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
	)	
	)	

PETITION FOR RECONSIDERATION OF CTIA

Thomas C. Power
Senior Vice President and General Counsel

Maria Kirby
Assistant Vice President, Regulatory Affairs
and Associate General Counsel

Scott K. Bergmann
Vice President, Regulatory Affairs

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

January 3, 2017

TABLE OF CONTENTS

EXECUTIVE SUMMARY

CTIA members are committed to safeguarding the privacy and security of their customers' data, and they have invested heavily in programs and processes to do so. Although CTIA members acknowledge Commission efforts to address the complicated issues of data privacy and security, the rules adopted in the *Report and Order* (the "Rules") actually undermine the Commission's stated goals.

CTIA's Petition for Reconsideration ("Petition") identifies material errors and omissions in the *Report and Order* and urges the Commission to address several arguments that were presented to the Commission during the Comment period but were not fully considered, and vacate, modify, or clarify the Rules accordingly. Specifically, the Commission should reconsider its application of the Rules to broadband service. If the Commission nevertheless declines to vacate the Rules in their entirety, it should limit the scope of information to which the Rules apply to customer proprietary network information ("CPNI"), amend certain definitions in the Rules, reconsider restrictions that the Rules impose on the use of financial inducements and service offerings in exchange for the use of customer information, allow providers flexibility to determine when to provide notice to customers, and narrow several aspects of the data breach notification requirements to align with the approaches taken by the Federal Trade Commission ("FTC") and state laws.

Moreover, CTIA encourages the Commission to follow Commissioner Pai's suggestion and *fully* harmonize the Rules with the longstanding guidance provided by the FTC.[1] For instance, the Rules should allow providers to infer consent to use customer information for internal purposes and first-party marketing in most circumstances and should align the definition of "sensitive information" with the FTC's definition, which does not include web browsing or application usage history.

In addition, the Commission should vacate the Rules insofar as they are grounded in any statutory authority other than Section 222(c). The Commission suggests that Section 201(b), Section 202(a), Title III, and Section 706 may provide alternative bases for the Rules. The Commission's ability to regulate the privacy and security of customers' information is limited, however, to the authority Congress granted in Section 222(c), and none of these other provisions gives the Commission authority to impose privacy and security requirements.

Finally, if the Commission decides to preserve any aspects of the Rules, CTIA supports the Commission's decision to harmonize the broadband rules with the voice rules.

[1] *Report and Order* at Commissioner Pai dissent ("Commissioner Pai dissent) at 1 ("[S]ince the beginning of this proceeding, I have pushed for the [FCC] to parallel the FTC's framework as closely as possible.").

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
	)	
	)	

PETITION FOR RECONSIDERATION OF CTIA

Pursuant to Section 1.429 of the Commission's rules,[2] CTIA[3] hereby seeks reconsideration of several aspects of the *Report and Order* in the above-captioned proceeding.[4]

I. INTRODUCTION.

CTIA members take their obligations to protect the privacy and security of their customers' data seriously. Indeed, Internet service providers ("ISPs") already carefully adhere to relevant state and federal laws that safeguard customer data. Beyond their legal obligations, CTIA members recognize that protecting their customers' data is a good business practice. Thus, they have strong incentives to earn and maintain consumer trust and loyalty by doing so. Unfortunately, however, the Commission's goal of protecting the privacy and security of broadband customers' data is undermined by the rules outlined in the *Report and Order* (the "Rules") which suffer from serious infirmities. Accordingly, CTIA requests that the

---

[2] 47 C.F.R. § 1.429.

[3] CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[4] *In re Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Report and Order, __ FCC Rcd ___, FCC 16-148, WC Docket No. 16-106 (rel. Nov. 2, 2016) ("*Report and Order*").

Commission reconsider its application of the Rules to broadband service and to information beyond CPNI, and to vacate the Rules insofar as necessary on these grounds, as explained below.

II. THE COMMISSION DOES NOT HAVE AUTHORITY TO RECLASSIFY BROADBAND AS A "COMMON CARRIER" SERVICE.

As CTIA argued in its Comments, Section 222 is a Title II provision that, at its outermost edges, reaches only telecommunications service providers' provision of telecommunications services.[5] If broadband service cannot be classified as a telecommunications service, it follows that Section 222 cannot be extended to cover ISPs' provision of broadband service. Therefore, if the Commission reverses its decision to reclassify broadband services as telecommunications services, it should repeal the Rules as they apply to broadband services.[6] The new Rules, however, should stay in effect as they apply to traditional telecommunications services, provided that they are aligned with the FTC's approach to privacy and data security, as outlined below.

III. THE COMMISSION DOES NOT HAVE AUTHORITY TO EXTEND SECTION 222 TO THE PROVISION OF BROADBAND SERVICE.

In paragraphs 336 through 341 of the *Report and Order*, the Commission argues that Section 222 should be read to reach beyond telephony to cover broadband services. Specifically, the Commission seeks to shoehorn jurisdiction over broadband services into Section 222(a) and dismiss the telephone-specific language found in other subsections of Section 222.[7] As Commissioner O'Rielly noted, the Commission, in so doing, "is forced to ignore or explain away language that clearly contradicts its position, regulate by analogy, or simply create new

[5] Comments of CTIA, WC Docket No. 16-106, at 14 (filed May 26, 2016) ("CTIA Comments").

[6] Several parties are seeking a rehearing en banc of the D.C. Circuit's recent decision in *U.S. Telecom Ass'n v. FCC*, 825 F.3d 674 (D.C. Cir. 2016), which upheld the Commission's *Open Internet Order*.

[7] *Report and Order* ¶ 341 ("[E]ven if commenters could establish that these more specific parts of Section 222 are qualified in ways that limit their scope to voice telephony . . . or that exclude BIAS from their scope, we would still find that a[n] [ISP] . . . has customer privacy obligations under Section 222(a).").

obligations out of thin air."[8] Indeed, the Commission's argument that it has authority to regulate the data privacy and security practices of broadband providers fails as a matter of statutory interpretation, as Section 222 refers throughout to "voice" services, and contravenes the legislative history of the Act.[9] The Commission's extension of Section 222 to cover broadband services is therefore neither permissible nor reasonable and should be reconsidered.

IV. SECTION 222(a) DOES NOT GIVE THE COMMISSION AUTHORITY OVER ISPs' DATA PRIVACY AND SECURITY PRACTICES BEYOND THOSE RELATED TO CPNI UNDER SECTION 222(c).

The Commission concludes that Section 222(a) provides legal authority to impose a duty on broadband providers to protect a new, made-up category of information that the Commission calls "customer proprietary information."[10] As the comments of CTIA and others made clear, however, Section 222(a) does not impose any such duty beyond CPNI.[11]

---

[8] *Report and Order* at Commissioner O'Rielly dissent ("Commissioner O'Rielly dissent") at 1.

