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

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

PETITION FOR RECONSIDERATION OF NCTA - THE INTERNET & TELEVISION ASSOCIATION

Rick Chessen
Loretta Polk
Jennifer K. McKee
NCTA - The Internet & Television Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431

Christopher J. Harvie
Ari Z. Moskowitz
Mintz, Levin, Cohn, Ferris, Glovsky & Popeo, P.C.
701 Pennsylvania Avenue, N.W.
Suite 900
Washington, D.C. 20004-2608

January 3, 2017

TABLE OF CONTENTS

SUMMARY i

INTRODUCTION 1

I. THE BROADBAND PRIVACY RULES EXCEED THE SCOPE OF THE FCC's AUTHORITY 4

A. Section 222 Does Not Empower the Commission to Adopt Broadband Privacy Rules 4

B. Section 222(a) Does Not Authorize the Commission to Regulate ISP Use and Sharing of PII 6

C. IP Addresses and Other Device Identifiers Cannot be Classified as CPNI or PII Subject to the Constraints of Section 222 9

D. The Commission Lacks Authority under Section 222 to Regulate ISPs' Use and Sharing of the Content of Customer Communications 11

II. THE *ORDER* VIOLATES THE LONG-STANDING AND EFFECTIVE PRINCIPLES OF COMPETITIVE AND TECHNOLOGICAL NEUTRALITY BY UNJUSTIFIABLY SUBJECTING ISPs TO MORE STRINGENT PRIVACY RESTRICTIONS THAN OTHER INTERNET ENTITIES 12

A. The Commission Disregarded Substantial Record Evidence Demonstrating that Stricter Privacy Constraints on ISPs are Unwarranted 13

B. The Order Discards the Uniform Set of Online Privacy Obligations Established Under the FTC Framework without Any Showing of Consumer Harm from that Approach 16

C. The Order Fails to Identify Tangible Benefits that Outweigh the Rules' Considerable Costs to Competition, Innovation, and Consumer Welfare 19

III. THE RELIEF SOUGHT HERE WOULD AVOID THE CONSTITUTIONAL INFIRMITIES OF THE RULES 21

IV. THE DATA BREACH AND DATA SECURITY RULES ARE FLAWED AND SHOULD BE RECONSIDERED 23

CONCLUSION 25

SUMMARY

The Commission should reconsider and withdraw its *Order* adopting privacy and data security rules applicable to providers of broadband Internet access service (BIAS). The rules adopted in the *Order* are unsustainable for at least four reasons.

First, they exceed the scope of the Commission's authority under Section 222 of the Communications Act. Section 222 was designed to apply only to voice telephony services. The *Order* disregards arguments rooted in the language, legislative history, and structure of the Act demonstrating that Congress never intended for Section 222 to apply to Internet access service. The Commission's reliance on Section 222(a) as a source of authority for regulating use and sharing of the personally identifiable information (PII) of broadband customers is likewise unfounded. When Congress acts in the Communications Act to regulate PII, it does so explicitly. Section 222 is aimed at regulating a very specific, narrow set of data – call record information of voice telephony customers – and the language and structure of the Act demonstrate that Congress deliberately chose not to regulate PII under that provision. The *Order's* treatment of IP addresses and device identifiers, as well as its regulation of the content of broadband customer communications, are likewise unlawful exercises of authority under Section 222.

Second, the rules adopted in the *Order* arbitrarily and capriciously depart from the Federal Trade Commission's (FTC) long-standing and effective privacy framework applicable across the Internet (including to ISPs, which the FTC had vigorously studied before adopting its rules), establishing instead an asymmetric privacy regime that will harm consumers, competition, and innovation. Disregarding substantial record evidence showing that ISPs do not have more visibility into broadband customers' data than other Internet entities, the *Order* unjustifiably treats ISPs far more stringently than others with similar – or even greater – access to such data. The disparate framework imposed by the Commission reduces consumer welfare by depriving

ISPs of the same opportunity to provide their customers with data-driven services and capabilities as other Internet entities while also stifling their ability to provide much-needed competition in the highly concentrated online advertising market. It will confuse consumers by having two markedly different choice mechanisms for the same data sets, while failing to materially improve consumer privacy, since all non-ISPs coming into contact with this data will be subject to less stringent use and disclosure restrictions.

Third, the rules infringe on the protected speech of ISPs in a manner that cannot pass muster under the First Amendment. The *Order* establishes speaker-based distinctions that govern the manner in which similarly-situated companies competing in the Internet ecosystem may use and share the same set of information, which typically triggers heightened constitutional scrutiny. Even if analyzed under intermediate scrutiny, the rules would still fail since the Commission never adequately justifies its radical departures from the less restrictive and demonstrably effective FTC privacy framework.

Fourth, the *Order* establishes unworkable and conflicting data breach and data security requirements that will lead to over-notification to law enforcement and consumers of putative data breaches that do not actually cause harm as well as require ISPs to take measures to secure an impermissibly broad swath of non-sensitive data.

The broadband privacy *Order* is founded upon, and compounds the errors associated with, the ill-advised decision to reclassify BIAS as a telecommunications service. The pending appeal of Title II reclassification, coupled with the Commission's likely re-examination of that decision, further support the relief requested here, which is aimed at restoring the consistent application of the bedrock principles of transparency, choice, and security across the Internet.

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

NCTA - The Internet & Television Association (NCTA), pursuant to Section 1.429 of the Commission's rules, respectfully submits this Petition for Reconsideration of the Report and Order released November 2, 2016 in the above-captioned proceeding.[1/]

INTRODUCTION

NCTA hereby requests that the Commission reconsider and withdraw the broadband privacy rules adopted on October 27, 2016. Triggered by the ill-conceived decision to reclassify broadband Internet access service (BIAS) as a Title II offering, and based on an incorrect reading of Section 222 of the Communications Act, the new broadband privacy rules are untenable as a matter of both law and policy.

Congress did not authorize the Commission to regulate the privacy practices of Internet service providers (ISPs) when it adopted the protections for customer proprietary network information (CPNI) set forth in Section 222 of the Communications Act. Nor did Congress empower the Commission to regulate the personally identifiable information (PII) collected and used by providers, or to restrict the use and sharing of device identifiers such as IP addresses.

[1/] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* Report and Order, FCC 16-148 (rel. Nov. 2, 2016) ("*Order*"). A summary of the *Order* and rules adopted therein was published in the Federal Register on December 2, 2016. *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* 81 Fed. Reg. 87,274 (Dec. 2, 2016) (amending 47 C.F.R. § 64.2001 et seq.).

But even if the Commission did possess authority under Section 222 to adopt broadband privacy rules, the *Order* should still be rescinded. As the Federal Trade Commission (FTC) and the Administration have previously – and correctly – concluded, broadband consumers should receive consistent protection of their personal data from all entities in the online ecosystem.[2/] Instead of meeting that goal, the *Order* ignores substantial record evidence and unjustifiably departs from the well-established and effective FTC framework applicable to the rest of the Internet in several key respects.

