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

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

REPLY COMMENTS OF CHARTER COMMUNICATIONS, INC.

July 6, 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
	)	
	)	

REPLY COMMENTS OF CHARTER COMMUNICATIONS, INC.

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

INTRODUCTION AND EXECUTIVE SUMMARY

Charter Communications, Inc. ("Charter") is committed to protecting the privacy and security of its customers' data. Charter values and relies on the trust and loyalty of its customers, and it recognizes that strong, proactive data privacy and security practices are critical to maintaining its customer relationships. As one commenter explained, unlike other entities in the Internet ecosystem, Internet service providers ("ISPs") have ongoing relationships with their customers and therefore have particular incentive to protect the privacy of their customers' information.[2] Indeed, Charter has invested heavily to protect its customers' privacy and security through its implementation of numerous controls and processes to protect customer data. In addition to these upfront investments, Charter conducts regular audits to ensure compliance with these processes; voluntarily monitors its networks for signs of unauthorized access to, or misuse

---

[1] *In re Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, 31 FCC Rcd 2500 (2016) ("*NPRM*").

[2] *See* Comments of Howard Beales (May 27, 2016) ("*Beales Comments*"), at 6 ("[E]dge providers, ad networks and other online entities . . . have only ephemeral relationships with consumers, [whereas][ISPs] have ongoing business relationships with their subscribers and therefore must safeguard their privacy in order to retain their trust and their business. The fact that firms with high levels of repeat purchasers are relatively unlikely to engage in opportunistic behavior towards consumers is widely agreed upon in the consumer protection literature.").

of customer information; and alerts customers when it detects malicious activity that may have compromised their information.

Charter has found that the current privacy regime works well and is prepared to operate under reasonable privacy rules. The Commission has taken on an exceedingly complex topic, however, and the stakes for consumers, ISPs, and the Internet ecosystem are high. Thus, although Charter applauds the Commission's attention to data privacy and security, given the complexity of the issues, Charter urges the Commission to take the time necessary to regulate in a manner that avoids unintended consequences.

The Commission posed over 500 questions in the NPRM, many of which delve into specific business practices and technical operations. In the short time since the NPRM was issued, Charter has already identified numerous areas in which the proposed rules would negatively impact both the customer experience and Charter's legitimate business activities. Moreover, the Commission received over 50,000 initial comments to its proposal. The Commission should not issue rules without carefully considering these comments and evaluating the impact that the proposed rules will have on consumers and ISPs.

Although Charter supports continued and proactive efforts to strengthen data privacy and security protections, Charter opposes the Commission's proposed rules for several reasons. *First*, as many commenters noted, the Commission lacks the authority to impose the rules under the Communications Act; adopting the rules would be arbitrary and capricious in violation of the Administrative Procedure Act ("APA"); and the proposed rules violate the First Amendment by imposing a prior restraint on constitutionally protected commercial speech. *Second*, the proposed rules would harm consumers by denying them access to information about new products and services and contravening their expectations and preferences for a uniform online

regulatory regime; stifling innovation and competition; and undermining consumers' ability to respond appropriately to information about data breaches. *Third*, the Commission's proposed rules would impede ISPs' ability to operate their networks, provide reliable customer service, and respond adequately to security threats and other unlawful activity, all without advancing the Commission's stated goal—protecting consumers' privacy interests. For all of these reasons, as discussed below, Charter respectfully requests that the Commission study these issues further and refrain from acting until it is prepared to issue rules that are lawful and appropriately tailored.

I. The Commission Is Legally Constrained From Adopting the Proposed Rules.

Commenters explained several reasons why the Commission is legally constrained from adopting the proposed rules. For instance, as numerous commenters argued, the text and legislative history of Section 222—the statute that the Commission relies on as a basis for its rulemaking—show that Congress designed the statute to govern only *voice* services, and it therefore cannot be extended to regulate customer information in the broadband context.[3] Moreover, as commenters also noted, even if the Commission could overcome this obstacle, it

[3] *See* Comments of CTIA (May 26, 2016) ("*CTIA Comments*"), at 16 (noting that "[b]oth the plain language of Section 222 and the legislative history make clear that [the] Congress drafted this section to protect certain information that carriers obtain solely by providing *voice* services to customers in a concentrated, closed market," and highlighting the "numerous references throughout the provision to '*call[s]*,' '*call* location information,' '*local exchange* carrier[s],' 'IP-enabled *voice* service[s],' '*telephone* exchange service[s],' '*telephone toll* service,' [and] '*telemarketing*,'" (first and second brackets added)); Comments of the National Cable & Telecommunications Association (May 27, 2016) ("*NCTA Comments*"), at 7-13 (stating that "Section 222 was written only with voice telephone service in mind, and the 'telephone-centric' nature of the Commission's current rules reflects nothing more than the limits of the statute itself," and noting that "[i]n its initial rulemakings implementing Section 222, the Commission clearly understood the services encompassed by the statute to be solely voice communications" and "likewise recognized that key statutory terms were infused with telephony concepts") (citing *In re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers Use of Customer Proprietary Network Information and Other Customer Information*, Notice of Proposed Rulemaking, 11 FCC Rcd 12,513, 12,524 ¶ 22 (1996); *In re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information and Other Customer Information*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8064-65, 8081-82 ¶¶ 2, 27 (1998) ("*1998 CPNI Order*"), vacated, in part, by *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999)).

still could not (1) expand the scope of customer information that Section 222 covers beyond customer proprietary network information ("CPNI"),[4] or (2) impose restrictions on the use and disclosure of de-identified information.[5] Commenters further explained that the other provisions of the Communications Act that the NPRM cites as possible sources of authority—Sections 201, 202, 705, and 706—provide no basis for the Commission's proposed rules.[6] In addition, as

[4] *CTIA Comments* at 25-35 (observing that Section 222(a) "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;" "Section 222(c) explains how this general prohibition operates with respect to customers;" and explaining that the statute defines CPNI "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"); *NCTA Comments* at 14-18 (discussing limited statutory authority with respect to customer information under Section 222); *Comcast Comments* at 71-75; Comments of AT&T (May 27, 2016) ("*AT&T Comments*") at 103-07; Comments of CenturyLink, Inc. (May 27, 2016) ("*CenturyLink Comments*"), at 13-15; Comments of Verizon (May 27, 2016) ("*Verizon Comments*"), at 53-60 (asserting that the text, structure, and legislative history of Section 222, as well as the way Congress phrased other privacy statutes, prohibits the Commission from extending Section 222 beyond CPNI).

[5] *CTIA Comments* at 35-37 (explaining that Section 222(c)(1) unambiguously excludes de-identified data from the provisions governing CPNI); Comments of Comcast (May 27, 2016) ("*Comcast Comments*") at 84-87 (same). In any event, as commenters noted, even if the Commission could lawfully expand the definition of information covered under Section 222 to include de-identified data, such a reading of the statute would undermine business practices that benefit consumers. *See, e.g., CTIA Comments* at 41 (noting that the Commission's proposed rules do not reflect how ISPs may regularly handle information that is "linkable" to individuals but is maintained in "non-linkable" format (*i.e.*, hashed or coded). For example, an ISP might use such information to authenticate customers by verifying that the IP address or MAC address to which service is being delivered is, in fact, associated with a customer. This information alone does not identify an individual customer, and therefore does not implicate any privacy interests. Yet such information, if theoretically linkable to an individual, would fall under the Commission's proposed rules and would be subject to the notice, choice, and data security requirements that they impose. As explained above and more fully below, the Commission's proposal would severely impede ISPs' ability to conduct internal operations and improve the products and services that customers want and expect to be offered. *See also* Comments of Future of Privacy Forum (May 27, 2016) ("*Future of Privacy Forum Comments*") at 2 (urging the Commission to "recognize that *non-aggregate* data can be de-identified in a manner that makes it not reasonably linkable to a specific individual" and to adopt rules that define "de-identified data" in line with the FTC and National Institute for Standards and Technology standards (emphasis in original)); Comments of State Privacy and Security Coalition (May 27, 2016) at 11-12 (urging the Commission to revise its definition of de-identified data to match the FTC's definition).

