcc.gov/bureaus/oet/tac/tacdocs/reports/2016/Securing%20-SDN-NFV%20-SWG-WP-Final.pdf

[556] *See NPRM*, 31 FCC Rcd at 2570 ¶ 215. The Commission also asks about "restricting access to sensitive data" and "requiring secure access for employees, agents, and contractors," among other things. *Id.* The Commission should not mandate those or other specific obligations. Secure access for employees, agents, and contractors is part of normal risk management, would be subject to definitional issues, will change over time, and is not suitable for a Commission mandate.

[557] FTC, *Start with Security*, *supra* note 468, at 12.

[558] Press Release, FCC Wireless Telecommunications Bureau Launches Inquiry into Mobile Device Security Updates, (May 9, 2016), https://apps.fcc.gov/edocs_public/attachmatch/DOC-339256A1.pdf.

[559] *See NPRM*, 31 FCC Rcd at 2570-71 ¶ 216 (asking if Commission should mandate or encourage encryption).

[560] SANS Whitepaper – April 2010, Transparent Data Encryption: New Technologies and Best Practices for Database Encryption, available at https://www.sans.org/reading-room/whitepapers/analyst/transparent-data-encryption-technologies-practices-database-encryption-34915.

is premature for the Commission to consider encryption mandates while law enforcement access issues are fluid.[561]

- **User authentication/password requirements.** ISPs ensure proper authentication in customer information security planning.[562] There is no need to micromanage specifics. Multifactor authentication[563] is a good security practice in many settings, but presents trade-offs in costs (hardware or software tokens), identity management challenges, and customer service. And there is no need to mandate passwords or criteria, like secret questions or character limits.[564] Some customers will be frustrated by the expense and hassle of tokens, password reset obligations, and proliferating, arcane challenge questions ("what is your paternal grandfather's middle name?"), which will increase service calls. ISPs should determine what works best. Relatedly, and especially here, the Commission would have to consider harmonization. Different methods for customers to access accounts and data—depending on whether data is connected to voice or broadband services—is unworkable.

- **Account change notifications.** Account change notices contribute to notice fatigue, particularly if triggered too easily. There is no epidemic of pretexting-like fraud[565] circumventing ISP controls, so remedial approaches from 2007 are inapt. Threats are different and constantly changing, and ISPs and others have robust security and anti-fraud capabilities that have changed the landscape.[566]

- **Training or corporate officer selection.** The Commission should avoid regulation of internal operations, like hiring criteria and training. ISPs know best what training and personnel will help them manage risk in their diverse organizations. The NPRM would convert training requirements from recent negotiated consent decrees into

---

[561] *See, e.g.*, *The Encryption Tightrope*, House Comm. on the Judiciary, 114th Cong. (2016) (statement of FBI Director James B. Comey), https://www.fbi.gov/news/testimony/encryption-tightrope-balancing-americans-security-and-privacy.

[562] The FTC's chief technologist recently noted that long-standing advice about changing passwords has been wrong—what once was a best practice should be reconsidered. *See* Lorrie Cranor, *Time to Rethink Mandatory Password Changes*, FTC Blog (Mar. 2, 2016), https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes ("Mandated password changes are a long-standing security practice," but "this practice may be less beneficial than previously thought, and sometimes even counterproductive.")

[563] *NPRM*, 31 FCC Rcd at 2564-65 ¶¶ 193-194.

[564] *Id.* at 2565-66 ¶ 197.

[565] *2007 CPNI Order*, 22 FCC Rcd at 6928 ¶ 1.

[566] *See* Jessica Rich, Director of the Bureau of Consumer Protection, FTC, Discussion Draft of H.R. __, Data Security and Breach Notification Act of 2015, at 14, Testimony Before the Subcomm. on Commerce, Manufacturing, and Trade of the H. Comm. On Energy and Commerce, 114th Congress 14 (Mar. 18, 2014), http://docs.house.gov/meetings/IF/IF17/20150318/103175/HHRG-114-IF17-Wstate-RichJ-20150318.pdf ("any trigger for providing notification should be sufficiently balanced so that consumers can take steps to protect themselves when their data is at risk, while avoiding over-notification, which may confuse consumers or cause them to ignore the notices they receive.").

broadly applicable rules.[567] The Commission should not export to thousands of ISPs obligations agreed to by a few companies to end enforcement actions. Small companies in particular need flexibility.