[9] CTIA Comments at 16-28; CTIA Reply Comments to Opposition to CTIA's Petition for Partial Reconsideration, WC Docket Nos. 11-42, 09-197, 10-90, at 6-8 (filed Oct. 19, 2015).

[10] *Report and Order* ¶¶ 343-345. Specifically, the Commission argued that the record contains no evidence that Congress intended Section 222(a) to be narrowly construed and the "most natural reading of Section 222(a) is that it imposes a broad duty on telecommunications carriers to protect proprietary information, one that is informed by but not necessarily limited to the more specific duties laid out in subsections (b) and (c)." *Report and Order* ¶ 345.

[11] 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. Congress drafted and structured Section 222 clearly: Congress articulated its general intent in subsection (a) and different carriers' specific obligations in the subsections that followed. Section 222(b) explains how this general prohibition operates with regard to *carriers'* proprietary information, and it "functions to cross reference overall concerns that some believed that equipment procurement by old-school [BOCs] would lead to sharing of improper information from manufacturers." Commissioner O'Rielly dissent at 1. As CTIA noted in its comments and Commissioner O'Rielly pointed out in his dissent, Section 273(g) of the Act outlines the Commission's authority to act with respect to the "proprietary information" of *equipment manufacturers*, and Section 273(d)(2) establishes confidentiality protections for information provided to standard-setting bodies and other entities. Section 222(c) explains the same with respect to *customers*, and, as commenters explained, it expressly limits the type of *customer* information to which the statute applies to CPNI, which is defined in Section 222(h). *See* CTIA Comments at 25-26 & n.53; Commissioner O'Rielly dissent at 1; *see also, e.g.*, Comments of AT&T, WC Docket No. 16-106, at 103-108 (filed May 27, 2016) ("AT&T Comments"); Comments of Sprint, WC Docket No. 16-106, at 5-6 (filed May 27, 2016); Comments of T-Mobile, WC Docket No. 16-106, at 16-17 (filed May 27, 2016); Comments of Verizon, WC Docket No. 16-106, at 53-60 (filed May 27, 2016).

Moreover, as CTIA explained in its Comments, and as Commissioner O'Rielly stated in his dissent, there is an important difference between "proprietary information," which Section 222 protects, and "personally identifiable information" and "personal information," which data privacy and security statutes already protect.[12] As an initial matter, the Commission misconstrues the definition of "proprietary" to include data that are widely available to the public and non-ISP providers in the online ecosystem. All kinds of data are made available to ISPs in a manner that is unique to ISPs, but what matters from a privacy perspective is whether the data are available to other parties. For example, MAC addresses and device identifiers are widely shared and collected across the Internet ecosystem and are in no sense "proprietary" information to anyone.[13] Similarly, IP addresses are broadcasted to websites when a person browses the web.[14] The Commission, however, tries to have it both ways: it argues that "proprietary information" covers "information that should not be exposed widely to the public," but it then dismisses the inconvenient fact that IP addresses are widely available by stating that, "whether information is available to third parties does not affect whether it meets the statutory definition of CPNI."[15]

In addition, the *TerraCom NAL*,[16] which the Commission incorrectly cites as precedent,[17] does not support this new definition of "proprietary information." The *TerraCom NAL*

[12] CTIA Comments at 31-34; Commissioner O'Rielly dissent at 2-3.

[13] *See* Peter Swire et al., *Online Privacy and ISPs* 71 & n.21 (The Institute for Information Security & Privacy at Georgia Tech, Working Paper, Feb. 29, 2016) ("*Swire Report*").

[14] *See, e.g.*, AT&T Comments at 13-25 (tracking exchange of information among hypothetical user, ISP, websites, search engines, apps, operating systems, and other entities in online ecosystem).

[15] *Report and Order* ¶¶ 70, 86; *see also* Commissioner O'Rielly dissent at 3.

[16] *In re TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325 (2014) ("*TerraCom NAL*").

[17] Notices of apparent liability for forfeiture represent only "tentative conclusions" of the Commission. *See, e.g., CBS Corp. v. FCC*, 663 F.3d 122, 130 (3d Cir. 2011), *cert. denied*, 132 S. Ct. 2677 (2012).

improperly and through tortured logic attempted to bootstrap "personal information" into the statutory definition of "proprietary information." Far from enhancing the Commission's argument, the statutory provisions that the Commission cited to in that notice of apparent liability actually support CTIA's position that "proprietary information" is *not* "personal information," but rather is information that warrants protection because of its commercial value.[18]

Moreover, the cases that the Commission cites in the *Report and Order* also undermine its expansive interpretation of Section 222(a). For instance, the Commission cites *National Cable & Telecommunications Ass'n v. FCC*[19] for the proposition that specific statutory provisions (*i.e.*, Sections 222(b) and 222(c)) do not circumscribe a general provision (*i.e.*, Section 222(a)).[20] Yet in *NCTA*, the "specific" provision at issue described the "*minimum* contents of regulations," thus leaving it open to the Commission to "cover a broader field" under the more "general" provision.[21] Unlike the "specific" provision at issue in *NCTA*, which invited

[18] *Report and Order* ¶ 85 n.192. Specifically, the two Communications Act provisions that the *Report and Order* points to in the *TerraCom NAL* concern the protection of confidential corporate information. For instance, the Commission cited to a Communications Act provision that requires the Corporation for Public Broadcasting to "maintain for public inspection certain financial information about programming grants;" but because "Congress also recognized that 'proprietary, confidential, or privileged information' should not be made public," it "expressly excluded such information from public discourse." *TerraCom NAL*, 29 FCC Rcd at 13330-31, ¶15. Congress did not protect this information because it was "personal," but because it could reveal programming funders' financial information. The Commission also noted that because entities that review telephone equipment interoperability "necessarily gain access to extremely valuable trade secrets, Congress explicitly prohibited those review entities from 'releasing or otherwise using any proprietary information' belonging to the manufacturer without written authorization." *TerraCom NAL*, 29 FCC Rcd at 13330-31, ¶15. (As discussed earlier, the entities that review equipment interoperability are governed by 47 U.S.C. § 273(d)(2). *See supra* note 11.) Again, Congress used the term "proprietary" to describe corporate—not personal—information that warranted protection because of its commercial value.

[19] 567 F.3d 659 (D.C. Cir. 2009) ("*NCTA*").

[20] *See Report and Order* ¶ 349 n.1019 (citing *NCTA*, 567 F.3d at 661).

[21] *NCTA*, 567 F.3d at 665 (emphasis added).

Commission expansion, Section 222(c) clearly limits the scope of customer information in Section 222(a) to CPNI, which is itemized specifically in Section 222(h).[22]

For the reasons stated above, Section 222 does not give the Commission authority to impose requirements on telecommunications carriers with respect to customer data beyond CPNI, and the Commission should vacate or modify the Rules accordingly.