[6] Commenters made clear that neither Section 201 nor Section 202 provided authority for the Commission's proposed rules. *See CTIA Comments* at 60-62; *NCTA Comments* at 25 ("Because Congress enacted a comprehensive privacy regime under Section 222, Section 201(b) cannot serve as an independent source of authority for the Commission to impose privacy protections on ISPs subject to Title II."); *Comcast Comments* at 68-70 (stating that "Section 222 represents the *maximum* privacy authority the Commission has under the Act" to the exclusion of other provisions, including Section 201(b)); *AT&T Comments* at 109-10; *Verizon Comments* at 48-50, 60-61. Commenters also explained that the Commission could not rely on either Section 705 or Section 706 to adopt the proposed rules. *See NCTA Comments* at 26 and cases cited therein. NCTA explained that Section 705 is coterminous with the Wiretap Act, and because the Wiretap Act does not prohibit (1) the interception or disclosure of non-content information associated with communications, (2) the interception and disclosure of the contents of

several commenters asserted, adopting the proposed rules would both be arbitrary and capricious[7] and violate the First Amendment.[8]

II. The Proposed Rules Would Harm Consumers.

Separate from the legal deficiencies, the proposed rules impose restrictions that impede the use of customer information to support legitimate business activities and that are inconsistent with current consumer expectations.[9] The proposed rules also will impede the development and marketing of new services. As a result, consumers will have less access to new service offerings and low-cost products and services, and they will be inundated with advertising that is less relevant and thereby more annoying. Moreover, the proposed breach notification rules would undermine consumers' and ISPs' ability to respond effectively in the event a breach occurs.

---

communications with implied consent of one of the parties to the communications, or (3) activities in which ISPs engage in the ordinary course of business, it would not reach the use and disclosure of CPNI (or "customer proprietary information"). *See also CTIA Comments* at 64 (noting that Section 705 applies to "any person," which would include edge providers and others in the online ecosystem that collect, use, and disclose consumers' online information, and that "[t]he 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"); *Comcast Comments* at 70-71; *AT&T Comments* at 110-12; *Verizon Comments* at 62.

[7] *Verizon Comments* at 29 ("By singling out broadband providers among similarly situated entities for special, burdensome privacy regulation, based on the mistaken view that they have unique and comprehensive access to their users' data, the Commission's proposed rules are arbitrary and capricious."); *AT&T Comments* at 88-90 (same).

[8] *See CTIA Comments* at 77 (explaining that "[t]he 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."); Comments of Laurence H. Tribe and Jonathan S. Massey (May 27, 2016) at 14 ("The FCC's proposed rules here would not survive any form of First Amendment scrutiny—whether the intermediate standard of *Central Hudson* or the strict scrutiny applied in *Sorrell*."); *see also NCTA Comments* at 33 (noting constitutional infirmities of speaker-based discriminatory treatment between ISPs and other entities online); *AT&T Comments* at 92 (noting opt-in consent requirements would violate strict and intermediate scrutiny); *Verizon Comments* at 30-31.

[9] As commenters noted, in addition to the legal flaws with the Commission's proposed rules, there are both legal and policy reasons that prevent the Commission from pursuing the NPRM's proposal to harmonize the proposed rules with Section 631 of the Communications Act, codified at 47 U.S.C. §551. *See NCTA Comments* at 35-38 (noting that, as a legal matter, Section 631 "occupies the field" with respect to the privacy obligations of cable providers when they provide cable services, and that "Section 621(c) of the Cable Act[] bars the Commission from imposing common carrier regulations on any cable service offered by a cable operator"); *Comcast Comments* at 12 (same).

A. The Proposed Rules Would Impede the Use of Customer Information That Supports Legitimate Business Activities.

The proposed rules would impede a number of legitimate business practices by imposing onerous notice and choice requirements. In this respect, the Commission's proposed regime departs from the well-established and successful approach taken by the FTC in its 2012 report on consumer privacy ("FTC Privacy Report")[10] (and in enforcement actions), and endorsed by the White House in the 2012 White House Privacy Report.[11]

Both the FTC and the White House privacy frameworks ensure strong consumer privacy protection through the core notice and choice principles that undergird all privacy regimes.[12] These frameworks also allow companies sufficient flexibility to innovate and adapt to ever-changing technology in the digital environment.[13] For instance, both the FTC Privacy Report and the 2012 White House Privacy Report articulate general transparency principles that companies should adopt, but they allow companies discretion to determine the best method of providing privacy notices to consumers, as well as what information those notices should

---

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

[11] *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 Report"), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[12] *Id.* at 7, 9 (noting that the proposed "consumer privacy bill of rights" reflects the "globally recognized Fair Information Practice Principles (FIPPs)" that "have become the globally recognized foundations for privacy protection"); FTC Privacy Report at 10 (stating that the FTC's framework is consistent with privacy frameworks around the globe, such as the Asia-Pacific Economic Cooperation Privacy Framework and the Organization for Economic Cooperation and Development privacy framework).

[13] FTC Privacy Report at 9 (explaining that the FTC's "privacy framework is designed to be flexible to permit and encourage innovation"); 2012 White House Privacy Report at 29, 35 (stating that the FTC has "effectively protect[ed] consumer data privacy within a flexible and evolving approach to changing technologies and markets" and asserting that the White House proposal is "flexible" and will "allow companies to implement the Consumer Privacy Bill of Rights in ways that fit the context in which they do business").

include.[14] In addition, both the FTC and the White House adopt strong choice mechanisms, but they allow companies to infer consent to use personal data in ways that are consistent with the context of their relationship to the customer or the context of the transaction. Such permitted uses include most first-party marketing, among other things.[15] Under the FTC framework, companies are urged to provide customers an opt-out mechanism when consent cannot be inferred from context. Importantly, the FTC recommends that companies obtain opt-in consent only under limited circumstances, such as when companies intentionally collect sensitive data—*i.e.*, information about children, health and financial information, Social Security numbers, and precise geolocation information—or when they make material retroactive changes to their privacy policies.

The Commission proposes to take a very different approach to both notice and choice, however. With respect to notice, the Commission proposes requirements that would dictate the content and timing of ISPs' publication of privacy policies.[16] In addition, the Commission seeks comment on a number of other potential requirements related to the placement, content, timing, standardization, and frequency of such notices.[17] The Commission should reconsider these proposed rules and potential additional requirements, as—for the reasons explained below—they

[14] FTC Privacy Report at 62 (stating that "[p]rivacy statements should account for variations in business models across different industry sectors" and that "prescribing a rigid format for use across all sectors is not appropriate"); 2012 White House Privacy Report at 16 (explaining that "[t]he company-to-consumer relationship should guide companies' decisions about which uses of personal data they will make most prominent in privacy notices").