The regulatory imbalance enshrined into law by the *Order* is thus not only arbitrary, capricious, and contrary to law, it will reduce consumer welfare, inhibit competition, and stifle innovation.[3/] And this asymmetric framework will generate consumer confusion, while doing nothing to enhance the overall privacy of broadband consumer data. The same data the *Order* constrains ISPs from using will continue to be routinely accessed and used by all other Internet entities operating under a different set of standards and requirements. In light of the FTC framework's success in protecting consumer privacy and promoting innovation, the Commission's obligation to engage in reasoned decision-making under the Administrative Procedure Act (APA) required at least that the costs associated with the proposed departures from that framework be weighed against their purported benefits.[4/] The lack of any such analysis in the *Order*, by itself, warrants reconsideration of the rules.[5/]

[2/] Dissenting Statement of Commissioner Ajit Pai at 3 ("Commissioner Pai Dissent")("[A]s everyone acknowledges, consumers have a uniform expectation of privacy.").

[3/] *See infra* at Section II. *See also* Oracle Corporation, Petition for Reconsideration, WC Docket No. 16-106, Dec. 21, 2016 ("Oracle Petition for Reconsideration"), at 2 ("ISP-specific privacy rules that depart from the privacy approach of the [FTC] . . . will hurt competition" and cause "corresponding harm to consumers.").

[4/] *See Motor Vehicle Mfrs. Ass'n of the U.S. v. State Farm Mutual Auto Ins. Co.*, 463 U.S. 29 (1983).

[5/] NCTA's request for reconsideration covers only the adoption of rules applicable to providers of BIAS. NCTA does not object to – or seek reconsideration of – the adoption of new rules to the extent they replace or update the existing CPNI rules applicable to voice services. The Commission correctly concluded that the voice

The rules adopted in the *Order* are predicated upon the still unsettled issue of the legal validity of the Commission's decision to reclassify BIAS as a telecommunications service, which is currently pending before the D.C. Circuit Court of Appeals.[6/] Commissioners Pai and O'Rielly recently announced their intention to "revisit . . . the Title II Net Neutrality proceeding more broadly, as soon as possible,"[7/] which also militates in favor of granting the instant petition. The relief requested here would, at a minimum, permit the Commission to defer the operative effect of the broadband privacy rules until the issue of BIAS reclassification is definitively resolved. It is not in the public interest to compel ISPs to initiate the process of complying with the arbitrary and unconstitutional broadband privacy rules, especially given that the tenuous legal predicate for their adoption will be revisited and likely revised. Revisiting the decision to reclassify BIAS as a Title II service would benefit consumers by restoring the applicability of the FTC's long-standing and effective privacy framework to broadband service.

The relief requested here will not leave broadband consumers unprotected. As the Commission itself has recognized, the "importance of privacy protection is certainly not new to the nation's largest broadband providers, all of which have publicly available privacy policies, describing their use and sharing of confidential customer information."[8/] ISPs have strong incentives to earn and maintain their customers' loyalty by protecting their data, and considerable experience in safeguarding customer data. And record evidence shows that ISPs have been subject to fewer FTC privacy enforcement actions than non-ISPs and that consumers

---

rules have outlived their usefulness. *See Order,* ¶ 3 (noting that revisions "bring[] privacy protections for voice telephony and other telecommunications services into the modern framework").

6/ *See* Joint Petition for Rehearing en banc of Petitioners National Cable & Telecommunications Association and American Cable Association, *United States Telecom Ass'n v. FCC*, No. 15-1063 (D.C. Cir. July 29, 2016).

7/ Letter from Commissioners Ajit Pai and Michael O'Rielly, to Meredith Atwell Baker, et. al. (Dec. 19, 2016), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1219/DOC-342677A1.pdf.

8/ *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* Notice of Proposed Rulemaking, WC Docket No. 16-106, FCC 16-39 (rel. April 1, 2016) ("NPRM"), at ¶ 10.

trust ISPs more than many other entities that collect their online data.[9/] ISPs' broadband privacy policies reflect the key principles of transparency, choice, and security that undergird the FTC's successful privacy framework that applied to all players in the Internet ecosystem until the FCC reclassified BIAS in the *Open Internet Order*. The relief requested here is aimed at preserving the continued primacy of those principles and their consistent application across the Internet.

I. THE BROADBAND PRIVACY RULES EXCEED THE SCOPE OF THE FCC's AUTHORITY

The rules adopted in the *Order* exceed the FCC's authority under Section 222. Congress enacted Section 222 to cover a specific and targeted data set (telephone customer call record information) readily accessible by a very limited number of entities (voice telephone service providers), but the *Order* attempts to rewrite the statute to accommodate an immensely broad data set (broadband customer data) accessible by millions of Internet entities.[10/] The Commission's interpretation strains Section 222 beyond its breaking point.

A. Section 222 Does Not Empower the Commission to Adopt Broadband Privacy Rules

The plain language, legislative history, and prior Commission constructions of Section 222 all confirm that the statute was intended to apply exclusively to voice telephony and functionally equivalent services.[11/] The *Order* does not seriously dispute that the statute was

---

9/ *See, e.g.,* Comcast Comments 37-38 and Appendix A.

10/ Dissenting Statement of Commissioner Michael O'Rielly ("Commissioner O'Rielly Dissent") at 1 ("Unlike traditional voice calls where the only parties that had access to call records were those already subject to section 222(c) – the local exchange carrier and in some instances the interexchange carrier – multiple parties that are unregulated by section 222 have access to an end user's online activities.").

11/ NCTA Comments at 7-13; CTIA Comments at 16-23; Comcast Comments at 66-68; Charter Reply Comments at 3-4.

designed to apply to telephone service,[12/] and that its extension to BIAS is thus solely a function of reclassification.[13/] While the *Order* avers that the term "telecommunications carrier" always has included entities other than voice telephony providers,[14/] it tellingly cites no instances of any such entity being subject to the CPNI rules in the first 20 years of administering the statute.[15/] The *Order* fails to reconcile its significant expansion of the scope of Section 222 with the myriad previous decisions and statements from the Commission that narrowly construed the statute in a telephone-centric manner.[16/]

The *Order* also never acknowledges that the need to jettison certain statutorily-defined terms – such as subscriber list information, telephone toll service, and telephone exchange service – as "categories that have no relevance for BIAS" itself raises substantial doubts as to whether BIAS was intended to be covered by the statute.[17/] Instead, the Commission erroneously

---

12/ *See e.g. Order*, ¶ 336 ("Some of [Section 222's] more-specific duties concerning CPNI are indeed relevant only in the context of voice telephony"); *id.* at ¶ 339 ("Section 222 includes provisions to address . . . telephone-specific concerns").

13/ Notwithstanding the *Order's* protestations to the contrary, *Order*, ¶ 335, that is an archetypal example of an agency's use of definitional authority to expand the reach of a statute beyond what Congress intended. NCTA Comments at 13; Comcast Comments at 67-68.

14/ *Order*, ¶ 335.