8. The Commission Lacks Legal Authority or Basis to Regulate ISPs' Collection, Retention, and Disposal of Data.

The Commission asks questions about whether to regulate data minimization, including limits on collection, retention, and disposal.[568] As discussed above, the Commission's authority under Section 222 is limited to regulating the use, disclosure, and permitting access to CPNI, and the Commission's authority under Section 705 is limited to regulating malfeasance. The Commission therefore has no statutory authority to regulate ISP data collection, retention, and disposal.[569] Whereas Congress has specifically mandated data collection, retention, or disposal requirements in other verticals, like cable or satellite, there is no such specific mandate for ISPs.[570] The Commission does not have authority to export the data minimization obligations from statutes like the Cable Privacy Act, the Satellite Privacy Act, and the Fair and Accurate Credit Transaction Act,[571] and therefore those statutes should not be used as models for

---

[567] *NPRM*, 31 FCC Rcd at 2562 ¶ 185 & n.303.

[568] *Id.* at 2572-74 ¶¶ 221-232.

[569] *See supra* Parts I.C.4, I.D.2.

[570] *See, e.g.*, Cable Privacy Act, 47 U.S.C. §551(e) ("A cable operator shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such . . . ."); Satellite Privacy Act, 47 U.S.C. §338(i)(6) ("A satellite carrier shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under paragraph (5) or pursuant to a court order."); Fair Credit and Accurate Credit Transaction Act, 15 U.S.C. § 1681w(a)(1) ("The Federal Trade Commission, the Securities and Exchange Commission, the Commodity Futures Trading Commission, the Federal banking agencies, and the National Credit Union Administration, with respect to the entities that are subject to their respective enforcement authority under section 1681s of this title, and in coordination as described in paragraph (2), shall issue final regulations requiring any person that maintains or otherwise possesses consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose to properly dispose of any such information or compilation.").

[571] *See Sebelius v. Cloer*, 133 S. Ct. 1886, 1894 (2013) (quoting *Bates v. United States*, 522 U.S. 23, 29–30 (1997)) ("We have long held that '[w]here Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion."); *see also Util. Air Regulatory Grp.*, 134 S. Ct. at 2442.

regulating collection and retention of ISP data.[572] This area is fraught with normative policy choices that should come from Congress, not the Commission.

In addition, mandated data minimization is not in the public interest. ISPs, like other businesses, have policies about data collection, retention, and protection, so regulation is unnecessary. As with other issues, if the Commission wants to go down this path, more review and specific proposals would be needed, given the complexity of the issues raised. Indeed, data minimization is complex.[573] An FTC report identified "the need to balance future, beneficial uses of data with privacy protection" and recommended that "data minimization" be handled "flexibl[y]" in a manner "that gives companies many options."[574] The Commission should not ban collection of specific information or mandate practices.[575] Likewise, the Commission need not regulate data retention or disposal. There are benefits to keeping data for consumer-facing and other legitimate business reasons.[576] While regular disposal can be a good practice, a mandate about what to delete and when is unnecessary and would jeopardize benefits and implicate third-party access. Given the breadth of information covered by new definitions, varied approaches may be appropriate.

---

[572] The other bases cited by the Commission do not justify forced data minimization. FIPPs are applied voluntarily by the private sector in context-specific ways. The 2012 *FTC Report* notes the utility of data minimization, but does not justify mandates.

[573] *See e.g.*, *Privacy in the Age of Big Data, A Time for Big Decisions*, 64 Stan. L. Rev. Online at 68 ("an increasing focus on express consent and data minimization, with little appreciation for the value of uses for data, could jeopardize innovation and beneficial societal advances.").

[574] FTC, *Internet of Things: Privacy & Security in a Connected World* at 38 (2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[575] *NPRM*, 31 FCC Rcd at 2572-73 ¶ 224.