V. IF THE COMMISSION DECLINES TO VACATE THE RULES IN THEIR ENTIRETY, IT SHOULD MODIFY THEM TO PROVIDE A MORE FLEXIBLE AND WORKABLE PRIVACY FRAMEWORK FOR ISPs.

If the Commission declines to vacate the Rules based on the foregoing, it should at least adopt Commissioner Pai's approach and modify them to parallel the FTC's technology neutral framework.[23] Moreover, it should modify the Rules regarding first-party marketing, not only to align with the FTC's approach, but also to comply with the First Amendment.

A. Web Browsing and App Usage History Should be Excluded from the Definition of "Sensitive Information."

CTIA urges the Commission to embrace the FTC's approach in full, including the FTC's definition of "sensitive information," which excludes web browsing and app usage history and their functional equivalents.

---

[22] The legislative history also supports this interpretation. *See* CTIA Comments at 28-29 (noting that when the full Congress passed Section 222, it did not include language that would have broadened the scope of customers' "proprietary information," but chose instead to pass a bill that *limited* the scope of Section 222 to CPNI). The Commission also cited *RadLAX Gateway Hotel, LLC v. Amalgamated Bank*, 132 S. Ct. 2065 (2012), to support its claim that the bedrock principle of statutory construction—that the specific governs the general—does not apply here. *Report and Order* ¶ 351 n.1028. The Commission concluded that the statement of general principles regarding customers' "proprietary information" in Section 222(a) should be read to expand the scope of the specific statutory obligation related to CPNI that is articulated in Section 222(c). *Report and Order* ¶ 351. But as CTIA made clear in its comments, if Section 222(a) imposed obligations with respect to customer information *beyond* CPNI, then the rest of Section 222 would both be incomprehensible and lead to absurd results. *See* CTIA Comments at 27-28 (showing that Section 222 is coherent and internally consistent *only if* it is read to limit customers' "proprietary information" to CPNI). The court in *RadLAX* recognized that, in such circumstances, the specific *should* supersede the general. *RadLAX*, 132 S. Ct. at 2072 (finding that the statutes should be interpreted under the "general/specific canon" where reading it otherwise would be "a surpassingly strange" way to achieve the purpose of the statute).

[23] *Report and Order* at Commissioner Pai dissent at 1.

As an initial matter, the Commission did not and cannot cite any record support for its assertion that web browsing and app usage history are "sensitive." Indeed, no other agency has classified such information as "sensitive," and the survey data that the Commission relies on contradicts its position.[24]

Moreover, the Commission cannot justify imposing these restrictions based on the false assertion that ISPs can "see every packet that a consumer sends and receives over the Internet," while edge providers see only a "slice" of consumers' Internet traffic.[25] As Commissioner Pai noted, this claim is without *any* basis in the record or reality.[26] Indeed, the Commission ignored entirely evidence in the record to the contrary, including EPIC's Comments, which state that it is "obvious that the more substantial threats for consumers are not the ISPs," as they do not have access to the data that large edge providers do.[27] The Commission also dismissed the findings in Professor Peter Swire's report, which found that certain technologies that are widely available and increasingly used—such as encryption and Virtual Private Networks—substantially limit ISPs' visibility into users' online activity, and that because the typical user accesses the Internet through multiple devices and various ISPs and Wi-Fi networks throughout the day, ISPs, at best, have fractured and variable access to web browsing activity and app usage.[28] Not only does the

[24] According to the Pew Report that the Commission cites, adults surveyed considered Social Security numbers, health information, the contents of phone conversations and email messages, and details of physical location over time to be "very sensitive." However, websites visited, search requests, media watched, and purchases made were deemed less so. *See* Lee Rainie, *The State of Privacy in Post-Snowden America*, PEWRESEARCHCENTER (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ ("Pew Report").

[25] *Report and Order* ¶ 30; *see also id.* ¶ 185 (stating that because of "the particular visibility of this information" to ISPs "web browsing history and application usage history, and their functional equivalents, are sensitive customer PI").

[26] Commissioner Pai dissent at 2.

[27] Comments of the Electronic Privacy Information Center, WC Docket No. 16-106, at 15 (filed May 27, 2016), ("EPIC Comments").

[28] CTIA Comments at 7-8; *Swire Report* at 23-34.

Commission lack factual support to characterize these categories of information as "sensitive," the Commission does not define these categories at all, imposing an enormous burden on providers to attempt to determine the precise scope of these terms.

Finally, consumers would not benefit from characterizing these data elements as "sensitive," as other participants in the online marketplace can access and use such data for their own marketing.[29] Indeed, there is no evidence whatsoever of privacy harms that consumers have experienced under the FTC's definition, which excludes these categories of data.[30] And in any event, it is not necessary to expand the definition, as any web browsing or app usage history that reveals information that the FTC considers sensitive, such as financial or health information, already would be covered under the definition of "sensitive information."

The Commission should therefore modify the Rules to exclude web browsing and app usage history from the definition of "sensitive information."

B. The Rules Improperly Restrict ISPs' Use of Customer Information for Most First-Party Purposes.

In the 2012 *Privacy Report*, the FTC recognized that companies generally should be able to engage in first-party uses of customer information on the basis of the customer's inferred consent.[31] Such uses generally do *not* raise privacy concerns, because they are consistent with

[29] Moreover, as CTIA explained in its comments, because information about consumers' online activities are widely available to a host of entities and available for purchase from data aggregators, the Commission's Rules would not do anything to prevent ISPs from purchasing this same information from other sources. Reply Comments of CTIA, WC Docket No. 16-106, at 54-55 (filed July 6, 2016) ("CTIA Reply Comments"); CTIA Comments at 49 n.141, 131. The Rules therefore would not materially benefit consumers.

[30] The FTC has a long history of effectively protecting consumer privacy through its sensitivity-based framework and strong *ex post* enforcement regime. *See* CTIA Reply Comments at 2 n.5 (citing numerous comments praising FTC's privacy enforcement approach).

[31] *See* FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers* 39-40 (Mar. 2012) ("*FTC Report*"), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commissionreport-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; *see also* CTIA Reply Comments at 72.

consumer expectations and the context of the relationship between the company and the customer, and because they do not risk a loss of customer control.[32]

The Commission should follow this well-reasoned approach and permit ISPs to use customer information (including individually identifiable CPNI) to engage in most first-party uses based on customers' inferred consent.[33] First-party marketing, for example, quintessentially falls within the context of the carrier-customer relationship,[34] and in a converging media landscape, as Commissioner O'Rielly noted, ISPs should be permitted to use customer information to market all products and services offered by any of its affiliates so long as the relationship is clear to customers. If such marketing exceeds the scope of Section 222(c), the Commission should exercise its forbearance authority.[35]

Further, the Commission should confirm that providers may use all customer information to the extent such use is limited to internal business intelligence and analytics. Such use is separate from direct contact with customers based on this information, which would be subject to the same consent requirement that would apply irrespective of the preceding internal use—*i.e.*, inferred consent for most first-party marketing but opt-in approval for marketing involving the deliberate use of sensitive information. The Commission likewise should confirm that providers may use any customer information in the "provision" of certain services that the Commission has

[32] CTIA Reply Comments at 72; CTIA Comments at 8-9, 120-22.