[15] 2012 White House Privacy Report at 17 (stating that "companies may infer consent to use personal data to conduct marketing in the context of most first-party relationships," as well as for other purposes that are consistent with the context of the company-customer relationship and integral to the company's operations); FTC Privacy Report at 38, 40 (explaining that the FTC's standard with respect to choice "should be sufficiently flexible to allow for innovation and new business models," and noting that the FTC "believes that most first-party marketing practices are consistent with the consumer's relationship with the business and thus do not necessitate consumer choice").

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

[17] *Id.* at 2529-31 ¶¶ 84-90.

are unnecessary, overly burdensome, and risk harming consumers and interfering with their enjoyment of broadband services, without appreciably advancing privacy protection.

As many commenters noted, ISPs currently provide their customers with detailed notices about their privacy practices, including, among other things, a description of what information they collect, how they use it, and with whom they share it.[18] Like all companies, ISPs have determined the best way to provide such notices, given the nature of their business models (including the types of services that they offer) and the interfaces through which they interact with consumers. Flexible rules that allow ISPs to continue to do so would neither undermine consumer privacy nor deprive the Commission of effective recourse in the event that an ISP's notice was deemed insufficient under such rules. Indeed, the FTC's successful track record of enforcement underscores that a flexible model provides a sufficient opportunity for recourse.[19]

The one-size-fits-all notice requirements proposed by the Commission, in contrast, would hamstring ISPs, limiting their ability to adapt to changes in technology and to evolve to respond to changes in consumer demand.[20] Moreover, as several commenters have noted, requiring more frequent notices to customers likely would lead to notice fatigue and create friction in users' online experience, interfering with their enjoyment of broadband services and making them less likely to pay attention to notices warning of the potential for actual harm.[21]

---

[18] *CTIA Comments* at 98 ("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.").

[19] *See* List of FTC Enforcement Actions, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises.

[20] *CTIA Comments* at 102 (urging the Commission not to impose a requirement to provide standardized notices because ISPs need flexibility).

[21] *See, e.g.*, Comments of Consumers' Research (May 27, 2016) ("*Consumers' Research Comments*"), at 24-26 ("Over-notification is not just irritating to consumers; it can also harm them by degrading consumers' experience with the BIAS provider, making them less likely to pay attention to notices that warn of actual harm"); Comments of Consumer Technology Association (May 27, 2016) ("*CTA Comments*"), at 11 (increasing notices to consumers "will

The Commission's proposed choice regime is even more problematic. Not only is such an approach unconstitutional,[22] but it also is out of step with consumer expectations and other well-established privacy frameworks, which regulate data based on their sensitivity and not the type of product or service that the company using the data is marketing.[23] The 2012 White House Privacy Report, for instance, cites personal health information and financial data as examples of sensitive information that may require extra protection.[24] Similarly, the FTC Privacy Report notes that greater harms can be associated with the revelation of sensitive information, such as health information and precise geolocation information, as compared to less sensitive information, such as purchase history or employment history.[25] The FTC further elaborates that the distinction between the *types* of data—*i.e.*, sensitive vs. non-sensitive data—becomes increasingly important when engaging in marketing activities, because using sensitive information to market to individuals carries additional risks of embarrassment, discrimination, and other potentially harmful conduct.[26]

In addition, the FTC recommends different choice mechanisms depending on the sensitivity of the data or whether the data will be shared, and in its comments, it urges the

---

leave them desensitized, tuned out, and unable to differentiate between consent requests that involve fairly innocuous data versus those that ask to use highly sensitive data").

[22] *See supra* at 5.

[23] Comments of Jon Leibowitz (May 23, 2016) at 8 ("[T]he proposed rules would impose a broad opt-in requirement upon broadband providers for the use of a wide swath of consumer data for an extensive range of practices-*including practices for which the FTC requires no choice at all because implied consent is presumed*" (emphasis in original)).

[24] 2012 White House Privacy Report at 11.

[25] *See* FTC Privacy Report at 8 ("[H]arms may include the unexpected revelation of previously private information, including both sensitive information (e.g., health information, precise geolocation information) and less sensitive information (e.g., purchase history, employment history) to unauthorized third parties.").

[26] FTC Privacy Report at 47; Comments of Consumer Protection Bureau Staff of the Federal Trade Commission (May 27, 2016) ("*FTC Comments*"), at 22-23 (recommending that the Commission "consider the FTC's longstanding approach, which calls for the level of choice to be tied to the sensitivity of data and the highly personalized nature of consumers' communications in determining the best way to protect consumers").

Commission to follow this approach.[27] The FTC has recognized that "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," and has therefore concluded that these practices generally do not require choice.[28] Even when companies use sensitive data for first-party marketing, the FTC Privacy Report limited the circumstances under which opt-in consent is required, stating that although affirmative consent should be obtained "where a company's business model is *designed to target* [advertising or other activities to] consumers based on sensitive data," not *all* uses of sensitive data necessitate opt-in choice. The FTC reasoned that "the risks to consumers may not justify the potential burdens on general audience businesses that *incidentally collect* and use sensitive information."[29] Thus, the FTC explained that "online retailers and services such as Amazon.com and Netflix need not provide choice when making product recommendations based on prior purchases," and then elaborated on what such a risk evaluation might look like: "[I]f Amazon.com were to recommend a book related to health or financial issues based on a prior purchase on the site, it need not provide choice. However, if a health website is designed to target people with particular medical conditions, that site should seek affirmative express consent when marketing to consumers."[30]

The 2012 White House Privacy Report adopted a similar approach, stating that "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,

[27] *See FTC Comments* at 22-23.
[28] FTC Privacy Report at 15-16, 40-41.
[29] FTC Privacy Report at 47-48 (emphasis in original).
[30] *Id.*

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."[31]

Conversely, although the Commission suggested in the NPRM that it recognized the importance of the distinction between sensitive and non-sensitive data,[32] under the Commission's proposal, ISPs would be able to infer consent to use personal data *only* to provide the underlying service and to market the very same service to which the customer already subscribes.[33] The proposed rules would allow ISPs to use personal data based on opt-out consent to market as-yet-to-be-defined "communications-related services."[34] All other uses, however, would require customers to *opt in* to the use of their data, even when that use is intended to present the customer with marketing opportunities that would benefit the customer.[35] As several commenters—including the FTC—noted, this approach does not accurately reflect either consumer expectations or the concerns that consumers have regarding sensitive data, as opposed to non-sensitive data.[36] Indeed, the Commission does not make any distinction between harmful and non-harmful uses of data, rendering its proposed rules inadequate to provide meaningful privacy protection and inappropriate for the dynamic and evolving Internet ecosystem.

As explained above, the FTC designed its framework to be flexible, allowing companies to engage in non-harmful uses of data while protecting consumers from potentially harmful uses,

---

[31] 2012 White House Privacy Report at 17.

[32] *See NPRM*, at 2509 ¶ ¶ 20-21 (explaining that "[t]he NPRM recognizes that the sensitivity and confidentiality of personal communications is one of the oldest and most established cornerstones of privacy law" and requesting comment on "whether there are particular types of information . . . [that] are so sensitive that they deserve special treatment").

[33] *Id*. at 2540 ¶ 114.

[34] *Id.* at 2543 ¶ 122.

[35] *Id.* at 2544-45 ¶ 127.