[576] *White House Privacy Report* at 39-40.

VII. The NPRM Data Breach Rules Are Harmful to Customers and to Carriers, and Are Therefore Not in the Public Interest.

As CITA has argued, the Commission has exceeded its authority under Section 222 by attempting to create out of whole cloth a new protected category of information that it calls "customer proprietary information." This exceedingly broad category is uniquely problematic in the context of the proposed breach notification rules. If the record bears out that consumer concern over privacy and security is a disincentive to broadband growth, then the proposal to require the creation of additional customer anxiety through extensive notifications in situations where there has been no confirmed breach or where the breach does not create a meaningful risk of harm will amplify that disincentive. The Commission should not adopt breach notification rules without substantial record evidence that *further* notifications would boost consumer confidence in broadband privacy and security. But at a minimum, several elements of the Proposed Rules require substantial modification.

A. The Commission Should Tighten Breach Notification Requirements.

Under the Commission's Proposed Rules, a data "breach" is any instance in which "a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information."[577] This definition is too broad along multiple dimensions, and, especially in conjunction with the expansive definition of "customer proprietary information," guarantees that ISPs will have to report minor non-harmful breaches, which reporting is costly to ISPs and of no use to consumers. As discussed here, to ensure consumers benefit from breach notices, the definition of breach should include a consumer harm threshold and an intent requirement (and/or an exception for good-faith access).

[577] *NPRM*, 31 FCC Rcd at 2525-26 ¶ 75 (quotation marks omitted).

1. The Commission Should Require Notification Only Where Harm Results or Is Likely to Result from Breach.

The Commission should require notification only if a breach causes harm or is likely to cause harm. Notifying customers of a data breach when no harm has occurred will not protect consumers. On the contrary, it will cause confusion and, through over-notification, will lead consumers to disregard notices even when harm has occurred. While failing to protect consumers, the Proposed Rules also will create confusion among many entities seeking to comply with both federal and state data breach notification laws.

The NPRM framework is at odds with the law in many states. The NPRM acknowledges that a number of states do not require companies to notify consumers when they have determined that no harm resulted from the breach,[578] and that other states require notification only if there is a likelihood of misuse or harm to the consumer.[579] Indeed, in some states, laws are calibrated to a particular type of harm, such as "substantial economic loss," or a reasonable likelihood or reasonable belief that the breach will cause "identity theft or fraud."[580]

In addition, the definition of "Personal Information" covered by state data breach laws generally is significantly narrower than the scope of information covered in the NPRM. For instance, the Arkansas Code defines "Personal Information" as an individual's first name or first initial, plus last name in combination with any of the following data elements, when either the name or the element is not redacted: Social Security number; driver's license or Arkansas identification card number; account number, credit card number, or debit card number in

[578] *NPRM*, 31 FCC Rcd at 2576 ¶ 237 n.371 (citing Alaska Stat. § 45.48.010(c); Arizona Stat. § 44-7501(G); Conn. Gen. Stat. § 36a-701b(b)(1)).

[579] *NPRM*, 31 FCC Rcd at 2576 ¶ 237 n.372 (citing Vt. Stat. Ann. Tit. 09 § 2435(d)(1); Md. Com. Law Code Ann. § 14-3504(c)).

[580] *Id.* at 2576 ¶ 238 & n.375 (citing Arizona Stat. § 44-7501(L)(1), Ky. Rev. Stat. § 365.732(1)(a)).

combination with any required security code, access code, or password that would permit access to an individual's financial account; and medical information.[581]

Furthermore, absent harm to consumers from a breach, there is no need to require ISPs to report every data breach with over 5,000 affected customers to the FBI and Secret Service. As discussed throughout these comments, the Proposed Rules' definition of "customer proprietary information" is sufficiently expansive that the mere disclosure of a customer's name could trigger a notification requirement, risking, among other things, to overextend law enforcement agencies that are already overburdened.