15/ Notably, the NPRM specifically referenced the years in which digital subscriber line (DSL) Internet access service was regulated as a Title II service, NPRM, ¶ 11, and hence was furnished by a "telecommunications carrier." But the Commission fails to show that DSL was ever actually subject to the CPNI rules. To the contrary, not until six years after enactment of Section 222 – and well after DSL had become a popular, mass market service – did the Commission even ask (but never resolve) whether Section 222 could be applied to DSL providers. *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information,* Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860, ¶ 146 (2002). Indeed, when the Commission reclassified wireline broadband service, including DSL, as an information service in 2005, it asked whether it should adopt CPNI-like privacy rules under Title I, without ever suggesting that DSL subscribers were losing privacy protections previously enjoyed under Title II, *Appropriate Framework for Broadband Access to the Internet over Wireline Facilities*, 20 FCC Rcd 14853, ¶ 12 (2005), thereby further belying the *Order's* claim that the statute must be reflexively applied to any service furnished by an entity classified as a "telecommunications carrier."

16/ Commissioner O'Rielly Dissent at 2 (highlighting "the limited purpose of section 222" and noting that it "was never intended to cover all information about a person. It defines and protects a specific set of call record information, and until just recently, that has been the Commission's interpretation as well"). *See also* NCTA Comments at 9-10.

17/ *See Order*, ¶ 336; NCTA Comments at 11.

concludes that simply by re-labelling ISPs as "telecommunications carriers," it is free to apply Section 222 to a service that the structure and legislative history demonstrate is clearly beyond the scope intended to be covered by Congress.[18/] In drafting the 1996 Act, Congress knew how to impose obligations on providers of Internet services, and it did so explicitly in Section 230, which was enacted contemporaneously with Section 222.[19/] The Commission tries to dismiss this argument by citing the disposition of a challenge to reclassification based on Section 230 in *U.S. Telecom Ass'n v. FCC*.[20/] But the fact that Section 230 did not itself classify Internet access service is immaterial. Section 230 demonstrates that Congress knew how to address Internet services in the 1996 Telecommunications Act and deliberately chose not to do so in Section 222. Because the Commission cannot override that choice, the rules should be withdrawn.[21/]

B. Section 222(a) Does Not Authorize the Commission to Regulate ISP Use and Sharing of PII

The *Order* found authority to regulate PII under Section 222(a) only by ignoring arguments raised in the proceeding demonstrating that neither the plain language of that provision nor the structure of the statute as a whole can support such a conclusion. Congress knows how to impose regulations on use and disclosure of PII in the Communications Act,

---

18/ *See*, *e.g.*, *Public Citizen v. Department of Justice,* 491 U.S. 440, 454 (1989) ("Looking beyond the naked text for guidance is perfectly proper when the result it apparently decrees… seems inconsistent with Congress' intention."); *Dorris v. Absher,* 179 F.3d 420, 429 (6th Cir. 1999)(where "literal interpretation" of statutory language "would lead to… an interpretation inconsistent with the intent of Congress," courts must "look beyond the language of the statute").

19/ CTIA Comments at 17; NCTA Comments at 9, n.14; Comcast Comments at 67-68.

20/ *Order*, ¶ 335.

21/ The lack of authority in Section 222 for the rules adopted in the *Order* vitiates any claim that they could be grounded in Sections 201, 202 or any other provision of the Act. NCTA Comments at 25; CTIA Comments at 60-63; AT&T Comments at 108-109; USTelecom Comments at 31-32. *See also* Commissioner O'Rielly Dissent at 3 ("By specifically enacting section 222, Congress made clear that the authority to regulate privacy is found in that provision."); *Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934,* Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, ¶ 153 (1999) ("[T]he specific consumer privacy and consumer choice protections established in section 222 supersede the general protections identified in sections 201(b) and 202(a).").

having done so in the Cable and Satellite Privacy Acts in Sections 631 and 338 – yet it did not do so here.[22/] If, as the *Order* claims, the protection of PII is "at the heart of most privacy regimes,"[23/] it is telling that Congress chose not to use the term PII anywhere in Section 222.

Forgoing any analysis of these prior Congressional determinations and specific statutory references to PII, the Commission simply asserts "today that" such information "is PII" under Section 222.[24/] But the statute bars such a determination. Section 222 specifically defines a customers' name, address, and telephone number "as used in this section"[25/] as "subscriber list information," which is excluded from the privacy protections applied to CPNI.[26/] The *Order* never addresses the argument that because subsection (h) clearly defines name, address, and telephone number information as "subscriber list information" for purposes of Section 222, the Commission cannot then use subsection (a) to redefine these categories as PII.[27/] Instead, the *Order* maintains that Congress employed the oblique route of authorizing regulation of PII under Section 222 via a single reference to a different term (proprietary information), while also classifying the most basic elements of PII – name, address and telephone number – as something else entirely (subscriber list information) for purposes of construing Section 222. Even putting aside the statutory definition of subscriber list information, the *Order* fails to explain, let alone distinguish, the fact that the Commission "previously found that names, addresses, and telephone numbers are not CPNI, *even when not published as subscriber list information*."[28/] The *Order's*

22/ NCTA Comments at 14-15.

23/ *Order*, ¶ 88.

24/ *See id*.

25/ 47 U.S.C. § 222(h)(emphasis added).

26/ 47 U.S.C. § 222(h)(1), (3).

27/ *See* NCTA Comments at 15.

28/ *Order*, ¶ 99 (emphasis added).

conclusory assertion to the contrary is simply untenable, in light of this clear precedent and Congress' direct use of the term PII elsewhere in the Communications Act.[29/]

The *Order* also fails to refute arguments that Congress could not have intended Section 222(a) to serve as a substantive constraint on use or disclosure of PII because the structure of the statute – in particular, the exceptions to the constraints on use and disclosure of protected data – presupposes that Section 222(a) does not restrict use or disclosure of any data at all. Section 222(e) imposes an affirmative duty on carriers to enable third-party directory providers to publish subscriber list information, which includes names, addresses, and phone numbers, "notwithstanding subsections (b), (c), and (d)."[30/] If name, address, and telephone number information were protected as confidential proprietary information under (a), then effectuating the publication directive in subsection (e) would have required Congress to include (a) in subsection (e)'s "notwithstanding" clause. Congress declined to take such a step, however, reinforcing the conclusion that Section 222(a) was not intended to be read as imposing substantive safeguards on the use and disclosure of any information.

The *Order* unsuccessfully seeks to avoid this conclusion by asserting that there was no need to include subsection (a) in the "notwithstanding" clause in (e) because subsection (a) only protects confidential information and subscriber list information "by definition is published and therefore is not confidential."[31/] This argument only highlights the internal contradictions of the Commission's tortured logic. The Commission cannot, as it does, assert in one part of the *Order* that customer proprietary information (CPI) under Section 222(a) consists of information that "should not be exposed widely to the public," while maintaining elsewhere that Section 222(a)

29/ *See, e.g.*, Verizon Comments at 58-59; NCTA Comments at 15.

30/ 47 U.S.C. § 222(e); NCTA Comments at 16.