[36] *See, e.g., FTC Comments* at 22.

such as those that may cause embarrassment or discrimination. The Commission's proposed rules, by contrast, do not provide adequate flexibility for ISPs to engage in the broad range of non-harmful uses of data that are essential to their business and marketing operations, such as offering new products and services to existing customers and conducting routine business activities (*e.g.*, authenticating customers). In addition, the types of data that ISPs collect and use do not present the risks of harm that the FTC Privacy Report cites as examples, such as the unexpected revelation of health information.[37]

The Commission should adopt the approach taken by the FTC and other privacy regimes.[38] These frameworks are well-established and comport with consumer expectations. Moreover, they provide robust consumer protection, while allowing businesses to provide their customers with frictionless service and offers regarding products and services that may be of interest to them.

B. The Proposed Rules Are Inconsistent with Consumer Expectations and Would Undermine Their Experience and Access to New Products And Services.

Consumers enjoy broadband services that are tailored to them and reflect their tastes and choices in entertainment, retail, and other products and services. Consumer preference for relevant marketing information is clear from industry experience with ad-blocking tools. Despite ready access to tools that block advertisements and other targeted offers, many consumers appreciate the availability of personalized suggestions and the vast majority forgo the opportunity to opt out of personal customization.[39] Indeed, online consumers expect websites to

[37] FTC Privacy Report at 8.

[38] *NCTA Comments* at 42-43.

[39] *See id.* at 39-40 n.131 (citing ClarityRay, *Ad-Blocking, Measured*, at 4 (May 2012), http://www.slideshare.net/arttoseo/clarity-ray-adblockreport; Genesis Media Ad Blocking Survey (Aug. 7, 2015), http://www.genesismedia.com/news/survey-of-over-11500-adults-finds-76-percent-have-neverused-ad-blockers/).

collect information and to use that information to make content more personalized. Having conducted their online activity for years under the FTC's uniform and flexible framework, consumers do not expect to opt in to such usage. Specifically, when presented with a variety of options for bundled services, consumers readily take advantage of this flexibility to choose a service that maximizes their preferences regarding price and content, without regard to whether the service provides them an opportunity to opt in to the use of their data.

Unlike the FTC framework, which allows companies, for the most part, to infer consent to use personal data to provide such tailored marketing and personalized suggestions, the Commission's proposed rules would hamper ISPs' ability to make these offers. They would prohibit the use of personal data on the basis of implied, or even opt-out, consent to market a wide range of service options, preventing customers from getting the information they want and need to make choices in the marketplace. Therefore, far from empowering consumer choice, as they purport to do, the proposed rules would actually curtail the flow of relevant information to consumers and impede their ability to make informed decisions.

In addition to obstructing consumers' access to information, the proposed rules also would reduce ISPs' incentive to innovate. Without the certainty that they could market new products effectively, ISPs would be less likely to invest in new products and services.[40]

Finally, allowing ISPs to easily market new products and bundled service offerings facilitates competition, which, in turn, lowers prices for broadband services. As the Commission

[40] *See Comcast Comments* at 51 ("It would discourage ISPs from investing time and resources in developing new products and services out of a concern that they will not be able to effectively market and monetize them. It would also reduce revenues the ISP receives from discounted bundled offerings, thereby reducing its ability to invest in broadband deployment, upgrades, and innovation, as the FCC previously recognized[.]"); Comments of American Cable Association (May 27, 2016) ("*ACA Comments*"), at 31 ("[The proposed] framework would make it extremely difficult—if not impossible—to effectively market and deploy innovative products to their consumers.").

itself has recognized, "increase[d] competition for bundles of video and broadband . . . will stimulate lower prices, not only for the Applicants' bundles, but also for competitors' bundled products—benefiting consumers and serving the public interest."[41] Without the ability to tailor marketing and effectively communicate with customers about the opportunity to purchase new products and bundled services, customers will lose the opportunity for cost savings that they otherwise would have.

In sum, not only would the proposed rules fail to offer consumers any measurable privacy protection, they actually would harm consumers by undermining their expectations online, denying them choice, discouraging innovation, and reducing competition that would lower prices for consumers.[42]

C. Consumers Do Not Demand a New, Cumbersome Privacy Framework for ISPs That Differs from the FTC Framework.

Consumers expect and enjoy an integrated Internet experience.[43] As discussed above, however, the proposed rules would regulate the data that ISPs use and disclose differently from the way that edge providers are regulated with respect to the same uses of the same data.[44] Applying different privacy regimes to different aspects of consumers' Internet activities will confuse consumers and undermine their expectations and preferences for a seamless and consistent experience across the online ecosystem.[45] As another commenter explained, "[m]ost

---

[41] *Comcast Comments* at 45 (quoting *In re Applications of AT&T Inc. and DIRECTV*, Memorandum Opinion and Order 30 FCC Rcd 9131, 9134 ¶ 4 (2015)).

[42] *Id*. at 44; *CenturyLink Comments* at 26-27.

[43] *NCTA Comments* at 53-54.

[44] *See id.* at 53 ("Data associated with sending an email, requesting a Web page, entering a search request, receiving a marketing offer or an advertisement, or engaging in other common Internet activities will be subject to materially different legal and regulatory regimes during the milliseconds in which such transmissions are initiated, transmitted, processed and responded to—depending upon the identity of the entity handling such data.").

[45] Comments of Progressive Policy Institute (May 26, 2016) at 2 (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 agreed that '*[a]ll companies collecting data online should follow the same consumer privacy rules so*

consumers do not sharply distinguish among the various interdependent actors in the Internet ecosystem, and all but the savviest will assume that the same general privacy rules apply to their mobile operating system (or web browser or coffee-shop WiFi operator) as apply to their mobile ISP."[46] For example, the average consumer would be confused and surprised to learn that, if he or she had taken proactive steps to adjust privacy settings relating to services provided by his or her ISP, such privacy settings or limitations did not extend to a web browser or mobile app. Further complicating this model, ISPs can act beyond their traditional role as a service provider in multiple other capacities where they use consumer information for a wide variety of legitimate and reasonable purposes. Where different privacy rules apply to different aspects the ISPs' operations or different types of uses of information, consumers will find it difficult to understand where their privacy preferences do, and do not, apply. As many commenters noted, the proposed rules also will undermine ISPs' efforts to provide comprehensive and clear privacy notices about their enterprise-wide information collection and use practices, as explaining all of the different applicable privacy regimes and how they operate with respect to different uses of customer information will confound consumers and make it more difficult for them to understand how their privacy is being protected.[47]

---

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"); *NCTA Comments* at 54-55; *see also Comcast Comments* at 42-43 ("Where a set of rules applies to companies in the same ecosystem differently, the government's efforts to regulate one set of companies but not another, are bound to sow confusion, *especially when the same data is at issue*." (emphasis in original)).

[46] *AT&T Comments* at 56-57.