CTIA strongly disagrees with the NPRM's proposal to require notice to consumers when a breach has *not* occurred but when there is a discovery of conduct "that would reasonably lead to exposure of customer [proprietary information]."[582] This approach does not benefit consumers, and it is likely to lead to customer confusion, uncertainty, and overreaction. Further, over time, receipt of notification after notification of non-events would lessen the impact of notifications to consumers when an actual breach of sensitive data occurs. It also could lead to direct consumer harms, such as if a consumer were to request a credit freeze under the mistaken belief that the possibility of exposure of certain non-sensitive information, with little to no risk of identification, could lead to fraud or identity theft.

2. The Commission Should Adopt an Intent Requirement, or, at the Very Least, an Exception for Good Faith Access.

Compounding the problem of not distinguishing a harmful breach from non-harmful breaches is the fact that the NPRM definition of breach has no intentionality requirement. The end result is that the Proposed Rules will require ISPs to provide *the same* notice to consumers of

[581] Ark. Code § 4-110-103(7).

[582] *NPRM*, 31 FCC Rcd at 2577 ¶ 242.

inadvertent, non-harmful breaches and of intentional, harmful breaches. This, in turn, will cause consumers to ignore notifications about sensitive information about which they might otherwise want and need to know.

The NPRM seeks comment on whether to include an intent requirement, stating that many state data breach retention laws do *not* include such a requirement, and acknowledges that some states include an exception for good faith access to covered data by an employee or agent where the information was not used improperly and was not further disclosed.[583] It also asks whether to include an exception in its definition.[584]

CTIA strongly urges the Commission to include an intent requirement in its definition of data breach. Under the Proposed Rules, a data breach would occur when an employee improperly accesses any of the following: a customer's name and telephone number, the port accessed by the customer's browser, or the traffic data from his or her connection.[585] Another example of a disclosure of innocuous data that would qualify as a "breach" would be the unauthorized disclosure of a small amount of service tier data (*e.g.*, speed), tied to identifiable information such as the account holder's name. Any such access is "reportable" under the rules, even if it is the result of an employee's inadvertent mistake in the ordinary course of business—regardless of size or scope or consumer impact. Put simply, as recognized by other data security

[583] *NPRM*, 31 FCC Rcd at 2577 ¶ 243 & n.383 (citing Haw. Rev. Stat. § 487N-1)); *see also* Ark. Code § 4-110-103(1)(B); Colo. § 6-1-716(1)(a); Mass. Gen. Laws § 93H-1; Wyo. Code § 40-12-501).

[584] *NPRM*, 31 FCC Rcd at 2526 ¶ 76 (citing Alaska Stat. § 45.48.090; Ga. Code Ann. § 10-1-911(1); Ariz. Rev. Stat. § 44-7501(L)(1)).

[585] *Id.* at 2521-22 ¶ 62.

regimes, an employee's inadvertent opening of the wrong customer file should not constitute a data breach.[586]

In the event that the Commission does not adopt an intent requirement, at the very least it *must* adopt a flexible and broad exception for good faith access to covered data by employees, agents, and vendors. To be effective, such an exception cannot be limited to only employees and agents, but instead must apply to any vendor to the extent that the vendor's access does not cause harm to consumers. Otherwise, the statute would cover accidental access, even if there is no resulting harm to consumers. As described below, the rule as currently proposed will lead consumers to ignore alerts that are important to them, while imposing onerous requirements on ISPs.

B. The NPRM Notice Timelines Will Result in Less Effective Breach Responses, Customer Confusion, and Unnecessary Costs.

As an initial matter, the NPRM risks confusion through the proposed rule that companies provide notice to the Commission within seven days of "discovery." The NPRM does not clearly define "discovery." This omission invites confusion and will make it difficult for entities to comply with the rule as proposed. Furthermore, at the very least, any rule should reflect that there may be instances when a customer or third party "discovers" a breach and notifies an ISP; the trigger in such instances should be when *the ISP* discovers the breach—not when it is first discovered.

Additionally, the timelines for breach notification set forth in the NPRM are unrealistic.[587] It is generally difficult to know the scope of a breach, the affected parties, and

[586] As discussed below, ECPA, which imposes civil and criminal penalties for "unauthorized access" to computer systems, requires intent to engage in the prohibited activity.