[33] *See FTC Report* at 47-48 ("[T]h[e] requirement of affirmative consent for first-party marketing using sensitive data should be limited [to] . . . where a company's business model is *designed to target* consumers based on sensitive data . . . .").

[34] *See generally FTC Report* at 40-48 (discussing first-party marketing general rule and exceptions).

[35] *See* Commissioner O'Rielly dissent at 6; Letter from James J.R. Talbot, AT&T, to Marlene H. Dortch, Secretary, FCC, WC Docket 16-106 at 4 (dated Oct. 4, 2016) ("AT&T Ex Parte") (explaining that doing so would meet the three-part test for forbearance under Section 10 of the Communications Act); *see also FTC Report* at 41-42 (explaining that affiliates are first parties where relationship is clear).

recognized are "necessary to, or used in, the provision of service."[36] And, the Commission should confirm that consent is implied to use customer information for the purpose of de-identifying or aggregating data; such analysis is wholly internal and reduces privacy risks in any event.

The *Report and Order* offer no record-based justification for creating asymmetric restrictions with respect to ISPs' first-party uses of customer information.[37] First, the Commission's reliance on the Do Not Call Registry and CAN-SPAM regulations is misplaced. To be sure, the Do Not Call Registry permits consumers to "opt out of receiving calls even from companies with which they have a prior business relationship," and CAN-SPAM likewise allows consumers to "opt out of the receipt of future commercial email."[38] But both systems presume consent *until* a customer exercises the right to opt out, after which point companies, irrespective of any prior business relationship, must cease marketing communications. Here too, the Commission should recognize that first-party marketing is inherently consensual until the customer opts out.[39] Second, the Commission mischaracterizes the record in this proceeding, stating that "the record . . . indicates that customers expect choice with regard to the privacy of their online communications."[40] The comments the Commission cites for this proposition, however, have *nothing* to do with consumers' attitudes about the use of customer information for

[36] *Report and Order* ¶ 206 (defining these services to include, for example, upkeep of "[customer premises equipment], as well as other customer devices, inside wiring installation, maintenance, and repair, as well as technical support").

[37] *Id.* ¶¶ 199-200.

[38] *Id.* ¶ 200.

[39] Moreover, the Do Not Call Registry and CAN SPAM rules, which apply to telecommunications carriers, already address how customers can opt out of receiving marketing messages and therefore obviate the need for further mechanisms here.

[40] *Report and Order* ¶ 199.

the delivery of first-party marketing.[41] And none of these commenters explains why a customer's expectations within the context of his or her relationship with an ISP would be any different from expectations with other large-platform providers.[42]

Moreover, as the *Report and Order* recognizes, such uses can yield substantial customer benefits.[43] For example, first-party marketing facilitates promotion of new and enhanced services, products, and bundles, enhancing competition.[44] This effect is far from speculative; the market for mobile products and services is highly competitive,[45] and mobile ISPs have demonstrated their commitment to pro-consumer and pro-competitive packaging.[46]

Accordingly, the Commission should amend the Rules to permit the use of customer information for most first-party purposes.

C. Restrictions on the Use of Information Collected From and About Customers in the Ordinary Course of Business Should Be Deemed Unconstitutional.

In addition, restrictions on the use of information collected from and about customers in the ordinary course of business—including, but not only, for marketing purposes—are unconstitutional restrictions on protected speech.[47] The Commission asserts incorrectly that its choice regime governing ISPs' uses and disclosures of customer information meets the multipart

---

[41] *Id.* ¶ 199 n.580. For example, the Commission cites several Comments that make assertions about customer expectations generally but that do not discuss consumer concerns about first-party online marketing—and that fail to cite any third-party source for support in any event.

[42] *FTC Report* at 56.

[43] *Report and Order* ¶ 385.

[44] CTIA Comments at 79-80, 126-27.

[45] CTIA Reply Comments at 55-56.

[46] CTIA Comments at 79-80.

[47] *See U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1228 n.1 (10th Cir. 1999); Laurence H. Tribe, *The Federal Communications Commission's Proposed Broadband Privacy Rules Would Violate the First Amendment, attached to* Letter from Thomas C. Power, CTIA, Rick Chessen, NCTA, and Jon Banks, USTelecom, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 (filed May 27, 2016). Although this Petition analyzes the Rules under intermediate scrutiny, CTIA reasserts that the proper analysis should proceed under *Sorrell v. IMS Health, Inc.*, 564 U.S. 552 (2011).

Central Hudson test and therefore is constitutional.[48] The Commission, however, has failed to justify the restrictions at each step, and the Commission's last-minute adoption of a sensitivity-based choice regime does not cure these constitutional infirmities.[49]

First, the Commission has failed to articulate a record-based and cognizable state interest to justify the rules.[50] The Commission asserts that a "substantial public interest" in protecting customers' privacy extends to controlling the *use* of customer information and not just the *disclosure* of such information.[51] As CTIA set forth, this assertion is unmoored from the case law, and the only record support for a use-based theory of privacy harm are comments that lack any nexus to ISP practices or Section 222 and/or that rely on speculation.[52] It is thus unsurprising that the *Report and Order* suffers from similar shortcomings, citing academic literature for the proposition "that misuse by the collecting entity can harm individuals' privacy, even apart from disclosure."[53] Like the pro-NPRM commenters, however, the Commission offers no actual evidence that ISPs' purely internal (*e.g.*, intelligence and analytics) or contextual

[48] *See, e.g.*, *Report and Order* ¶ 375. Under *Central Hudson Gas &Electric Corp. v. Public Service Commission of New York*, 447 U.S. 557 (1980), if commercial speech concerns lawful activity and is not misleading, then the government may restrict it only if (1) the interest advanced by the regulation is substantial; (2) the regulation and materially advances that interest; and (3) the regulation is not more extensive than necessary, *id.* at 566.

[49] CTIA's focus in the instant Petition on the "use" restrictions is not intended to waive CTIA's position that the restrictions on disclosure fail the *Central Hudson* test as well because the latter lack adequate support in the record. *See* CTIA Reply Comments at 48-51. Further, the Commission's classification of web browsing and app usage as sensitive information, in particular, is unmoored from any record-based theory of privacy harm (*i.e.*, there is no valid state interest justifying this classification) and creates asymmetric rules for ISPs vis-à-vis other edge providers (*i.e.*, the classification fail to advance any state interest, given the open nature of the ecosystem), and therefore independently fails constitutional scrutiny.

