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	)	

COMMENTS OF THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

William A. Check, Ph. D
Senior Vice President
Matthew Tooley
Vice President of Broadband Technology
Science & Technology

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

Rick Chessen
Loretta P. Polk
Jennifer K. McKee
National Cable & Telecommunications
Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431

May 27, 2016

TABLE OF CONTENTS

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	)	

COMMENTS OF THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

The National Cable & Telecommunications Association ("*NCTA*")[1/] hereby submits its comments on the Notice of Proposed Rulemaking ("*Notice*" or "NPRM") in the above-captioned proceeding.[2/]

INTRODUCTION AND SUMMARY

Consumers' private personal information should receive consistent protection across the broadband ecosystem. The Commission could have accomplished that goal by harmonizing its proposed privacy framework for broadband Internet service providers (ISPs or "broadband service providers") with the longstanding Federal Trade Commission (FTC) framework that has successfully protected consumers for years and will continue to apply to all broadband entities other than ISPs. Instead, the Commission has proposed an asymmetric privacy framework that unlawfully and unfairly singles out ISPs for burdensome treatment. This regulatory imbalance will lead to significant consumer confusion, upset common and settled Internet practices, inhibit

---

1/ NCTA is the principal trade association for the U.S. cable industry, representing cable operators serving more than 80 percent of the nation's cable television households, more than 200 cable program networks, and others associated with the cable industry. The cable industry is the nation's largest provider of broadband service after investing over $245 billion since 1996 to build two-way interactive networks with fiber optic technology. Cable companies also provide state-of-the-art competitive voice service to approximately 30 million customers.

2/ *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).

competition, stifle innovation, and reduce consumer welfare. And it will do nothing to increase the privacy of consumer data, since the same data that ISPs will be constrained from using is accessible to and used by numerous other broadband entities subject to far less stringent restrictions.

The Commission's proposed privacy framework is legally unsustainable. First, the Commission lacks statutory authority to impose the proposed rules under Section 222 because that provision only applies to privacy in the telephony context. Second, even assuming that Section 222 does apply to broadband, it only applies to data that meets the narrow definition of "customer proprietary network information" (CPNI); it is not, as the Commission asserts, a general privacy statute that encompasses all forms of personally identifiable information. Third, Section 222 imposes restrictions on the use of CPNI only to the extent that it is "individually identifiable," a statutory directive misapplied by the Commission. Fourth, none of the "kitchen sink" statutory provisions cited by the Commission are sources of standalone authority and/or could not be exercised consistently with the constraints of Section 222.

In addition to being legally unsustainable, the proposed privacy framework would be reckless and unwise as a matter of policy. The proposed approach rejects the FTC's carefully-considered, flexible framework and instead imposes a set of one-sided prescriptive obligations that will make it difficult for ISPs to innovate, offer new services and new capabilities to consumers, and adapt to changing market conditions and technological developments. None of these outcomes are necessary. Nothing about the reclassification of broadband Internet access service compels the Commission to impose an entirely new regime that departs from the FTC's framework. The Internet has thrived under the FTC's technology-neutral, unified set of privacy obligations that, until now, has applied to ISPs and non-ISPs alike.

Key differences between the FTC framework and the Commission's proposed rules include:

- The FTC applies an opt-out approach to govern use of customer data in most instances, with opt-in reserved only for uses of the most sensitive consumer data (e.g., health and children's data). The Commission's proposed rules, by contrast, would make opt-in the default mechanism. By mandating opt-in for a range of data uses for which most consumers decline to exercise opt-out rights under the FTC Framework, the proposal unnecessarily restricts beneficial data uses that today are commonly permitted by most consumers.

- The FTC exempts de-identified data from the notice-and-approval permissions regime, thereby encouraging companies to take effective measures to reduce privacy risks by anonymizing customer data. The Commission proposal subjects a broader scope of data to the permissions regime – including data items that cannot on their own identify specific persons – and offers no exception for data de-identified at the account or customer level.