[587] The Commission proposes the following timelines: (1) notification to the Commission of any breach of customer proprietary information no later than 7 days after discovery; and (2) notification to affected customers of breaches of

nature or potential risk of harm, within 7 to10 days. This timeline ignores the necessary steps that a company must undertake following discovery of a breach. The initial period after discovering the possibility of a breach is critical to stopping the harm (shutting down accounts, fixing systems, etc.). The company must then investigate what happened: it must mount a forensic (or other) investigation to determine whether a breach (exposure of personal data) has occurred or not, whether the attack is still underway, and what data was impacted; patch the vulnerabilities that led to the breach; make a determination as to whether the affected individuals are at risk for identity theft or fraud ; validate the identity of all individuals whose data were exposed (which may be especially difficult if the data breached did not directly identify specific consumers, but may be considered by the Commission to be "linkable" to identifiable individuals); confirm all contact information for affected individuals; ensure that all customer care employees are prepared to accurately answer questions received by customers after they receive notice; have remedies in place to offer consumers; and draft notices to comply with the Commission's rules—as well as comply with up to 47 different state law requirements.[588]

Only after those steps are complete should an ISP, or an entity, notify customers. CTIA's members will endeavor, in the event of a breach, to provide such notifications quickly, but this may not always be feasible within an arbitrarily defined, short window. Moreover, customers

---

customer proprietary information no later than 10 days after the discovery of the breach (subject to law enforcement needs, which may include notification to the FBI and U.S. Secret Service within 7 days of the discovery of the breach). *See NPRM*, 31 FCC Rcd at 2575 ¶ 234.

[588] *See, e.g.*, U.S. Dep't of Justice, Cybersecurity Unit (Computer Crime & Intellectual Property Section, Criminal Division), *Best Practices for Victim Response and Reporting of Cyber Incidents* (April 2015), https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf (providing "best practices" for preparing a cyber incident response plan and in preparing to respond to cyber incidents); Paul Cichonski et al., U.S. Dep't of Commerce, NIST, *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology* (Aug 2012), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (providing guidelines for establishing incident response capabilities for federal agencies).

are often made aware of breaches before receiving formal notice, either because they brought the breach to the company's attention or because the company has had to shut down access to accounts. All of the above must occur as a company continues to investigate the breach and learn new facts.

The Commission's proposal will lead to not just over-notification, which is problematic itself, but also notices that include inaccurate information. If an ISP is required to provide early notice, before it has fully investigated a breach and is aware of all the relevant facts, it is more likely to send an incomplete or not wholly accurate notice, which in turn, would necessitate confusing supplemental notices. The NPRM also creates a perverse incentive for ISPs to focus their energy on consumer notice and reporting, rather than patching existing (and in some cases, exposed) vulnerabilities to prevent a breach of additional data. At a minimum, the notification period should be triggered only after discovery or notification has occurred, an initial investigation is complete, and the identities of affected customers are known.

A number of real-world scenarios illustrate why the NPRM's short notice period is a problem. For instance, the breach of federal employee information at the Office of Personnel Management ("OPM"), which made the headlines, showed how difficult it can be to determine the nature and scope of a breach. OPM initially identified a breach in early 2015 and then identified another breach in June 2015. For this second breach, OPM did not even start to notify affected individuals until September 30 and then continued for approximately three months.[589] If the Commission insists upon a short notification timeframe, then an affected ISP that is unable to confirm precisely who was impacted due to a shortened forensic investigation may alert its entire

[589] *See Cybersecurity Resource Center: Cybersecurity Incidents, "What Happened,"* Office of Personnel Management, https://www.opm.gov/cybersecurity/cybersecurity-incidents/; Beth Colbert, *Notifying Those Impacted by the Recent Cyber Intrusion*, Office of Personnel Management, Director's Blog (Oct. 1, 2015), https://www.opm.gov/blogs/Director/2015/10/1/Notifying-Those-Impacted-by-the-Recent-Cyber-Intrusion/.

customer base "just to be safe," causing many consumers to be alarmed unnecessarily. Such an approach might be necessary from an administrative and compliance perspective, but it could have negative consequences for subscribers, who, for example, cancel credit cards or cancel service when it is not necessary to do so. Another potential harm from a short notification timeframe may occur if a company reports a data breach while a cyberattack is still underway. The attacker may then be able to shift tactics and erase some of its tracks, leading to further data leakage and incomplete awareness for the firm, the public, and law enforcement about how the breach was carried out and what data may have been taken.