[50] *See U.S. West*, 182 F.3d at 1234-35; CTIA Comments at 81-82.

[51] *Report and Order* ¶ 376.

[52] *See* Letter from Scott K. Bergmann and Maria L. Kirby, CTIA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 13-16 (filed Sept. 16, 2016) (analyzing privacy "harms" associated with data collection and use relied upon by Paul Ohm, Public Knowledge, and New America's OTI).

[53] *Report and Order* ¶ 378. As CTIA has explained, although the state's interest in protection of privacy can extend to first-party uses that are uniquely vexatious or that intrude into a uniquely personal space (*i.e.*, the home), the record fails to establish such a cognizable interest here, and, in any event, that interest would justify, at most, opt-out restrictions. *See, e.g.*, CTIA Reply Comments at 46-47; CTIA Comments at 81-82, 88-90.

(*e.g.*, first-party marketing) uses of information in the ordinary course of business that do not involve disclosure to a non-affiliate creates any privacy-based risk of harm to customers.[54]

The Commission states that the Rules requiring customer approval for uses of information collected in the ordinary course of business satisfy the second prong of the *Central Hudson* test because they directly and materially advance the Commission's interest in protecting customer privacy. Specifically, the Commission asserts that the Rules prevent the use of personal information "without [customers'] prior approval in a way that the customers do not or cannot reasonably expect,"[55] and reflect customer expectations by applying graduated consent requirements based on the sensitivity of the underlying data.[56] But nothing in the record shows that customers do not expect first-party information processing, including marketing, by their ISPs. Indeed, the record supports the opposite conclusion.[57] Moreover, nothing in the record suggests that customers have unique privacy expectations or concerns as to their ISPs. Again, to the contrary, the record instead indicates that customers prefer uniform regulation of data in the online ecosystem.[58] And finally, nothing in the record substantiates that ISPs actually *are* a

---

[54] Instead, the *Report and Order* cites comments and secondary sources that make vague assertions regarding customers' concerns about online privacy and security generally but that fail to establish a causal connection between consumers' concerns about the use of personal data for first-party marketing and any reluctance on the part of consumers to use broadband services. *Report and Order* ¶¶ 379-380. This is inadequate. *See U.S. West*, 182 F.3d at 1234-35. Indeed, in one of the more bizarre paragraphs of the *Report and Order*, the Commission cites as support for the proposition that the state interest in privacy extends *beyond* disclosure, language from a D.C. Circuit opinion stating that there is a state interest in allowing a consumer to "determin[e] for oneself when, how, and to whom personal information *will be disclosed to others*." *Report and Order* ¶ 378 (emphasis added) (quoting *NCTA v. FCC*, 555 F.3d 996, 1001 (D.C. Cir. 2009)). And in support for the proposition that privacy concerns "chill[]" online activity, the Commission cites a study that proves the exact opposite—*viz.*, that online usage continues to increase, including usage of applications that create genuine privacy risks, notwithstanding any privacy concerns. *See* CTIA Comments at 70 n.217. Moreover, to the extent that the Commission has made a showing that a *minority* of survey respondents are concerned with data collection, *see Report and Order* ¶ 379, that showing is a non-sequitur, because Section 222(c) does not restrict *collection*, and at most supports only opt-*out* restrictions.

[55] *Report and Order* ¶ 382.

[56] *Id.* ¶ 383.

[57] *See* CTIA Reply Comments at 72; CTIA Comments at 8-9, 120-22.

[58] *See* Comments of Progressive Policy Institute, WC Docket No. 16-106, at 2 (filed May 26, 2016) ("By an overwhelming 90% - 8% margin, Internet users agree that '*all Internet companies should operate under the same set*

unique threat to privacy in the online ecosystem.[59] Under these circumstances, the imposition of differentiated restrictions on only one class of commercial speakers in an open ecosystem is independently disqualifying at *Central Hudson* step two.[60]

Finally, the *Report and Order* fails to justify the Rules at the third prong of the *Central Hudson* test: that any speech restriction is no more extensive than necessary. With respect to non-sensitive information, for example, the Commission acknowledges that customers expect that their information will be used for first-party marketing and that such uses yield customer benefits "in the form of more personalized service offerings and possible cost saving."[61] Especially in light of these benefits, there is no basis for not allowing ISPs to engage in first-party marketing involving at least non-sensitive information with inferred consent.[62]

Furthermore, with respect to the heightened consent requirement for uses of sensitive information, the Commission defends its Rules governing notice and choice only insofar as they apply to the *disclosure*, not to the *use*, of sensitive information.[63] Indeed, the latter application is indefensible as a constitutional matter. In the *Report and Order*, the Commission fails to offer

---

of rules and regulations so that standards are fair and equal across the board,' including 74% of Internet users who say they strongly agree with that statement.").

[59] *See* CTIA Reply Comments at 51-60. Further, even if the record *did* reflect that ISPs pose a unique privacy threat (which it does not), the Rules still would not materially advance any interest in privacy, because they would not prevent ISPs from purchasing identical information about their own customers from data brokers (strengthening the market position of those brokers) and lawfully using that information in the same ways that the Rules intend to restrict. *See* Commissioner O'Rielly dissent at 2, 5-6; CTIA Comments at 48-50. The free flow of customer information also demonstrates the absurdity of referring to such data as "proprietary."

[60] *See* CTIA Comments at 85-86 & n.272 (citing cases).

[61] *Report and Order* ¶ 385.

[62] The FTC's 2012 *Privacy Report* thoroughly examined the harms associated with the use of sensitive information and concluded that the use of non-sensitive information (and even most non-deliberate uses of sensitive information) for first-party purposes generally falls within consumer expectations and does not require customer choice. In contrast, opt-in approval *may* be warranted where a company's business model is designed to target consumers based on their sensitive data. CTIA Comments at 37-38, 120-21; *see also FTC Report* at 47-48.

[63] The Commission states that "the record reflects that customers reasonably expect that their sensitive information will not be *shared* without their affirmative consent," but it conspicuously does not state the same about the *use* of such information. *Report and Order* ¶ 386 (emphasis added).

any basis other than a reference to studies showing that default choices are "sticky" to support its assertion that an opt-out consent requirement would not be sufficient to protect consumers from harm resulting from the use of such information.[64] Ironically, the "stickiness" of default settings is an *independent reason* why the Rules *fail Central Hudson*; customers who are privacy neutral—or who affirmatively would prefer to exchange their privacy for cheaper service or enhanced offerings—will be "stuck" not receiving speech under the Commission's opt-in regime, notwithstanding their preferences. The rules are thus *a fortiori* more extensive than necessary. And in any event, because the Commission bears the burden of satisfying *Central Hudson*,[65] in the absence of evidence that privacy-conscious customers are not adequately protected by an opt-out regime, the Rules fail the third prong of *Central Hudson*.