31/ *Order*, ¶ 351.

does not in any manner restrict wide publication of the name, address and telephone number information that it seeks to classify as CPI.[32/] While validating Commissioner O'Rielly's observation that the *Order* "at times… runs circles around itself," rules grounded in such a circular and self-contradictory reading of their statutory foundation are simply unsustainable.[33/]

C. IP Addresses and Other Device Identifiers Cannot be Classified as CPNI or PII Subject to the Constraints of Section 222

In defining IP addresses and other identifiers as CPNI, the *Order* both contradicts itself and fails to adequately address questions raised in the record about how such information can be defined as CPNI and subject to the restrictions of Section 222(c). IP addresses and similar identifiers cannot be classified as CPNI subject to the constraints of Section 222 because they are not (1) provided by the customer to the carrier, (2) proprietary, or (3) individually identifiable.

The statute defines CPNI as "information… that is made available *to* the carrier *by* the customer."[34/] IP addresses, however, are assigned *by* the carrier *to* the customer and hence cannot fall within that definition.[35/] The *Order* states this reading of the text should be discarded because it "undermines the privacy protective purpose of the statute,"[36/] but such faulty reasoning would effectively nullify the import of *any* statutory text the Commission views as conflicting with its policy objectives. The *Order* goes on to note that "but for the carrier-customer relationship, the customer would not have an IP address,"[37/] but this argument is equally true for all data generated in the course of that relationship, and hence would render

---

32/ *Compare Order*, ¶ 86 *with id.,* ¶ 351.

33/ Commissioner O'Rielly Dissent at 3.

34/ 47 U.S.C. § 222(h)(1)(A) (emphasis added). NCTA Comments at 21; Comcast Comments at 77; Letter from Loretta Polk, NCTA, to Marlene H. Dortch, Secretary, Federal Communications Commission, WC Docket No. 16-106 (Oct. 20, 2016) ("NCTA Ex Parte"), at 11-12.

35/ Charter Reply Comments at 26; Comcast Comments at 77; NCTA Comments at 21.

36/ *Order*, ¶ 70.

37/ *Id.*

meaningless the limiting principle that CPNI must be "made available to the carrier by the customer."[38/] The *Order* fares no better when it suggests that "IP addresses are roughly analogous to telephone numbers,"[39/] since Section 222 and FCC precedent expressly exclude phone numbers from the definition of CPNI.[40/]

Nor are IP addresses "proprietary."[41/] Rather, they are broadly available to a wide variety of entities in the Internet ecosystem.[42/] The *Order* merely asserts that "whether information is available to third parties does not affect whether it meets the statutory definition of CPNI."[43/] Yet just a few paragraphs later the *Order* "reaffirms" the opposite: that "it is clear that Congress used the term 'proprietary information' broadly to encompass all types of information that should not be exposed widely to the public."[44/]

The *Order* additionally suggests that an IP address "is ultimately just a proxy for the customer," but even supporters of the Commission's rules acknowledge that this is technically incorrect. As the Electronic Frontier Foundation pointed out, IP addresses, on their own, do not identify specific individuals.[45/] Instead they identify device endpoints that may be used by

---

38/ 47 U.S.C. § 222(h)(1)(A) (emphasis added).

39/ *Order*, ¶ 68.

40/ 47 U.S.C. §§ 222(h)(1)(B), (h)(3)(A). Comcast Comments at 80; NCTA Ex Parte at 12. Nor is the *Order* saved by its claim that "[t]he Commission has previously held telephone numbers dialed to be CPNI." *Order*, ¶ 68, n. 138. As noted in Comcast's comments, "While it may be true that telephone numbers dialed are considered CPNI, the customer's telephone number is not CPNI." Comcast Comments at 80, n. 212 *citing Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Information and Other Customer Information, Order,* 13 FCC Rcd 12390, ¶¶ 8-9 (1998).

41/ NCTA Comments at 21-23; Comcast Comments at 77-81.

42/ Comcast Comments at 81; CTIA Comments at 44; Richard Bennett Comments at 3.

43/ *Order*, ¶ 70.

44/ *Order*, ¶ 86.

45/ *Unreliable Informants: IP Addresses, Digital Tips and Police Raids*, ELECTRONIC FRONTIER FOUNDATION, at 6 (Sept. 2016), https://www.eff.org/files/2016/09/22/2016.09.20_final_formatted_ip_ address_white_paper. pdf ("[U]sing an IP address to identify a specific individual is problematic because there is nothing about the addresses themselves that make them personally identifiable"); *Why IP Addresses Alone Don't Identify Criminals*,

multiple individuals, or, in the case of IPv6 addresses, may denote hundreds or even thousands of endpoint devices that sit behind a local gateway.[46/] Thus, even if IP addresses could be considered CPNI, they would still not be subject to the use and sharing constraints of Section 222(c) because they are not individually identifiable.[47/] For similar reasons, IP addresses cannot, on their own, be considered PII – NIST and the FTC both take the position that IP addresses could be considered PII only when associated with other information that identifies an individual.[48/] Further, as NCTA noted in this proceeding, "Courts have consistently declined to hold that an IP address – *by itself* – can be classified as identifying information."[49/]

The *Order* suggests that when a provider assigns a static IP address and associates that IP address in its records with that customer, "it is difficult to portray that scenario as not involving PII."[50/] But that scenario shows only that an IP address, in combination with other customer data, *could* be identifiable in certain instances. That is a far cry from the *Order's* findings that an IP address "meets the statutory definition of CPNI" and should also be classified as PII – determinations that cannot stand up to analysis under Section 222 and hence should be rescinded.

D. The Commission Lacks Authority under Section 222 to Regulate ISPs' Use and Sharing of the Content of Customer Communications

The *Order* asserts authority to regulate the content of communications under Section 222 without citing any statutory basis for reaching that conclusion.[51/] To the contrary, the Commission concluded in previous proceedings that "call content information is not considered

---

ELECTRONIC FRONTIER FOUNDATION (Aug. 24, 2011), https://www.eff.org/deeplinks/2011/08/why-ip-addresses-alone-dont-identify-criminals ("[I]n many situations, an IP address isn't personally identifying at all.").

46/ NCTA Comments at 23.

47/ *See e.g.,* NCTA Ex Parte at 8-12.

48/ NCTA Ex Parte at 8-10.

49/ *Id.* at 10-11, nn. 34-37.

50/ *Order*, ¶ 115.

51/ *Order*, ¶ 104.

CPNI,"[52/] and never revisited those rulings. The *Order*, however, asserts that Section 222 establishes "a framework for protecting the content carried by telecommunications carriers," without discussing or referencing its prior contrary findings.[53/] While the *Order* cites other statutes signaling Congressional intent to protect content, none fall within Title II of the Communications Act.[54/] If anything, these statutes demonstrate that when Congress seeks to regulate content, it does so expressly and deliberately – and chose not to do so in Section 222.[55/] The rules adopted in the *Order* must be withdrawn because they exceed the FCC's authority.