C. The NPRM Rules Jeopardize Consumers by Not Containing Any Agreement by the Commission to Keep Breaches Confidential Prior to Customer Notification.

The NPRM does not offer any commitment by the Commission to keep the existence of a data breach confidential during the three days allowed between notice to the Commission and notice to customers. In theory, the Commission could independently notify the public that an ISP had filed a data breach notice, before the ISP could communicate directly to its customers, or could choose to post all ISP breach notifications on a public website, which could allow enterprising bloggers or reporters to break the news. This would lead to further harm to ISPs and customers, given that the facts will necessarily be undeveloped in that short timeframe, and consumers will then be still more likely to receive evolving information rather than clear instructions. Accordingly, the Commission should clarify that any breach notifications submitted to it or to the FBI will be held in confidence until customer notice has begun.

D. The NPRM Rules Conflict with State Laws and Other Federal Laws, Rendering Compliance by ISPs Virtually Impossible.

The Commission has failed to explain why, given extensive regulation in this area, its involvement is necessary. As the Commission itself recognizes, 47 states, as well as the District

of Columbia, Guam, Puerto Rico, and the Virgin Islands, have all adopted data breach notification laws, and those laws apply to the rest of the Internet ecosystem, including numerous entities that hold the same data as, or more data than, ISPs.[590] The Proposed Rules would conflict with many of the intent and harm requirements in these laws and certainly complicates compliance by adding another set of requirements to follow.

The NPRM may conflict with state law requirements, to the extent it requires notice within seven days of "discovery" of a breach without allowing time for an investigation and risk of harm analysis. While many state laws simply provide that notice is not required if a risk of harm is not present, some states (and HIPAA) require a risk of harm analysis.[591] The NPRM does not analyze these state statutes and explain why they are insufficient or how an overlapping, conflicting federal regime otherwise would be in the public interest.

Moreover, the Commission should be clear about the extent to which it would preempt state law requirements. The NPRM is largely silent on this question, other than to say that state laws are preempted where necessary, such as to enforce the seven business day waiting period after notice to federal law enforcement.[592] With the expansion of notice requirements to cover breaches of "customer proprietary information," the potential for conflict with state notice requirements increases. For instance, if state law enforcement requests a delay in notice to the public due to an ongoing investigation, would the Commission's ten-day rule for notice to

---

[590] *NPRM*, 31 FCC Rcd at 2574-75 ¶¶ 233–235; *see also* National Conference of State Legislatures, *Security Breach Notification Laws* (Jan. 4, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (citing breach laws of 47 states and 4 territories).

[591] *See, e.g.*, Kan. Stat. 50-7a02(a) ("A person that conducts business in this state, or a government, governmental subdivision or agency that owns or licenses computerized data that includes personal information shall, when it becomes aware of any breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused.").

[592] 47 C.F.R. § 64.2011(b)(1).

customers trump that request? Neither ISPs nor state law enforcement would be well served by seeking a declaratory ruling from the Commission on this question, following a breach. To the extent that Section 222(a) is construed as a font of authority for *some* data breach notification rules, which it cannot be,[593] there is still nothing in the statute or the legislative history that suggests that Congress intended to preempt state regulation of the varieties of information that might be handled by a wide set of commercial entities, in addition to telecommunications carriers. This is in contrast to cases where express preemption of inconsistent state laws is provided in the Act, such as Section 251(d)(3).[594]

The proposed data breach notification rules also are unreasonable to the extent that they conflict with the provisions in the Electronic Communications Privacy Act (ECPA) that govern unauthorized access to data through "computer trespassing," nor is CTIA aware of any indication from media reporting or advocacy groups of a need to impose a higher "computer trespassing" requirement on ISPs. Specifically, while ECPA prohibits the unauthorized access to data, or exceeding authorized access to data, it includes an intent requirement.[595] ECPA also exempts from the definition of a "computer trespasser" any "person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer."[596]

---

[593] *See supra* note 55.