D. Other Rule Definitions That Impermissibly Expand the Scope of the Commission's Authority Should be Amended.

In addition, the Commission should modify certain definitions that exceed the scope of the Commission's authority and will have unintended consequences.

CPNI. Congress already defined CPNI in Section 222,[66] and the Rules therefore should be amended to exclude the following information from the definition of CPNI:

- *Location information that is not precise geolocation information or call detail information*: the Commission suggests, without making clear, that CPNI includes only information that is "sufficiently precise to qualify as geo-location [information] CPNI";[67]

[64] *Id.* ¶ 387.

[65] *See, e.g.*, *Edenfield v. Fane*, 507 U.S. 761, 770-71 (1993).

[66] Section 222(h)(1)(A) defines CPNI as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use" of the telecommunications service, and "that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."

[67] *See Report and Order* ¶¶ 65-66; *see also id.* ¶¶ 9, 179 (defining "sensitive information" to include "precise geolocation information").

- *IP addresses*: because they are provided *to* the customer *by* the provider,[68] IP addresses do not meet the statutory definition of CPNI;[69]

- *Domain names*: they are similar to IP addresses and cannot be CPNI for the same reason;[70]

- *Customers' addresses*: such information is expressly excluded from the definition of CPNI under Section 222(e);[71]

- *Information that is linkable only to a device and not a specific individual*: Section 222 applies to "individually identifiable" CPNI and cannot capture data that is linked or linkable to a device, if that device is not linked to a specific individual;[72] and

- *The following information which is neither proprietary nor sensitive:*

    - *MAC addresses*: they are merely used to facilitate traffic flow between the provider and the customer's router;[73]

    - *Customer Premises Equipment and customer device information*: this information does not fall into any Section 222 data element;

    - *Application header information*: this information is sent between an end user's device and an edge provider in order to render service;[74] and

    - *Type of service* (fixed or mobile, cable or fiber): the customer and provider jointly agree on the service plan and, in many cases, the type of service offered already may be established and publicized by the ISP.[75]

[68] Comments of National Cable & Telecommunications Association, WC Docket No. 16-106, at Appendix at 14 (filed May 27, 2016); Comments of Comcast Corporation, WC Docket No. 16-106, at 77 (filed May 27, 2016); Comments of Paul Vixie, CEO, Farsight Security, WC Docket No. 16-106, at 6 (field May 1, 2016) ("Farsight Security Comments").

[69] *Report and Order* ¶ 168. Moreover, the analogy that the Commission makes to telephone numbers is inapposite, because Section 222(e) expressly excludes customers' phone numbers from the definition of CPNI.

[70] Farsight Security Comments at 6.

[71] Indeed, as CTIA noted, the Commission has long recognized that "the definition of CPNI does not include a customer's name, address, and telephone number." CTIA Comments at 45 (quoting *In re Implementation of the Telecommunications Act of 1996*, Order, 13 FCC Rcd 12390, 12395-96, ¶¶ 8-9 (1998)).

[72] Commissioner O'Rielly dissent at 3; AT&T Ex Parte at 4.

[73] Farsight Security Comments at 5.

[74] *Report and Order* ¶ 76.

[75] Farsight Security Comments at 5.

In addition, the Rules should not cover information that providers "create and append" to a customer's Internet traffic.[76] Such information is not "made available" to the carrier by the customer by virtue of the relationship, as required by the statute.[77]

Contents of communications. The Rules should define the "content of communications" as the FTC did in its comments to include only the "contents of emails; communications on social media; search terms; web site comments; items in shopping carts; inputs on web-based forms; and consumers' documents, photos, videos, books read, [and] movies watched."[78] The Commission's definition of "contents" is much more expansive[79] and potentially includes metadata, such as the source and destination email addresses, website URLs, names of applications that customers use, etc.[80] The *Report and Order* purports to base its definition on the Electronic Communications Privacy Act ("ECPA") and Section 705 of the Communications Act.[81] ECPA does not treat source and destination email addresses as "content," however, and courts have held that URLs are not "contents" of communications under ECPA.[82]

PII. The Rules should not include persistent online and advertising IDs in the definition of PII. Such information is used merely to facilitate online advertising, and because it is not

---

[76] *Report and Order* ¶ 51.

[77] *See* CTIA Comments at 48-50.

[78] FTC Comments at 20.

[79] *Report and Order* ¶ 102 (defining "contents" to include "any part of the substance, purport, or meaning of a communication or any other part of a communication that is highly suggestive of the substance, purpose, or meaning of a communication").

[80] *Id.* ¶¶ 103-104.

[81] The "contents" of a communication means "any information concerning the substance, purport, or meaning of" a communication under ECPA, 18 U.S.C. § 2510(8), and "the existence, contents, substance, purport, effect, or meaning" of a communication under Section 705 of the Communications Act, codified as 47 U.S.C. § 605(a).

[82] *See Graf v. Zynga Game Network, Inc.*, 750 F.3d 1098, 1104 (9th Cir. 2014) (holding that under ECPA, a user's Facebook ID and the URL of the webpage the Facebook user clicked on were not "contents of any communication" under ECPA, but rather "record" information (quotation marks omitted)); *see also In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125, 137 (3d Cir. 2015), *cert. denied* 137 S. Ct. 36 (2016) (stating that URLs that function merely as location identifiers for websites are not "content" under ECPA).

used, on its own, "to identify, contact, or precisely locate a particular individual," it does not constitute PII.[83]

Customer. The Rules should not define "customer" to include applicants as well as current customers. A relationship between the applicant and the provider is not final until there is an agreement to provide services.

Material change. Finally, the Commission should narrow the definition of "material change" to "any change that a reasonable customer would consider important to her decisions on her privacy," which would align with the FTC's definition (following Commissioner Pai's suggested approach) and would exclude the following language: "including any change to information required by the privacy notice described in section 64.2003."[84] Otherwise, even changes to the privacy notice that no customers, acting reasonably under the circumstances, would consider important to their privacy decisions would require opt-in consent, thus creating notice fatigue for consumers and imposing unnecessary costs on providers.

E. The Restrictions on Certain Service Offerings are Unnecessary.

The Commission should repeal Section 64.2011 of the Rules, which limits ISPs' offering financial incentives in exchange for the use of personal information and prohibits ISPs from offering service in exchange for such information. Because the record shows that competition among wireless broadband providers is strong and switching costs for consumers are low, these requirements are unnecessary.[85] Moreover, these restrictions would deny consumers access to

---

[83] Network Advertising Initiative, *Understanding Online Advertising*, https://www.networkadvertising.org/faq; *see supra* Part IV (explaining that Section 222 applies only to "individually identifiable" CPNI).