II. THE *ORDER* VIOLATES THE LONG-STANDING AND EFFECTIVE PRINCIPLES OF COMPETITIVE AND TECHNOLOGICAL NEUTRALITY BY UNJUSTIFIABLY SUBJECTING ISPs TO MORE STRINGENT PRIVACY RESTRICTIONS THAN OTHER INTERNET ENTITIES

Even assuming *arguendo* that the Commission possesses the authority to adopt broadband privacy rules, withdrawal of the rules set forth in the *Order* is still necessary. The asymmetric rules adopted in the *Order* are arbitrary and capricious because they are unnecessary, unjustified, unmoored from a cost-benefit assessment, and unlikely to advance the Commission's stated goal of enhancing consumer privacy. Rather, they are likely to harm consumers, competition, and innovation.[56/]

52/ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Networking Information and Other Customer Information*, Notice of Proposed Rulemaking, 11 FCC Rcd 12513, ¶ 47 (1996) (emphasis added). *See also Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Networking Information; Use of Data Regarding Alarm Monitoring Service Providers*, 11 FCC Rcd 9553, n. 18 (1996) ("Ameritech concurs with our conclusion that call content information does not constitute CPNI.").

53/ *Order*, ¶ 104.

54/ *Id.* at n. 261.

55/ The *Order* also expressly disclaims that it is basing its authority to regulate content on Section 705 of the Act, stating that Section 222 is a source of authority to regulate content independent of Section 705. *Order*, ¶¶ 104-105. Nor could the Commission have relied on Section 705 for its restrictive content regulations in any case. *See* NCTA Comments at 26-27, CTIA Comments at 63-64; TechFreedom Comments at 24-32.

56/ Dissenting Statement of Commissioner Ajit Pai at 3 ("[The Commission] has adopted one-sided rules that will cement edge providers' dominance in the online advertising market and lead to consumer confusion about which companies can and cannot use their data.").

A. The Commission Disregarded Substantial Record Evidence Demonstrating that Stricter Privacy Constraints on ISPs are Unwarranted

The *Order* erroneously finds that ISPs are uniquely positioned with respect to access to online customer data, and that finding underpins its imposition of more stringent restrictions on ISPs than on edge providers. The *Order*'s findings were thoroughly debunked in a comprehensive study by Professor Peter Swire examining Internet functionality and the flow of broadband consumer data over the network.[57/] Highlighting the fact that consumers access the Internet via multiple devices and ISPs throughout the day, the exponential growth of encryption, and the prevalence of virtual private networks (VPNs), Professor Swire concludes that "based on a factual analysis of today's Internet ecosystem in the United States, ISPs have neither comprehensive nor unique access to information about users' online activity."[58/] Due to those developments, each ISP today has less visibility over broadband consumer data than in 2012 when the FTC concluded – after extensive research and analysis – that a technology-neutral framework to online privacy regulation is the best approach for ISPs and non-ISPs alike.[59/] Further, Professor Swire found that due to their unique insights into user activity and dominance in cross-context and cross-device tracking, "non-ISPs often have access to more and a wider range of user information than ISPs."[60/]

Rather than grapple seriously with the findings of the Swire study, which were strongly affirmed by a broad cross-section of commenters,[61/] the *Order* simply asserts that "edge

---

57/ Peter Swire, Justin Hemmings, Alana Kirkland, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, The Institute for Information Security & Privacy at Georgia Tech (May 2016) (submitted in Docket No. WC 16-106) ("Swire Paper").

58/ *Id.* at 4.

59/ *See* Comcast Comments at 26-27.

60/ Swire Paper at 4.

61/ *See e.g.* Charter Reply Comments at 16-17; International Center for Law & Economics Comments at 9, Appendix A; Internet Commerce Coalition Comments at 9-10; American Commitment Comments at 2; ACLP

providers only see a slice of any given consumer's Internet traffic."[62/] But the record is replete with evidence, showing that large edge providers have as much – if not more – insight into broadband customer activity than ISPs.[63/] For example, empirical research showing that Google tracking technology is present on 92 percent of the top 100 websites – and on 8 out of every 10 of the top 1 million websites – was simply ignored without explanation in favor of material more supportive of the Commission majority's pre-ordained view on the relative scope of ISP and edge provider visibility over broadband consumer data.[64/]

Likewise, the *Order* downplays the significance of encryption on ISP visibility, and ignores the fact that the visibility advantages wielded by large edge providers widen as more network traffic is encrypted.[65/] No commenter seriously disputed the general trend in the marketplace toward greater use of encryption and greater reliance on VPNs, which, at a minimum, raises serious questions about the durability of the rationale for the asymmetric framework adopted in the *Order*. Even privacy advocates inclined to support the Commission

---

Comments at 14; ITIF Comments at 5; Professor Christopher Yoo Comments at 4; Richard Bennett Comments at 5; EPIC Comments at 15-16; Consumers' Research at 7; Citizens Against Government Waste Reply Comments at 3; Multicultural Media, Telecom and Internet Council, et al. (MMTC), Comments at 6-7; Communications Workers of America Comments at 5-8; Electronic Transactions Association Comments at 6-7.

62/ *Order*, ¶ 30. *But see* Oracle Petition for Reconsideration at 4 ("[T]he *Order's* flawed assertions about the internet ecosystem neglect at least two key consumer information-harvesting edge providers services that substantially alter the privacy landscape: operating systems and web browsers. . . .These services offer their providers as much, or likely more, access to information such as web browsing history compared to [ISPs].").

63/ NCTA Reply Comments at 21-23 (compiling record evidence regarding edge provider visibility over broadband consumer data); Comcast Reply Comments at 34-37 (same). *See also* Memorandum, *FCC Communications Privacy Rulemaking*, Electronic Privacy Information Center, 1 (Mar. 18, 2016), *available at* https://epic.org/privacy/consumer/EPIC-Draft-FCC-Privacy-Rules.pdf ("EPIC Memo") ("[M]any of the largest email, search, and social media companies exceed the scope and data collection activities of the ISPs"); Consumer Watchdog Comments at 3 ("As the Pew results demonstrate, it is not just [ISPs] that prompt people's privacy concerns. It is the entire Internet ecosystem.").

64/ *Compare, e.g.,* NCTA Comments at 49 and *Order*, ¶ 30. *See also* Oracle Petition for Reconsideration at 4, 7 ("The *Order* underestimates how Google combines and uses collected data to create full profiles of individuals. . . the Commission's failure to fully take into account the detailed record of Google's massive information-gathering capabilities is a disservice to consumers and must be corrected. That correction should begin by eliminating the asymmetrical treatment of ISPs that hamstrings them as competitors.").

65/ Richard Bennett Comments at 5 (When data is encrypted, however, "there is an enormous difference between the small pool of information available to ISPs and the much larger pool visible to web services.").

acknowledge that a finding that ISPs represent a more significant risk to online privacy than large edge providers constitutes a defective and inaccurate foundation for the new rules.[66/] And the Commission never addresses, let alone justifies, how its rules could depart so radically from the FTC's and Administration's technology-neutral approach, even though the FTC had expressly studied ISPs and other large platform providers in 2012 and concluded that the same privacy rules should apply to ISPs and non-ISPs alike.