[594] 47 U.S.C. § 251(d)(3) ("In prescribing and enforcing regulations to implement the requirements of this section, the Commission shall not preclude the enforcement of any regulation, order, or policy of a State commission that[] . . . is consistent with the requirements of this section; and does not substantially prevent the implementation of the requirements of this section and the purposes of this part.").

[595] *See* 18 U.S.C. §§ 2511, 2512.

[596] *Id.* § 2510(21)(B).

E. The Commission Should Not Require ISPs to Provide Notification in the Event of a Third-Party Breach.

The Commission should not require ISPs to notify customers of a third-party breach. This mandate also would result in over-notification, particularly because third parties have their own obligations to report, which, if the Proposed Rules are adopted, may differ from the requirements imposed on ISPs, depending on where the breach occurred. Providers should retain the flexibility to work together with third parties when appropriate to provide notice. Indeed, as discussed previously, NIST has determined that collaboration between various private entities (including ISPs) and law enforcement in the event of a breach can be instrumental to limiting harm; Commission rules that interfere with, or prevent, such collaboration are not in the public interest.

CONCLUSION

CTIA reiterates that its members are committed to protecting the online privacy of their customers. Under the FTC's proposed privacy regime, myriad state and federal laws, and self-regulatory codes of conduct, mobile ISPs have developed transparent, customer-friendly policies and practices to ensure that customers are aware of how their information is both being used and kept secure.

Likewise, CTIA recognizes that the Commission may have a role to play in the protection of customer privacy, and has urged the Commission to adhere to the FTC privacy standards that have governed ISPs for years and, in developing rules, to follow the example set by the FTC. Specifically, following a two-year collaborative process featuring workshops, meetings, and meaningful industry participation, the FTC adopted a flexible online privacy regime that was carefully calibrated to reflect not only customer expectations, but also providers' needs for flexibility. The FTC correctly identified that heightened privacy protections, in the form of

enhanced customer choice, should be available only in certain specific circumstances that present additional privacy risks—for example, a company's deliberate use of sensitive customer information. Otherwise, however, the FTC concluded that routine uses of customer information, whether for first-party marketing or other legitimate business uses—many of which benefit not just carriers, but also other providers and customers—occur within the context of the relationship with the customer, and generally can proceed on the basis of implied consent, or, at most, opt-out consent. In these respects, the FTC's approach is largely consistent with other touchstone privacy regimes, including those proposed by the White House and adopted by the European Union.

At the outset of this rulemaking process, CTIA and other industry associations recommended that the Commission adopt a similar model for the regulation of ISPs, and, if necessary, provide backstop enforcement against ISPs that do not honor the principles of transparency, notice and choice, and data security. Such an approach also would be consistent with the recommendations of many policy experts that, given rapidly changing business arrangements and models, products and services, and emerging threats, privacy regulation should be flexible and technology neutral. Moreover, that approach is exactly what consumers *expect*: that their data will receive uniform protection under a coherent regulatory regime that applies across platforms, as data flows in and through the open Internet ecosystem. It also allows them to tell companies what they *prefer*, as they will have the opportunity to make simple privacy decisions that are consistent with the context of the transaction and their relationship to their ISP.

The NPRM suggests, however, that the Commission is preparing to head off on its own course. Instead of providing flexibility, the Commission appears ready to impose prescriptive requirements regarding how, when, and on what basis ISPs may use customer information for

even the most routine business operations—as well as how ISPs must communicate with their customers. Rather than promote technology- and platform-neutrality, the Commission appears poised to adopt an asymmetric privacy regime that subjects ISPs to an entirely different set of requirements than edge providers like search engines, ad networks, and social media platforms that have, use, and disclose the same information as (if not more information than) ISPs. And rather than honoring customer expectations, the Commission appears committed to relying on antiquated distinctions between "communications" and "non-communications-related" products and services—distinctions which have nothing to do with privacy, and which no longer make sense in today's open, competitive, and converging Internet ecosystem.