[84] *Report and Order*, App. A, § 64.2002(i); *see also id.* ¶ 158.

[85] *See* CTIA Reply Comments at 55-56; CTIA Comments at 115-16 (describing how wireless broadband providers are moving away from term-contracts with cancellation penalties and offering to pay for switching costs for new customers).

affordable services,[86] and would skew the marketplace, depriving consumers of the choice to share their information in exchange for benefits.[87]

F. The Rules Regarding Notice at the Point of Sale are Unnecessarily Inflexible.

The Rules require ISPs to provide customers their privacy policies at the point of sale.[88] ISPs should have flexibility, however, in determining when and how to provide notice for purposes of soliciting approval to use and disclose customer information. CTIA therefore urges the Commission to follow Commissioner Pai and adopt the FTC's approach, which gives companies flexibility regarding when they provide choice mechanisms and how they "design and develop choice mechanisms that are practical for particular business models or contexts."[89]

G. The Scope of Certain Aspects of the Data Breach Notification Requirements Should be Narrowed.

The Commission should make several changes to its Rules regarding data breach notification. Specifically, the Rules should require notification only when a provider determines that "harm" is reasonably likely to occur as a result of the breach. This not only is what consumers expect, but also is consistent with other breach notification statutes.[90] Moreover, this

---

[86] *See* Comments of MMTC, et al., WC Docket No. 16-106, at 8 (filed May 27, 2016) ("MMTC Comments") (explaining that not "all alternative payment programs are necessarily wrong or abusive" and noting that "low-income consumers . . . could benefit from discounts or other financial inducements offered by ISPs"); Comments of Asian Americans Advancing Justice, et al., WC Docket No. 16-106, at [unpaginated] 3 (filed May 27, 2016) ("AAPI Comments") ("If the Commission were to prohibit financial inducements that were designed to support low-income broadband adoption, more vulnerable AAPI consumers would be deterred from online use. Without affordable alternatives, efforts to prevent the aforementioned [discounted] services would only hurt…low-income communities.").

[87] CTIA Reply Comments at 30; Comments of Mobile Future, WC Docket No. 16-106, at 7-8 (filed May 27, 2016); AAPI Comments at [unpaginated] 3; MMTC Comments at 8.

[88] 47 C.F.R. § 64.2003(c)(1).

[89] *FTC Report* at 50.

[90] *See* Idaho Code Ann. § 28-51-105(1) (requiring notification only if harm has occurred or is reasonably likely to occur); Kan. Stat. §§ 50-7a01(h), 50-7a02(a) (same); Ky. Rev. Stat. §365.732(1)(a) (same); Neb. Rev. Stat. § 87-803(1) (same) S.C. Code § 39-1-90(A) (same).

change would accomplish what the Commission intended: it would prevent consumer alarm in cases where harm is not reasonably likely to occur.[91]

The Rules also should be limited to breaches of "sensitive" information, as defined in the Rules and amended as described above, or a customer's first name, or first initial and last name, in combination with one or more of the elements of CPNI or customer PI, not including a customer's address, phone number, or email address.[92] Otherwise, providers would be required to investigate every instance where customer data were affected, resulting in substantial costs and inefficiencies. In addition, the Rules should not define "harm" to include "emotional" harm, such as damage to reputation, embarrassment, and so forth, rather than just physical and financial harm. Such a subjective determination is virtually impossible to make and would lead to significant over-notification to customers where there is no reasonable belief that harm has occurred.

The Commission also should carve out from the definition of "breach" any unauthorized access (or access in excess of authorization) to customer PI by a person who has no *intent* to use or disclose such information. As the Commission itself acknowledged in the NPRM, even state data breach laws include exceptions for good faith access by employees or agents where the information was not used improperly or further disclosed.[93] Defining a breach more broadly would impose additional burdens on providers without any benefit to consumers. Indeed, if the

---

[91] *Report and Order* ¶¶ 272-73.

[92] As CTIA noted in its Comments, state data breach laws typically define "personal information" much more narrowly to include only certain types of information. *See, e.g.,* Ark. Code § 4-110-103(7) (defining "personal information" for purposes of breach notification as an individual's first name or first initial, plus last name in combination with any of the following data elements: Social Security number; driver's license or Arkansas identification card number; account number, credit card number, or debit card number in combination with any required security code, access code, or password that would allow access to an individual's financial account; and medical information); CTIA Comments at 176-77.

[93] *See In re Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, 31 FCC Rcd 2500, 2577 ¶ 242 (2016) ("NPRM") (*citing* Haw. Rev. Stat. § 487N-1); *see also* Ark. Code § 4-110-103(1)(B); Colo. § 6-1-716(1)(a); Mass. Gen. Laws ch. 93H, § 1; Wyo. Stat. § 40-12-501).

Rules do not include a carve out, providers would be required to notify customers whose accounts were accidently accessed by an agent during a customer service call because of a typographical error or misunderstanding.

Finally, the timeline for breach notification should not be triggered when a provider reasonably determines that a breach has occurred. Instead, the triggering event should turn on harm assessment (*i.e.*, when the provider establishes that harm has occurred or is reasonably likely to occur). This approach aligns with the Commission's intent and reasoning with respect to the timing of breach notification, as it ensures that the provider will be able "to properly determine the scope and impact of the breach, and to the extent necessary, to most immediately focus resources on preventing further breaches."[94]

VI. THE ALTERNATIVE STATUTORY BASES CITED BY THE COMMISSION FAIL TO PROVIDE AUTHORITY TO REGULATE BROADBAND CUSTOMER PRIVACY.

Despite Chairman Wheeler's commitment that this rulemaking would proceed under Section 222,[95] the Commission asserts, largely summarily, that other provisions of the federal telecommunications laws support the Rules.[96] CTIA respectfully urges the Commission to reconsider this results-oriented approach. As the Commission previously has recognized, it cannot look to generic statutory provisions to adopt rules that are inconsistent with more specific provisions that reflect Congress's express intent.[97]

---

[94] *Report and Order* ¶ 284.

[95] *See* Tom Wheeler, Testimony Before the Subcomm. on Privacy, Technology, and the Law, *Examining the Proposed FCC Privacy Rules* at 54:44-55:10 (May 11, 2016), http://www.judiciary.senate.gov/meetings/examining-the-proposed-fcc-privacy-rules.

[96] *See Report and Order* Part IV.B.

[97] *See In re Protecting and Promoting the Open Internet*, Report and Order on Remand, 30 FCC Rcd 5601, 5822 ¶ 465 n.1392 (2015).