The *Order* also wrongly concludes that ISPs occupy a unique gatekeeper role that justifies singularly restrictive limits on their ability to use customer data.[67/] The Commission majority reaches this conclusion without discussing the evidence in the record demonstrating that most consumers access the Internet via multiple devices and over multiple networks operated by multiple broadband providers.[68/] Indeed, the record shows that the competitive constraints on ISPs are more substantial than on large edge providers in several market segments – including search, social media, operating system platforms, browsers, and online advertising – which are more highly concentrated and subject to less burdensome restrictions on use and sharing of broadband consumer data.[69/] Switching between ISPs is no more difficult, inconvenient, or

---

66/ *See* EPIC Memo at 1-2 ("Agencies engaged in rulemaking actions have a duty to accurately frame the problem they seek to address. The current description of the problem presents ISPs as the most significant component of online communications that pose the greatest threat to consumer privacy. This description is inconsistent with the reality of the online communications ecosystem, incorrectly frames the scope of communications privacy issues facing Americans today, and is counterproductive to consumer privacy.").

67/ *Order*, ¶¶ 28, 30, 36.

68/ Swire Paper at 7 (Average Internet user has 6 connected devices, "many of which are mobile and connect from diverse and changing locations that are served by multiple ISPs"); EPIC Comments at 16 ("Internet users routinely shift from one ISP to another, as they move between home, office, mobile, and open WiFi services. However, all pathways lead to essentially one Internet search company and one social network company."); Comcast Comments at 27; Verizon Comments at 24.

69/ NCTA Reply Comments at 27-28 (compiling data in the record on concentration in search, online advertising, operating systems, and social networks). *See also* Comcast Reply Comments at 36; NCTA Comments at 52 (same); "Forget AT&T. The Real Monopolies are Google and Facebook," *New York Times*, December 13, 2016 ("Alphabet has an 83 percent share of the mobile search market in the United States and just under 63 percent of the US mobile phone operating systems market… In the first quarter of 2016, 85 cents of every new dollar spent in online advertising will go to Google or Facebook.").

costly than changing email providers, switching mobile operating systems, or moving to a new social network.[70/] Accordingly, the rules adopted in the *Order* should be withdrawn because they are founded upon erroneous conceptions of how the Internet functions and fallacious premises regarding ISPs' putative gatekeeper role and unique visibility over broadband data.

B. The Order Discards the Uniform Set of Online Privacy Obligations Established Under the FTC Framework without Any Showing of Consumer Harm from that Approach

The *Order* fails to proffer any evidence of harm to consumers – neither past, present, nor reasonably anticipated – arising from the technology-neutral approach to privacy protection employed for many years by the FTC.[71/] To the contrary, the record is rife with evidence regarding the success of the FTC framework at balancing the twin objectives of providing consumers control over their personal information while also preserving opportunities for companies to engage in beneficial uses of data that lead to innovation, new products and capabilities, and customized services.[72/] Indeed, the *Order* itself in several places lauds the FTC framework as a model of effective privacy protection.[73/] Conversely, it never identifies any instance in which ISP customers, prior to reclassification, suffered concrete harm from having their data protected under the FTC framework rather than under a more restrictive set of rules.[74/]

[70/] *See* NCTA Reply Comments at 27-28; AT&T Comments at 47; Comcast Comments at 38-42. *See also* Oracle Petition for Reconsideration at 7 ("The *Order* also attempts to draw a false distinction between consumers' choices and expectations with respect to their ISPs versus their edge providers and operating systems.").

[71/] Professor J. Howard Beales Comments at 2 ("[The NPRM] identifies no adverse consequences to consumers that have resulted from broadband provider privacy practices" under the FTC Framework.).

[72/] *See e.g.*, NCTA Comments at 39-41; Jon Leibowitz Comments at 1-4; Internet Commerce Coalition Comments at 5-6; Association of National Advertisers Comments at 12-13, 19-20.

[73/] *See e.g.*, *Order*, ¶¶ 4, 24, 107. *See also* Statement of Chairman Wheeler ("I want to thank the FTC… for leading the way with the FTC's privacy framework.").

[74/] As commenters noted, ISPs have a proven track record of protecting the privacy of their customers, and none of the 500 FTC privacy and data security enforcement actions referenced in the *Order* were brought against an ISP. *See* Comcast Comments at 37-38; NCTA Comments at 50-51.

While several commenters offered detailed guidance to the Commission on how it could adopt rules that mirror the FTC's approach,[75/] the *Order* adopts "rules that radically depart from the FTC framework."[76/] For example, the *Order* fails to justify the decision to regulate use and sharing of web browsing and app usage data by ISPs more stringently than use and sharing of such data by all other Internet entities. Consumers benefit from online advertising, individualized content, and product improvements based on browsing information, and those that wish to forego those benefits are free to opt-out of having their data used for such purposes under the FTC's approach.[77/] There is no evidence in the record of consumer harm arising from ISPs utilizing web browsing and app usage data subject to opt-out approval under the FTC framework, nor is there any rational basis for deeming such information sensitive when possessed by an ISP, but non-sensitive when possessed by any other Internet entity. The *Order* simply asserts that ISP use of web browsing and app usage data must be constrained more severely than prior to reclassification of BIAS.[78/]

The *Order* likewise fails to demonstrate why ISPs should be subject to stricter limits on their ability to use broadband customer data to market their other products and services than all other Internet entities. Making it harder for ISPs to apprise their customers of new services and capabilities would harm, rather than improve, consumers' broadband experience.[79/] There is no evidence of consumer dissatisfaction with the flexibility provided for first-party data uses under

---

75/ CTIA Comments at 4-5, Appx A; USTelecom Comments at 8-16; Verizon Comments at 7-16; AT&T Comments at 30-35; Professor J. Howard Beales Comments at 9-14; Future of Privacy Forum Comments at 26-33; ITIF Comments at 16-19; IMS Health Comments at 10-14; Leibowitz Comments at 3-13.

76/ Commissioner Pai Dissent at 2.

77/ Joshua D. Wright, *An Economic Analysis of the FCC's Proposed Regulation of Broadband Privacy*, at 17-18, 25-28; Professor J. Howard Beales Comments at 8.

78/ *See Order*, ¶¶ 181-85.