[47] *Id*; *see also CTIA Comments* at 116 & n.364; Comments of Mobile Future (May 27, 2016) at 7 ("Applying new and different rules to one subset of the complex Internet ecosystem while other participants in the ecosystem remain subject to the FTC's existing regime will create customer confusion" which can result in "frustration."); *Consumers' Research Comments* at 10-11 ("The proposed regime is complex and confusing, both on its own and in conjunction with policies that would govern edge providers. As a court said years ago about early CPNI efforts, 'it defies credulity that consumers will understand the complicated regulatory framework sufficiently to effectively implement their preferences." (citation omitted)); *id.* at 14 (explaining that asymmetric regulation "will be difficult for consumers to appreciate" and "may lead consumers to assume that the FCC's restrictions apply to all online activity" leading consumers "to be less vigilant online"); *NCTA Comments* at 54-55 ("Consumers do not expect their

Moreover, the proposed rules would impose requirements to deliver additional notices and obtain frequent consent from consumers, interrupting what is currently a seamless Internet experience and creating new information costs and unnecessary burdens on consumers.[48] This could cause consumers to suffer "warning fatigue," leading them to reflexively consent or withhold consent, regardless of what their true preference might be if they were fully informed.[49]

D. ISPs Do Not Occupy a Unique Position in the Internet Ecosystem.

As many commenters noted, the proposed rules reflect a misperception about how the Internet operates.[50] Specifically, the Commission justifies its restrictions on ISPs' use of customer information based on the premise that ISPs occupy a unique position in the Internet ecosystem that gives them unfettered and incomparable access to information about consumers' online activities.[51] This notion, however, is belied by readily available facts. As Professor Peter Swire recently demonstrated, online services and consumers are increasingly using technologies—such as encryption and Virtual Private Networks—that prevent ISPs from viewing consumers' online activity.[52] In addition, the average Internet user accesses the Internet through multiple devices—and over multiple ISPs' networks—throughout the day. This leaves ISPs with

---

basic privacy protections will vary substantially based on the type of broadband entity they are interacting with at any particular time. . . . [T]he regulatory asymmetry created by the Commission's regime is likely to make privacy notices more complex and confusing."); *Consumer Technology Association Comments* at 3-4 ("[D]espite the fact that frameworks in place today are currently working to protect consumers, the Commission proposes to muddy the regulatory waters with onerous and prescriptive rules. This proposed approach will inhibit the ability of [ISPs] to innovate and will confuse consumers, all with little to no benefit to consumers. (footnote omitted)); *cf.* Comments of Level 3 Communications (May 27, 2016) at 8 (explaining that differentiated restrictions for uses for broadband and voice services could result in customer confusion).

[48] *NCTA Comments* at 54-55; *Comcast Comments* at 42-43.

[49] *Comcast Comments* at 44; *ACA Comments* at 21-22.

[50] *AT&T Comments* at 9-12; *CTIA Comments* at 7-8; *NCTA Comments* at 11-12, 40-41;
Comments of Nick Feamster (May 27, 2016) ("*Feamster Comments*"), at 1-3.

[51] *NPRM*, 31 FCC Rcd at 2501-02, 2584-85 ¶¶ 2, 265.

[52] 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.

a fragmented and incomplete view of consumers' online activity. By contrast, the shift to mobile broadband service and multiple devices has *not* impeded edge providers' access to information about consumers' online behavior.[53] Indeed, search engines, browsers, operating systems, social media platforms, and other online entities have access to far more—and a wider variety of—information about consumers' online activity than ISPs do.[54]

Even consumer groups filed comments urging the Commission to recognize the threat that edge providers—as opposed to ISPs—pose to consumer privacy. For instance, the Electronic Privacy Information Center criticized the Commission for its "narrow focus in this rulemaking on ISPs" because in doing so, it "misses a significant portion of invasive tracking practices that threaten the privacy of consumers' online communications."[55] In addition, Consumer Watchdog cited the Pew study on which the Commission relied as justification for its proposed rules as evidence that consumers who have concerns about their online privacy are in fact focused on "the entire Internet ecosystem," not just ISPs.[56] But the Commission's proposed rules would do nothing to address the privacy interests that edge providers implicate. Instead, these edge providers would continue to collect, use, and share information about both consumers' online *and* offline activities to market new products and services just as they always have done.[57]

[53] *Id.* at 3.

[54] *Id.* at 8; *AT&T Comments* at 12-30 (describing how consumers' information is collected, used, and shared online by edge providers).

[55] Comments of Electronic Information Privacy Center (May 27, 2016) at 4, 15-16.

[56] Comments of Consumer Watchdog (May 27, 2016) at 3.

[57] *Future of Privacy Forum Comments* at 11; *CTIA Comments* at 136.

E. The Proposed Rules Would Reduce Competition In the Online Advertising Market, Leaving Consumers with Fewer Options and Higher Prices.

Unsurprisingly, edge providers currently dominate the market for online advertising. Google, for example, controls 65% of the market for online search, from which it derives tremendous data for targeted advertising.[58] And Facebook, which also depends on online behavioral advertising for its revenue, dominates the market for social networking, with almost 44% market share.[59] These companies offer consumers a take-it-or-leave-it option: consumers may use their services in exchange for receiving ads based on their online (and, in some cases, offline) activity, or they may use another search engine or social network. Many consumers choose to use them, giving Google and Facebook digital display ad revenues in 2014 that accounted for about one-fifth and just below one-quarter, respectively, of the U.S. online advertising market.[60] Google and Facebook are not the only large players in the online advertising market, however. Indeed, the top ten online ad-selling companies, none of which is an ISP, together earn over 70% of online advertising revenue.[61]

Under the Commission's proposed rules, edge providers will continue to collect, use and share consumer information for online advertising under the FTC's flexible regulatory framework, while ISPs—the new entrants to the online advertising market—will be severely constrained from using precisely the same information to develop new business models based on

[58] *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.

[59] *See* Statista, *Leading Social Media Websites in the United States in May 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/ (last visited June 30, 2016).

[60] eMarketer, *Facebook and Twitter Will Take 33% Share of US Digital Display Market by 2017* (Mar. 26, 2015), http://www.emarketer.com/Article/Facebook-Twitter-Will-Take-33-Share-of-US-Digital-Display-Market-by-2017/1012274 (last visited June 30, 2016).

[61] *Swire Report* at 8; see also sources cited, infra Part V.A.2.

ad-generated revenue.[62] Consumer data is critical to online advertising and the products and services that depend, at least in part, on online advertising revenue and online marketing.[63] This business model has become ubiquitous in the Internet ecosystem and has been—and will continue to be—responsible for the Internet's growth and development.[64] By regulating ISPs' use and disclosure of customer information more strictly than other entities in the online ecosystem, the proposed rules would tilt the playing field in favor of Facebook, Google, and other edge providers, enabling them to continue to dominate the market.[65]

This will harm consumers. As economists and a former FTC Commissioner have explained, the broadband market is a multi-sided market with multiple players.[66] Asymmetric regulation of this market will stifle competition, likely increasing costs for consumers.[67] Specifically, the proposed rules requiring ISPs to obtain opt-in consent before using customer data to market anything other than communications-related services will force consumers who desire information about new, innovative products and services, discounts, and other cost-saving

---

[62] *Comcast Comments* at 53 (citing IAB, Internet Advertising Revenue Report at 11 (Oct. 2015), http://www.iab.com/wp-content/uploads/2015/10/IAB_Internet_Advertising_Revenue_Report_HY_2015.pdf).

[63] *See* Executive Office of the President of the United States, *Big Data: Seizing Opportunities, Preserving Values* (May 2014) at 40, https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf; *Comcast Comments* at 53 ("[C]onsumer information has essentially become the currency of the Twenty-First Century online advertising market."), https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

[64] *AT&T Comments* at 2-3; Comments of Association of National Advertisers (May 27, 2016) at 5-11.