If the Commission proceeds on this course, the technology-specific nature of the Proposed Rules will do nothing to actually enhance privacy protections for consumer data, since the vast majority of broadband companies, such as edge providers, will have access to the very same (or more) data but will be exempt from the rules. While thus failing to advance consumer privacy beyond what the FTC regime already compels, the Proposed Rules will produce substantial public interest harms in other respects. First, the Proposed Rules will harm ISPs by imposing administrative costs and burdens, while simultaneously depriving ISPs of new sources of revenue. These effects will frustrate the Commission's objective of achieving further deployment of advanced broadband infrastructure, both because costs may be passed on to consumers (depressing demand), and because ISPs will have fewer resources to devote to capital-intensive investments like network expansion (inhibiting supply). The Proposed Rules also will harm competition. Unlike ILECs in the 1996 traditional voice marketplace, ISPs *are the disruptive entrants* and potential competitors to the ten firms that currently comprise a dominant 70% share of the online advertising market. What's more, the Proposed Rules will

jeopardize, rather than enhance, data security. ISPs must have flexibility to respond to emerging cybersecurity threats, and there is widespread consensus that robust information sharing is a critical aspect of any cybersecurity response.

Given these likely effects, it is not surprising that the Proposed Rules also are contrary to law. Indeed, as a threshold matter, the Proposed Rules are contrary to the Communications Act as a whole and Section 222 more specifically, because they regulate ISPs' provision of broadband service. Even if that is not the case, however, the Rules also unambiguously exceed clear limitations in Section 222—by creating a new category of protected information, by encompassing de-identified data, by defining CPNI more broadly than the statute will bear, potentially by restricting ISPs' use of information even with customer approval, potentially by restricting ISPs' use of information obtained other than by virtue of providing service, and potentially by restricting ISPs' use of arbitration. Nor can the Commission look to other, more general provisions of the Communications Act to prohibit practices that Section 222, the most relevant provision of the Act, unambiguously preserves.

Finally, even if the Proposed Rules did not suffer from these policy and legal shortcomings, they nonetheless cannot stand, because they impose quintessential speaker-based and content-based burdens on valuable speech—including first-party marketing, delivery of third-party advertising, and the exchange of information generated in the course of business. Any such burdens are presumptively invalid under the First Amendment. Moreover, on an as-applied basis, the Proposed Rules fail at virtually every step of the *Central Hudson* analysis. These significant constitutional infirmities also deprive the Commission of the deference that would normally attach to rules promulgated under the Communications Act, and would require a reviewing court to adopt a more reasonable interpretation of Section 222.

CTIA appreciates the Commission's commitment to consumer privacy and the Commission's sense of urgency. But the problems in the NPRM would be fatal on appeal, and protracted uncertainty and litigation are not in the public interest. Additionally, there is simply no need for the Commission to try to do in two months what it took the FTC two years to accomplish; to the contrary, CTIA respectfully submits that there will be nothing in the record demonstrating a unique need to adopt ISP-specific restrictions, when the FTC declined to do so four years ago. Instead, the Commission should recognize the deficiencies in the NPRM and begin working toward a consensus path forward. CTIA is ready to work with the Commission, other associations, individual providers, advocacy groups, and consumers alike in charting this path based on principles of transparency, customer choice, and data security.

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

May 26, 2016

APPENDIX A

March 1, 2016

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

Dear Chairman Wheeler,

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

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

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

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

Respectfully submitted,

Matthew M. Polka
President & CEO
American Cable Association

Steven K. Berry
President & CEO
Competitive Carriers Association

Meredith Attwell Baker
President & CEO
CTIA

Michael Powell
President & CEO
National Cable & Telecommunications Association

Walter B. McCormick, Jr.
President & CEO
USTelecom

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

Privacy Framework

Discussion Paper

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

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

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

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

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

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

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

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

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

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

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

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

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

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