79/ *See e.g.,* Letter of October 20, 2016 from Jennifer Hightower, Senior Vice President and General Counsel, Cox Communications, to Marlene H. Dortch, Secretary, Federal Communications Commission, WC Docket No. 16-106, at 1-4; Charter Reply Comments at 7, 12-13; Comcast Reply Comments at 12-14.

the FTC framework and the White House Consumer Privacy Bill of Rights.[80/] The *Order* suggests that its treatment of ISP first-party marketing activity "is consistent with . . . FTC Staff comments,"[81/] but that is incorrect. The FTC Staff comments specifically noted that the restrictiveness of the Commission's approach to first-party marketing "does not reflect" consumer expectations because "consumers may prefer to hear about new innovative products offered by their BIAS providers."[82/]

Despite asserting that consumers have a different set of privacy expectations when their personal information is handled by ISPs rather than edge providers,[83/] the *Order* never offers any empirical data demonstrating this to be the case.[84/] In fact, several studies highlighted in the record show the exact opposite – namely, that consumers trust their ISPs to protect their data significantly more than many other entities in the Internet ecosystem.[85/] Moreover, a national survey conducted by Public Opinion Strategies and Peter D. Hart demonstrated that an overwhelming majority of consumers, 94 percent, believe that all companies collecting broadband customer data should be subject to the same set of privacy rules.[86/] The *Order*, however, does not discuss any of the studies or survey data that undermine the rationale for the disparate treatment embodied in the rules. Further, notwithstanding the objections of commenters, the *Order* never reconciles its decision to subject ISPs to more stringent privacy restrictions with the Commission's prior findings that the "continuing relationship" carriers have

---

80/ NCTA Reply Comments at 20.

81/ *Order*, ¶ 199.

82/ FTC Staff Comments at 22-23.

83/ *See Order*, ¶ 35.

84/ The Pew and NTIA studies cited by the Commission and supporters of the proposed rules address consumer expectations across the entire broadband ecosystem, but do not identify any issues unique to ISPs that would support the disparate treatment embodied in the proposed rules. *See Order*, ¶ 87.

85/ NCTA Comments at 51; Comcast Comments at 34-36.

86/ Progressive Policy Institute, Internet User Survey at 2.

with their customers reduces the risks of misuse of customer data compared to other entities that may have more ephemeral – and less direct – interactions with broadband consumers.[87/] Because the *Order* repudiated the technology-neutral privacy framework that governed broadband consumer data prior to reclassification and jettisoned key elements of the demonstrably effective FTC regime in favor of more stringent restrictions that consumers neither sought nor needed, the rules adopted therein should be withdrawn.

C. The Order Fails to Identify Tangible Benefits that Outweigh the Rules' Considerable Costs to Competition, Innovation, and Consumer Welfare

Given the FTC framework's successful track record and the value to both competition and consumer expectations of having a unified set of privacy obligations applicable to all Internet entities using online customer data, it was incumbent upon the Commission to weigh the costs and benefits of the new regulatory burdens for ISPs. The *Order*, however, fails to assess the potential adverse effects of departing from the FTC framework or consider whether the costs outweigh the purported benefits of the rules.

Apart from the substantial costs and burdens of conforming their customer data handling practices and protocols to the Commission's new constraints, the rules adopted in the *Order* clearly limit the ability of ISPs, relative to all other Internet entities, to develop and furnish data-driven services and capabilities for their customers. The rules also inhibit the ability of ISPs, relative to all other Internet entities, to inform their customers of new products, services, promotions, and incentives of interest to them.[88/] Thus, data-driven services and capabilities will

---

87/ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information,* Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860, at ¶¶ 37, 55 (2002).

88/ Comcast Reply Comments at 13-14.

become more costly for ISPs to develop and furnish, and adjunct and complementary services available to ISP customers will be more expensive to market and offer.

The asymmetric framework established by the Commission's rules also will hinder ISPs from entering the online advertising market, thereby stifling an opportunity to bring new competition into a market dominated today by two large edge providers.[89/] The aggregate effects of these costs and burdens will likely be higher prices to consumers, less investment and innovation by ISPs in data-driven services, reduced consumer awareness of new ISP products and discount offerings, and less competition in the market for online advertising.[90/] Moreover, the *Order* never explains how consumer welfare is enhanced by treating a broadband customer's web browsing and app usage data as sensitive and subject to strict and unreasonable opt-in usage constraints when passing through ISP servers, and then treating that same exact data more flexibly as non-sensitive milliseconds later when it leaves the ISP facilities and transits to and from the edge. The effect of this irrational disparity is to impose considerable new burdens on ISPs while offering little incremental privacy protection for consumers.

While highlighting the value of reducing consumer confusion,[91/] the *Order* never addresses the point that establishing two different choice standards applicable to the same type of broadband customer data will engender confusion.[92/] Consumers that decline to opt-in to ISP use of their data for marketing and advertising purposes may not understand why or how major search, social media, operating systems, and others can continue to use that data for the same

---

89/ Oracle Petition for Reconsideration at 3 ("These rules will create a chilling effect by giving 'a clear competitive advantage to edge providers' that already dominate the digital advertising market"); *See also supra* n. 69; Comcast Comments at 53-54 (explaining and documenting that the top-10 participants controlling over 70% of the online advertising market are edge providers).

90/ *See* NCTA Comments at 58-59; Comcast Reply Comments at 21-24.

91/ *See Order*, ¶¶ 4, 24, 107.

92/ *See* NCTA Reply Comments at 29-31; MMTC Comments at 3-7; NAACP, LULAC, et. al, at 2; Comcast Reply Comments at 10-12; Charter Reply Comments at 14-15.

purposes – and they may mistakenly hold the ISP accountable for that use. Likewise, other consumers may be frustrated or angry that, due to changes in the choice architecture for first-party marketing triggered by the rules, they were not alerted to promotional services or discounts their neighbors enjoy. By failing to consider the negative impact on investment, innovation, competition, and value, the *Order* offers no basis for concluding that the benefits of the new rules outweigh their costs and burdens. For these reasons as well, the rules should be withdrawn.

III. THE RELIEF SOUGHT HERE WOULD AVOID THE CONSTITUTIONAL INFIRMITIES OF THE RULES

The *Order's* unwarranted departure from the FTC's effective and technology-neutral framework violates the First Amendment. The rules adopted in the *Order* create speaker-based distinctions that are subject to heightened First Amendment scrutiny.[93/] Use or sharing of broadband customer web browsing and app usage data by ISPs requires opt-in consent, while all other Internet entities may use or disclose this very same information subject to opt-out consent. There is ample evidence in the record – and discussed above – that this speaker-based distinction will create material disparities in the respective abilities of ISPs and non-ISPs to offer and derive revenue from data-driven services and capabilities, due to significant variances between participation rates for a given data usage activity based upon whether an opt-in or opt-out choice is offered.[94/] Moreover, while non-ISPs are permitted to use broadband data to market other products and services they offer without seeking customer permission (*i.e.*, based on implied consent), under the Commission's regime ISPs will be the only Internet entities largely restricted

---

93/ *Sorrell v. IMS Health, Inc*., 564 U.S. 552, 570-71 (2011) (holding that the process of gathering and analyzing data in preparation for speech is protected by the First Amendment and noting that imposition of speaker-based rules "is sufficient to justify application of heightened scrutiny").