[65] *NCTA Comments* at 57; *ACA Comments* at 21-22; *see also AT&T Comments* at 55 ("ISPs would thus face severe impediments in trying to use their own customer data to market those services, whereas non-ISP providers would remain free to use all existing customer data however they wish to promote their equivalent services.").

[66] White Paper of Joshua D. Wright (May 27, 2016) ("*Wright White Paper*"), at 4 (explaining that ISPs "compete as platforms in a multi-sided market, and their ability to develop and foster revenue streams on one side of the market is inextricably linked to their ability to satisfy consumer demand and offer significant cost savings on the other side"); *Beales Comments* at 10 ("Markets for consumer information, online advertising, and digital content are all part of the larger Internet ecosystem.").

[67] Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud*, 103 Nw. U. L. Rev. 1, 11-12 (2008) (noting that "privacy rules that limit how information can be used and shared across firms will artificially push towards greater consolidation, something that usually works against maintaining robust competition").

opportunities to bear the costs of more privacy-conscious consumers.[68] And limiting ISPs' ability to use data for ad-supported content and services will deny consumers the chance to choose among a broad array of ad-based products and services from *both* ISPs and edge providers, without providing any privacy benefits.[69]

F. The Proposed Breach Notification Standards Would Also Harm Consumers.

The Commission's proposed rules for breach notification would lead to ineffective breach response, create consumer confusion, and impose unnecessary costs. The Commission proposes to define a "breach" as "any instance" of access, use, or disclosure of "customer proprietary information" without—or in excess of—authorization, regardless of the intent. This definition is overly broad, both with respect to the information that it covers and the event that would trigger notification.

First, not all "customer proprietary information," if wrongfully accessed, would pose a risk of harm to consumers. For instance, an ISP employee's unauthorized access to a list of the names and addresses of an ISP's customers—without more—would not pose any risk of identity theft to those customers. For the most part, such information is publicly available, and a rule that required ISPs to notify customers in the event of a breach of such limited information would impose additional costs on ISPs and mislead customers without furthering their privacy interests. The same is true of a breach involving purely technical information, such as IP addresses or the technical configuration related to a customer's broadband service. Thus, the Commission should

[68] *Comcast Comments* at 52-57; Comments of Direct Marketing Association (May 27, 2016) at 17-19; *Verizon Comments* at 34-35.

[69] *Beales Comments* at 11 (stating that the proposed rules would harm consumers by preventing them from receiving information from ISPs about new products and services, and that the "presumed 'extra protection' of an opt-in rule is an illusion"); *Wright White Paper* at 22 (noting that Moody's Investor Service concluded that the proposed rules could prohibit some broadband providers from generating advertising revenues).

apply any data breach notification requirement to a much narrower set of information, which should *not* include IP addresses, MAC addresses, persistent identifiers, and any other information that, standing alone, would pose no risk of harm to consumers if breached.[70]

Second, the Commission should not require ISPs to notify consumers about breaches that may pose absolutely no risk of harm to them.[71] For good reason, the majority of U.S. breach notification laws establish a threshold of potential harm that triggers breach notification.[72] The Commission's proposal to forgo such a threshold would lead to over-notification, confusing consumers and causing them to suffer "notice fatigue."[73] Unable to discern breaches that pose risk of harm from those that do not, consumers eventually would disregard such notices and fail to respond when the circumstances actually warranted action.[74] The Commission likely did not intend this result.

---

[70] *FTC Comments* at 32 (recommending the breach notification requirement cover a much narrower set of personal information than the Commission proposes).

[71] *Id.* (recommending the same).

[72] The Gramm-Leach-Bliley Act ("GLBA"), the Health Insurance Portability and Accountability Act ("HIPAA"), as well as 33 of the 47 state breach notification laws incorporate a risk-based assessment prior to requiring notification to individuals when their personal information has been compromised. 12 C.F.R. Pt. 364, Appendix B, Supplement A; 45 C.F.R. § 164.402(2). *Cf.* Md. Code Com. Law § 14-3504(a) (exempting from the definition of a "[b]reach of the security of a system" any "good faith acquisition of personal information by an employee or agent of a business for the purposes of the business, provided that the personal information is not used or subject to further unauthorized disclosure").

[73] *FTC Comments* at 31-32; Comments of INCOMPAS (May 27, 2016) at 10 (the proposal "makes it likely that customers will receive an increased number of breach notifications, leading to customer confusion, notice fatigue, and decreased confidence in their telecommunications service"); *CTA Comments* at 10 (proposed rules will "[a]dd[] another heap to the mountain of notices" consumers already receive); *Verizon Comments* at 69 ("[T]he inevitable result of the Commission's proposal is that customers will receive notifications that they do not care about and that create unnecessary confusion and anxiety, such that customers could stop paying attention to notices altogether and miss those that might actually be important.").

[74] *Comcast Comments* at 61-62; *see also ACA Comments* at 37 ("[A]s consumers learn that the breach notifications more often than not relate to inadvertent breaches with little or no risk of consumer harm, it will become less likely that they will pay attention to any data breach notification (including those with an actual likelihood of consumer harm).").

The NPRM *does* acknowledge the problem of notice fatigue in the breach context, but provides no analysis concerning the effect that the proposed rules would have on consumers.[75] Indeed, although the NPRM asked whether notices regarding account changes or to solicit customer consent would create notice fatigue, it did not address the issue in the context of breach notifications.[76]

In addition, the Commission should expand the time period within which ISPs must notify consumers to 60 days after discovery of the breach. The Commission's proposed 10-day notification window is far too short a period of time within which to complete an investigation and ensure accurate reporting.[77] A reasonable investigation often involves engaging third parties, such as forensic investigators who require time to assess the situation before beginning an investigation. Moreover, it takes more than 10 days from the discovery of a breach to accurately and thoroughly investigate and conduct a risk assessment, especially in the event of network intrusions. Likewise, if there is a need to involve law enforcement, it can take days to communicate with the relevant law enforcement agency and procure dedicated resources, delaying the time when the investigation can begin in earnest.

A 10-day window also would put the Commission's rules drastically out of sync with other U.S. breach notification laws. For instance, HIPAA requires notification to affected individuals within 60 days of discovery.[78] And state breach notification laws typically require notification to individuals in the "most expedient time possible and without unreasonable

[75] *NPRM*, 31 FCC Rcd at 2509 ¶ 23.
[76] *Id.* at 2550, 2567 ¶¶ 141, 202.
[77] *Comcast Comments* at 63-64.
[78] 45 C.F.R. § 164.404(b).

delay."[79] A minority of state breach notification laws have any specific notification timelines at all, and of those that do, the *shortest* timeframe is in Florida, where a party has 30 days to provide notification with a possible extension of an additional 15 days.[80]

Finally, the Commission should ensure that ISPs are not required to notify the customers of their business customers in the event of a breach. An ISP that provides service to a hotel, for instance, should notify the hotel—under a reasonable breach notification standard—in the event of a breach, but the hotel—not the ISP—should be responsible for notifying any hotel customers affected by the breach.

The National Retail Federation ("NRF") urges the Commission to take a different approach. Specifically, it proposes a requirement that ISPs notify not only their own business customers, but also all of their business customers' customers, in the event of a breach.[81] Such a requirement is untenable. ISPs likely would never know which business customers' customers, if any, may have been affected by the underlying breach. And in any event, the business customer—not the ISP—has the information necessary and is in the best position to notify its own customers.