The Commission makes the conclusory assertion that Section 201(b) and Section 202(a) provide the Commission with authority to regulate broadband providers' data privacy and security practices.[98] As CTIA has explained, however, neither provision gives the Commission such authority. And indeed, the Commission previously has recognized that Congress drafted Section 222 precisely because Section 201 did not cover privacy, stating when it adopted the 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."[99] In this new comprehensive framework, Congress set forth protections for CPNI and other categories of customer information described in Section 222 (such as aggregate customer information), but declined to set forth protections for a broader set of customer information, including personally identifiable information. The legislative history thus demonstrates that Congress unambiguously intended the Commission's privacy authority to be limited to the categories of information set forth in Section 222. This authority supersedes any prior authority the Commission had.[100]

The Commission fares no better invoking Title III to justify the Rules for mobile ISPs.[101] The Commission argues that its authority under Section 303(b) derives from the provision's requirement that the Commission "[p]rescribe the nature of the service to be rendered by each

---

[98] 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." Section 202(a) 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…for or in connection with like communication service."

[99] *In re Implementation of the Telecommunications Act of 1996*, Second Report and Order and Further NPRM, 13 FCC Rcd 8061, 8073 ¶ 14 (1998).

[100] *See* CTIA Reply Comments at 26-29. CTIA also independently has demonstrated that it strains credulity to claim that ISPs' privacy and data security practices are practices "in connection with" the provision of service; the practices are therefore beyond the scope of Sections 201 and 202 as a textual matter. *See* CTIA Comments at 61.

[101] *See Report and Order* ¶ 371.

class of licensed stations and each station within any class."[102] As CTIA explained, however, Section 303(b) does not give the Commission authority to regulate any aspect of the provider-subscriber relationship. Courts have limited the Commission's authority under this provision to adopt only rules that "define[] the form" of radio services for given license classes that fall within Section 303(b)'s ambit. The regulation of customer data falls outside this limited grant of authority.[103] Section 303(r) likewise fails. Although Section 303 enables the Commission to "[m]ake such rules and regulations … as may be necessary to carry out the provisions" of the Communications Act, it does not give the Commission unbounded authority to "carry out its mandates through rulemaking."[104] Rules emanating from Section 303(r) must be tethered to the use of otherwise-delegated authority. Because the Rules are not "necessary" to carry out Section 222's mandates, let alone those of any other Communications Act provision, Section 303(r) cannot serve as a basis for these Rules. Moreover, Section 316 does nothing more than provide the Commission with authority to modify the actual terms of radio station licenses through the procedural methods outlined in that statute. The Rules do not modify anything related to features of radio service governed by licenses. Rather, they would regulate ISPs' business practices far removed from the actual provision of licensed service.

Finally, the *Report and Order*'s analysis of Section 706 fails to satisfy even the minimum requirements of the Administrative Procedure Act, let alone show that the Rules comport with Section 706.[105] Indeed, the Rules are *flatly inconsistent* with Section 706: they will significantly

[102] *Report and Order* ¶ 371 (quoting 47 U.S.C. § 303(b)).

[103] *See* CTIA Comments at 72.

[104] *See Report and Order* ¶ 371.

[105] *See Ass'n of Private Sector Colleges & Univs. v. Duncan*, 681 F.3d 427, 441 (D.C. Cir. 2012) (discussing requirement that agencies respond to significant comments).

inhibit the deployment of network infrastructure by increasing compliance costs for ISPs while simultaneously depriving ISPs from developing new business models, and these effects are likely to be especially pronounced for mobile ISPs,[106] an argument which the *Report and Order* ignores entirely. Rather than address CTIA's arguments, the Commission merely recites that the Rules are "flexible" and "largely consistent" with the FTC's regime,[107] ignoring critical differences between the Commission's and the FTC's choice regimes, including with respect to first-party marketing and the usage of web browsing and app usage information, for example.

Moreover, Section 706 does not provide a legal basis for the Rules even under the Commission's preferred theory, because the Commission fails to cite to any evidence, other than vague assertions by commenters, that the Rules are tailored to promote the acceleration of broadband adoption.[108] CTIA demonstrated the methodological flaws animating these comments.[109] And even if privacy concerns did drive demand for broadband, which they do not, the Rules do nothing to restrict the privacy practices of large edge providers that have comprehensive tracking capabilities that exceed those of ISPs, as well as specific edge providers that more directly implicate privacy—*e.g.*, online banking platforms, health websites, and so forth.[110] And even if the *Report and Order* cited methodologically valid evidence (which it does not), and did not ignore greater threats to privacy in the online ecosystem (which it does), the *Report and Order* still would fail to trigger Section 706, because ISPs' investments in infrastructure are more directly the object of Section 706 than are the attenuated privacy effects

[106] *See* CTIA Comments at 66-67.
[107] *See Report and Order* ¶ 372.
[108] *Id.* ¶ 373.
[109] *See* CTIA Reply Comments at 31-32; CTIA Comments at 125-26.
[110] *See* CTIA Reply Comments at 32; CTIA Comments at 69-70.

on demand for broadband on which the Commission relies.[111] As Commissioner Pai has noted, the Commission has invoked Section 706 in support of policies intended to address secondary, indirect effects on broadband demand, and the result consistently has been to inhibit investment in broadband deployment;[112] the *Report and Order* is more of the same.

VII. CONCLUSION.

CTIA members understand the critical importance of protecting the privacy and security of consumers' personal information, and they have developed and implemented robust data security programs to do so. While CTIA members are committed to safeguarding their customers' data, and are required to do so under existing federal and state laws, the Rules adopted in the *Report and Order* must be reconsidered. The Commission does not have authority to regulate the data privacy and security practices of broadband providers, and even if it did, its authority would be limited to regulating ISPs' use and disclosure of CPNI. Moreover, the Rules the Commission issued suffer from constitutional and other legal and policy infirmities that compel the Commission to reconsider and vacate or modify the Rules, as outlined above. However, if there are any aspects of the Rules that *remain*, CTIA supports the Commission's decision to harmonize the broadband rules with the voice rules.

[111] *See* CTIA Reply Comments at 32; CTIA Comments at 66-67. CTIA presented each of these arguments during the rulemaking; the *Report and Order* fails to address any of them. *See Report and Order* ¶ 373.

[112] *See 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, 781 (2016) (Commissioner Pai, concurring) ("Indeed, the Administration has overseen the first-ever reduction in year-over-year investment by major broadband providers that happened outside a recession—and it occurred in the months following the FCC's rubber-stamp of President Obama's plan to regulate the Internet.").

Respectfully submitted,

/s/ Thomas C. Power

Thomas C. Power
Senior Vice President and General Counsel

Maria Kirby
Assistant Vice President, Regulatory Affairs
and Associate General Counsel

Scott K. Bergmann
Vice President, Regulatory Affairs

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

January 3, 2017