94/ Comcast Comments at 48-49; NCTA Comments at 79; International Center for Law and Economics Comments at 11-12; Thomas Lenard and Scott Wallsten, *An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking*, at 25-26 (submitted in Docket No. WC 16-106).

from doing so. As noted constitutional scholar Laurence Tribe concluded, these speaker-based disparities are impermissible under the First Amendment.[95/]

Notably, the *Order* never discusses the constitutional implications of its decision to treat similarly-situated speakers differently with respect to their use and disclosure of the same set of data. Instead, the Commission dismisses any suggestion that its rules implicate speaker-based constitutional harms, averring that criticism of a privacy regime for failing to "apply to all entities equally… would invalidate nearly every federal privacy law, considering the sectoral nature of our federal privacy laws."[96/] But the constitutional infirmity here is not that the Commission's rules fail to apply to all entities equally, it is that those rules result in the establishment of vastly different regulatory regimes applicable to entities competing in the same market sector and using the same set of customer data.

Even if evaluated under the intermediate scrutiny test for restrictions on commercial speech set forth in *Central Hudson*, the *Order* would still fail to pass constitutional muster**.** While generally invoking the importance of protecting privacy, the *Order* asserts no substantial government interest in regulating ISP use and disclosure of broadband customer data more strictly than other Internet entities with the same data.[97/] Further, as noted by many commenters, the rules fail to directly and materially advance the Commission's asserted government interest in protecting privacy because the rules are (1) under-inclusive in their disparate treatment of

---

[95/] Laurence H. Tribe and Jonathan S. Massey, *The Federal Communications Commission's Proposed Broadband Privacy Rules Would Violate The First Amendment*, at 23 (May 27, 2016) ("[T]he speaker specific nature of the FCC's proposal – the singling out of ISPs – raises separate concerns under First Amendment equal protection principles") ("Tribe Submission"); *Supplemental White Paper: A Response to Arguments That The Commission's Proposed Broadband Privacy Rules Would Be Consistent With The First Amendment*, at 2, 10 (Sept. 13, 2016) ("Tribe Supplement").

[96/] *Order*, ¶ 189.

[97/] *Order*, ¶¶ 376-381. *See also Sorrell*, 564 U.S. at 573; NCTA Reply Comments at 11-12; Tribe Submission at 16-24.

similarly situated entities and (2) over-inclusive in applying stringent privacy protections to data that is widely available to any Internet entity, such as IP addresses and MAC IDs.[98/]

The *Order* maintains that the rules advance the "government's interest in enabling customer[s] to avoid unwanted and unexpected use and disclosure of sensitive customer PI."[99/] But marketing based on Web browsing and app usage data is not unexpected by consumers – it is the model they are accustomed to with respect to Internet-based services and products. Moreover, for those consumers who do wish to "avoid unwanted and unexpected use" of their data, the availability of an opt-out mechanism fully accomplishes that objective – as it has for many years under the FTC privacy framework – in a less restrictive manner than the Commission's rules. Thus, the heightened restrictions on use of Web browsing and app usage data by ISPs, as well as the additional constraints on first-party marketing, are far more extensive than necessary to serve the government's asserted interest given the successful history of the less burdensome FTC framework.[100/]

IV. THE DATA BREACH AND DATA SECURITY RULES ARE FLAWED AND SHOULD BE RECONSIDERED

While the *Order* adopts a harm-based trigger to govern whether or not a breach requires notice to Federal authorities or consumers,[101/] the new rules negate the utility of that trigger by establishing a timeframe that starts at the discovery of the breach, not the determination regarding harm. Determining the likelihood of harm can be complex and time-consuming – particularly in light of the *Order's* expansive and abstract conception of harm – and making that determination often will require analysis that takes longer than the 7 days afforded to ISPs to

98/ Tribe Submission at 22-27; Tribe Supplement at 8; Comcast Comments at 94-99; NCTA Reply Comments at 11-12 ; CTIA Comments at 44-51.

99/ *Order*, ¶ 383.

100/ Tribe Submission at 33-38; NCTA Reply Comments at 12; Comcast at 91-94.

101/ *Order*, ¶¶ 263-274.

notify law enforcement under the rules.[102/] The timeframe adopted in the rules likely will operate to defeat any benefit gained from the harm-based notification trigger, resulting in over-notification to Federal authorities and heightening the likelihood of over-notification to consumers about breaches that may not ultimately result in any harm. Such an outcome does not benefit consumers or the Commission, as the *Order* itself recognizes.[103/]

The *Order*'s expansive definition of sensitive information also increases the risk of over-notification by presuming that a breach of sensitive data is harmful.[104/] While state data breach notification laws typically cover sensitive personal information, almost all apply an independent harm threshold without any such presumption of harm. In addition, the scope of harm capable of triggering a notification obligation is not limited to financial harm. It includes "physical and emotional harm," as well as reputational damage, personal embarrassment, or loss of control over the exposure of intimate personal details," while offering no guidance as to when such non-economic impacts rise to the level of harm that would trigger a notification requirement.[105/] The rules further diverge from existing state laws by eschewing an exception for encrypted information,[106/] or even a presumption that a breach of encrypted information is not harmful. The data breach rules should be reconsidered in order to more effectively balance the objectives of providing timely and accurate notification of breaches that do cause tangible harm, minimizing over-notification, and providing companies with adequate time to fully investigate a breach prior to notifying government officials and consumers.

102/ *See, e.g.*, Comcast Reply Comments at 17-18.

103/ *See Order*, ¶ 263 ("The record reflects various harms inherent in unnecessary notification, including notice fatigue, erosion of consumer confidence in the communications they receive from their provider, and compliance costs"). *See also* FTC Staff Comments at 32-33.

104/ *Order*, ¶ 267.

105/ *Order*, ¶ 266.

106/ See NCTA Comments at 92.

Lastly, the data security rules adopted in the *Order* also should be reconsidered. While the "reasonable measures" standard is appropriate, the scope of data subject to that standard is overbroad and in excess of the Commission's authority.[107/] Further, while the *Order* references the importance of consistent application of the "reasonable measures" standard across the Internet,[108/] there is no specific mechanism to ensure that the FCC interprets that test in the same manner as the FTC. To the contrary, the *Order* expresses its intention to look beyond the FTC's administration of that test and construe the "reasonable measures" standard in accordance with "implementation of data security requirements under HIPAA, GLBA, and other relevant statutory frameworks,"[109/] thereby heightening the risk of different interpretations. Accordingly, both the data breach and data security rules should be withdrawn.

CONCLUSION

For the foregoing reasons, the Commission should grant NCTA's petition for reconsideration and withdraw the rules adopted in the *Order*.

Respectfully submitted,

/s/ Rick Chessen

Rick Chessen
Loretta Polk
Jennifer K. McKee
NCTA – The Internet & Television Association
25 Massachusetts Avenue, N.W.
Suite 100
Washington, D.C. 20001-1431

Christopher J. Harvie
Ari Z. Moskowitz
Mintz, Levin, Cohn, Ferris Glovsky & Popeo, P.C.
701 Pennsylvania Avenue, N.W.
Suite 900
Washington, D.C. 20004-2608

January 3, 2017

107/ *See supra* at Section I. *See also* NCTA Comments at 87.

108/ *See Order*, ¶ 246.

109/ *Id.*, ¶ 250.