NRF's alternative suggestion that ISPs be required to notify the public in the event of a breach involving business customers is also problematic.[82] As stated above, ISPs would not know which of the business customers' customers—or even whether such customers—had been affected by the breach. Notifying the public would cause consumers, who, according to the FTC,

[79] *See, e.g.*, Cal. Civ. Code § 1798.29(a).

[80] Fla. Stat. § 501.171(4)(a) (requiring notification of a breach "no later than 30 days after the determination of a breach or reason to believe a breach occurred" unless subject to a delay authorized by the statute).

[81] Comments of National Retail Federation (May 27, 2016) at 7.

[82] *Id.* at 3.

are already "overwhelmed by the volume of breach notices they receive," to tune out of such notices and risk not taking action when there one day is an actual risk of harm.[83] Likewise, public notices could cause some consumers to take unnecessary action by canceling credit cards or purchasing credit monitoring, thereby incurring additional costs without advancing their privacy interests.

III. The Proposed Rules Would Harm ISPs' Network Management and Security and Impede Legitimate Business Activities.

In addition to harming consumers, the proposed rules would interfere with ISPs' ability to manage and operate their networks and ensure reliable service, impede ISPs' legitimate business activities, and interfere with ISPs' ability to adequately address cybersecurity threats.

A. Classifying IP Addresses and MAC Addresses as CPNI Would Undermine ISPs' Ability to Manage Their Networks and is Impermissible Under the Plain Language of Section 222.

ISPs' use and disclosure of IP and MAC addresses is essential to the proper functioning of the Internet. As the Chief Technology Officer and Senior Vice President for Science and Technology at NCTA explained in a comprehensive technical supplement to NCTA's comments, the regulation of certain network information, such as IP addresses, would interfere with network operations, including the following:

a. Proper functioning of email services;

b. Creation and assignment of IPv6 addresses;

c. Delivery of certain Internet of Things services (such as home security);

d. Transmission of data necessary for network routing;

e. Cybersecurity information sharing that Congress and the Obama administration sought to encourage through the enactment of the Cybersecurity Information Sharing Act; and

[83] *FTC Comments* at 31-32.

f. Proper operation of the domain name system ("DNS").[84]

In addition, including IP addresses and similar technical information in the definition of CPNI would force consumers to make decisions about the use and disclosure of these critical network data elements that they do not have the technical understanding or expertise to make.[85] Consumers could withhold consent to use or disclose such information without understanding that their decisions *would not* increase privacy protection but *would* prevent their ISP from providing reliable and uninterrupted service.[86]

Charter concurs with NCTA's description of how the regulation of certain network information, such as IP addresses, would interfere with overall network operations. Indeed, Charter routinely uses IP addresses and MAC addresses specific to subscriber's modems for authentication purposes. For example, by verifying this technical information, customers are able to watch television through the Charter mobile app within their home as well as recover their username (but not password). These types of use cases account for more than 1.5 million transactions per month across Charter's customer base. Classifying IP addresses and MAC addresses as CPNI would restrict the use of such technical information in a way that would inhibit these seamless authentication activities for nearly 25 percent of Charter's customers, including some use cases that would now require customers to either physically visit a Charter store with a government-issued identification or wait several days for required information to arrive via the U.S. Postal Service.

[84] *NCTA Comments* Appendix at 2-5, 11-33.

[85] *Id.* at 6 ("This would result in complexity and confusion to end-users who would be required to decide how their data is used for base-level technical functionality without understanding the consequences.").

[86] *Id.* at 6-7; *Comcast Comments* 59-61 (explaining the importance of using and sometimes disclosing customer information to guard against security threats and to provide effective service).

Similarly, IP addresses and MAC addresses are used to facilitate a wide variety of technical support and troubleshooting operations. In particular, this information is used to identify and diagnose Internet connectivity issues. Again, classifying this information as CPNI would restrict Charter's ability to use that data to resolve issues, disrupting the customer experience and inhibiting Charter's (and other ISPs') ability to provide efficient and immediate technical support.

Apart from the practical problems that classifying IP addresses as CPNI would create, the Commission cannot do so under the statute. Section 222 defines CPNI, in relevant part, as "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*."[87] But a customer does not make an IP address available to the ISP; rather, the ISP assigns IP addresses to customers' devices.[88] Thus, as other commenters explained, an IP address is not "made available to the carrier by the customer," as is required for information to constitute CPNI under Section 222(h)(1)(A). Because expanding CPNI to include IP addresses contradicts the plain, unambiguous language of Section 222, the Commission's proposed rule constitutes an unreasonable interpretation of the statute.

Furthermore, even if IP addresses did meet this statutory requirement, which they do not, they would not fit under any of the data elements (quantity, amount, technical configuration,

---

[87] Section 222(h)(1)(A) (emphasis added). Section 222(h)(1)(B) also states that CPNI includes "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." Because this information specifically pertains to telephone customers, it is not relevant here.

[88] *NCTA Comments* Appendix at 14 ("IP addresses locate endpoints on the network and are assigned by the ISP to the customer devices." (footnote omitted)); *Comcast Comments* at 77 (noting that IP addresses fail to meet this test because "the ISP *assigns the IP address to the customer premise device*" (emphasis in original)).

type, destination, or location) that are included within the statutory definition of CPNI.[89] IP addresses provide no indication of the quantity or amount of Internet services used by a consumer. Indeed, an IP address is unaffected by a consumer's subscription plan, "amount" of data used, or time spent on the Internet. IP addresses also do not relate to the "technical configuration" or "type" of Internet services a consumer uses. They are assigned to the consumer and relate to the device through which service is provided. Likewise, they do not reveal the "destination" of the consumer's communications. The Commission seeks to shoehorn IP addresses into the definition of CPNI by likening them to customers' telephone numbers in the voice telephony context.[90] This analogy, however, does not reflect the unique network management function, described above, that IP addresses play in the Internet ecosystem. Moreover, the analogy is inapposite because Section 222(e) expressly excludes customers' phone numbers from the definition of CPNI. For all of these reasons, IP addresses cannot be classified as CPNI under Section 222(h).

B. The Proposed Rules Would Impede Network Operations.

Several other aspects of the proposed rules also would impede network operations. For instance, the Commission should make clear that its adoption of the *statutory* exceptions under Section 222(d) in the broadband context would not prevent ISPs from adequately protecting their networks from threats and from delivering reliable service to their customers. ISPs need to use and disclose CPNI—and other information—to protect their networks against cyber threats and fraudulent, abusive, or unlawful use of their services, including spam, copyright violations, or

[89] *See* 47 U.S.C. § 222(h)(1)(A); *Comcast Comments* at 77-78 (explaining how IP addresses do not fit the statutory definition of CPNI).

[90] *See NPRM*, 31 FCC Rcd at 2516 ¶ 45 (asserting that "IP addresses are roughly analogous to telephone numbers in the voice telephony context").

criminal activity.[91] ISPs need to use and disclose information for such purposes. For instance, if an ISP has reason to believe that copyright protected material is being unlawfully consumed on its networks, it may need to use CPNI in order to investigate. In addition, ISPs must ensure that users are valid customers, and they may need to use CPNI to authenticate a customer's request for service. This is common practice. Indeed, there are many additional examples, which is why the plain language of the statute allows providers to use and disclose CPNI for such purposes.[92] The Commission does not have authority to rewrite the statute and must therefore ensure that any rules it adopts provide for these exceptions.

In addition, ISPs rely on third-party vendors and subject-matter experts to study and improve the reliability and security of broadband services in all of these areas.[93] Several commenters noted the importance of allowing the disclosure of such information to academics to foster research regarding data security, cybersecurity and network development and improvement.[94] The Commission's proposed rules would impede such beneficial—and essential—uses and sharing of critical information. The Commission therefore should make clear that such disclosures also are permitted under any rules it adopts.

---

[91] *See Comcast Comments* at 59-61 (discussing the permitted uses of customer information under Section 222(d)(2) to protect against illegal and abusive network uses).

[92] 47 U.S.C. § 222(d)(2) (allowing carriers to use, disclose, and permit access to CPNI "to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services").

[93] *Comcast Comments* at 60 (discussing information-sharing relationships with third parties to prevent and respond to such threats).

[94] *See, e.g., Comcast Comments* at 60; Comments of Lehr and Kenneally, (May 27, 2016) at 7-9, http://apps.fcc.gov/ecfs/document/view?id=60002081123 (explaining the importance of consumer data that "is important to enable and sustain academic research and a viable and vigorous ecosystem of third-party analysts and sustaining market competition across the value chain").

Several commenters urged the Commission to limit the exceptions under Section 222(d) to the use and disclosure of CPNI because Section 222(d) explicitly references only CPNI.[95] This argument merely proves Charter's point that Section 222 does not and cannot apply to any customer information beyond CPNI. That Section 222(d) references CPNI and not some other category of customer information shows that Congress intended to limit Section 222—with respect to customer information—to CPNI. As discussed above, any other reading renders the statute incoherent.[96]

Furthermore, limiting the exceptions under Section 222 to CPNI, while extending the rest of Section 222 to all customer personally identifiable information, would run headlong into the efforts that the Commission and industry, working together through the Commission's Communications, Security, Reliability, and Interoperability Council ("CSRIC") IV, have made to improve cybersecurity. Among other things, these efforts have included developing and adopting best practices that encourage robust sharing of cyber threat information, whether such information meets the technical definition of CPNI or not.[97] Moreover, ISPs regularly use a wide variety of data—including IP addresses, MAC addresses, and domain information—to model potential future threats, operate "feedback loops" which allow customers to better manage security risks to their email, proactively reset customers' passwords when a customer's email address has been compromised and is being used for malicious purposes, and help law

[95] *See* Comments of Electronic Frontier Foundation (May 27, 2016) at 8 ("We also disagree with the Commission's proposal to interpret the statutory exceptions in [Sections] 222(c) and (d) to include any customer [proprietary information], and not only CPNI." (footnote and internal quotation marks omitted)); Comments of New America Open Technology Institute (May 27, 2016) at 38-39 (urging the Commission not to extend Section 222(d) to cover "customer proprietary information" other than CPNI).

[96] *See supra* at 6.

[97] Communications Security, Reliability, and Interoperability Council IV, *Cybersecurity Risk Management and Best Practices Working Group 4: Final Report* (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

enforcement implement botnet takedowns.[98] Thus, limiting Section 222(d) to CPNI also would significantly undermine ISPs' ability to, *inter alia*, protect their networks, authenticate customers, respond to customer service requests, conduct customer satisfaction surveys, maintain parental controls, and prevent fraud.

C. The Proposed Rules Would Impede the Ability of ISPs to Address Cybersecurity Threats.

Finally, the Commission's proposed data security rules are overly prescriptive and do not give ISPs the flexibility they need to adapt to threats and changes in technology. In particular, the Commission should not impose strict requirements on ISPs to "*ensure* the security, confidentiality, and integrity of all [customer proprietary information]."[99] Perfect cybersecurity is not possible.[100] Instead, the Commission should enable ISPs to engage in risk management, which numerous federal agencies—including the Commission—have recognized is the key to strong cybersecurity protection.[101]

Risk is not static, and it cannot be eliminated. As NIST has explained, organizations must have the flexibility to determine what risk level is acceptable given the size and nature of their operations.[102] Moreover, proper risk management requires companies to be flexible and

---

[98] Comments of Messaging Malware Mobile Anti-Abuse Working Group Comments (May 27, 2016) at 3, 5.

[99] *NPRM*, 31 FCC Rcd at 2608-09 App. A (proposed rule 64.7005(a))(emphasis added).

[100] Jessica Rich, Alliance Against Fraud Coalition, National Consumers League, FTC, *Data Security: Why It's Important, What the FTC is Doing About It* 4 (Mar. 24, 2014), https://www.ftc.gov/system/files/documents/public_statements/295751/140324nclremarks.pdf (stating that the FTC recognizes that 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").

[101] *CTIA Comments* at 148-49.

[102] Nat'l Inst. of Standards & Tech., *Framework for Improving Critical Infrastructure Cybersecurity* 2 (Feb. 2014) ("NIST Framework"), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf ("Organizations will continue to have unique risks—different threats, different vulnerabilities, different risk tolerances—and how they implement the practices in the Framework will vary. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent.").

adapt to changes in technology and the threat landscape. The proposed rules, however, would create a "compliance mindset," deterring ISPs from developing innovative ways to combat cybersecurity threats, and thereby making networks and consumers' data less secure.[103]

The Commission should recall its prior position supporting a voluntary, industry-led approach. Two years ago, Chairman Wheeler made clear that the Commission would seek to regulate *only after* it had determined that industry had been unsuccessful.[104] Indeed, referring to the cybersecurity framework that various critical infrastructure industry sectors worked with NIST to develop ("NIST Framework"),[105] Chairman Wheeler said at that time, "[o]ur nation chose" risk management "over a traditional regulatory approach of prescriptive government mandates," and that this was appropriate because "[t]he pace of innovation on the Internet is much, much faster than the pace of a notice-and-comment rulemaking."[106] Industry has worked hard to adopt the NIST Framework, and just last year, members of the Commission's own CSRIC IV Working Group 4 developed and have begun to implement comprehensive best practices that are based on the NIST Framework and tailored to each communications industry sector. There is no reason to undermine these efforts by imposing baseline minimum standards on industry through this NPRM.

At most, the Commission should adopt the FTC's approach, which requires companies to follow commercially "reasonable" standards of care.[107] The FTC has refrained from imposing particular data security requirements on companies, recognizing that "industries and businesses

---

[103] *CTIA Comments* at 151-52 (explaining the specific ways in which the proposed rules would make networks less secure).

[104] Chairman Tom Wheeler, Remarks at American Enterprise Institute 1, 3 (June 12, 2014) ("Wheeler Remarks at AEI") https://apps.fcc.gov/edocs_public/attachmatch/DOC-327591A1.pdf.

[105] NIST Framework, *supra* n.154.

[106] Wheeler Remarks at AEI at 3-4.

[107] FTC, Data Security, https://www.ftc.gov/datasecurity (last visited June 29, 2016).

have a variety of network structures."[108] This approach has worked well, allowing companies to adapt to changes in technology and business models and to keep pace with evolving standards of care.

CONCLUSION

For the reasons discussed above, the Commission should decline to adopt its proposed rules. It should study these issues further before issuing rules that are lawful and appropriately tailored.

Respectfully submitted,

/s/ Nancy C. Libin
Nancy C. Libin
Counsel for Charter Communications, Inc.

July 6, 2016

[108] 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.