- The FTC treats a broader set of first-party practices as part of the context of the relationship with the customer. The Commission's proposed regime lists only a narrow set of uses where consent is implied, and the result will be to introduce considerable "friction" into the customer relationship and interfere with data flows in ways likely to disrupt current practices and annoy consumers.

- The FTC carefully examined the question of whether large platform providers, including major search engines and browser providers, as well as ISPs, should be subject to heightened restrictions and ultimately refrained from doing so. By contrast, the Commission's proposal asserts that ISPs alone have unique, comprehensive access to the Internet activity data of their customers, ignoring both academic research and statements from privacy advocates.

Adoption of the Commission's proposal risks transforming consumer broadband into a tedious, frustrating experience marred by frequent disruptions to solicit and obtain opt-in customer approval for a multitude of everyday practices that currently take place without interruption. For instance, under the Commission's proposal, commonplace and seamless acts that ISPs perform today – such as transmission or receipt of an email on an ISP account, engaging in Domain Name System (DNS) look-up for broadband service customers, or furnishing or authenticating an Internet-delivered product via a broadband service transmission – potentially would become subject to the Commission's permissions regime, and could therefore

necessitate soliciting and obtaining opt-in consent. It should not be necessary for ISPs to obtain approval to use IP addresses or other data elements to perform tasks and provide services requested by their customers – indeed, that recognition is the very essence of the FTC Framework's core principle of "context," – but the Commission's proposal fails to clearly accommodate basic functions routinely undertaken today by ISPs for their broadband customers.[3/] At this point, it is only possible to scratch the surface of the potential disruptions that could be engendered by the proposal in its current form, and it is inevitable that a wide range of common practices – and potential future innovations – will be inhibited or thwarted altogether.

It is clear, however, that consumer welfare will be harmed. The Commission's highly restrictive approach to first-party uses of data will make it much harder for ISPs to apprise their customers of products, services and offers of interest to them. The proposal also will make it more difficult for ISPs to use data analytics to improve their products and customer service, and will appreciably restrict their ability to provide relevant advertising to consumers. There is no evidence of consumer dissatisfaction with the manner in which first-party data uses were addressed under the FTC Framework or of consumer demand for privacy rule changes that would disproportionately burden ISPs' ability to enhance the quality of their service, improve their products, and provide advertising of greater interest to their customers. The default opt-in regime set forth in the Notice effectively would reduce consumer choice by unnecessarily encumbering ISPs' ability to provide consumers the same opportunities to benefit from data-driven, customized services and capabilities that they enjoy today.

[3/] Attached to these comments as an appendix is a paper prepared by two NCTA technologists setting forth several potential common use cases and broadband-related functionalities that potentially could be disrupted by the Commission's proposed rules. William A. Check & Matt Tooley, Technical Review of the Proposed CPNI Rules for Broadband, attached as Appendix A ("Technical Appendix").

Moreover, the proposed rules will lead to considerable consumer confusion. Broadband consumers will have one set of privacy rights when their data is handled by their ISP and then an entirely different set of rights when that same data is handled by everyone else in the broadband ecosystem. Consumers do not expect their basic privacy protections to vary based on the identity of the entity they are interacting with at any particular time. This confusion would heighten privacy and security risks for consumers, many of whom may mistakenly believe that the withholding of opt-in consent in one context restricts use of their data throughout the Internet.

In sum, the Commission's proposed privacy framework will harm consumers and reduce broadband investment, innovation and competition. Singling out ISPs for uniquely burdensome requirements will do nothing to increase consumer privacy but will only lead to increased confusion and higher broadband costs.

In addition to the unlawful and unwise privacy proposal, the Commission's proposed data security requirements are excessive, counterproductive, and inconsistent with existing Federal policy, including prior guidance and recommendations by the Commission. Rather than adhering to the FTC's approach of imposing only a general obligation to take reasonable measures to protect the security of customers' personal information – and afford companies the discretion to meet that obligation in the way that best suits their network architecture and business model – the Commission proposes highly prescriptive rules specifying the measures companies must take to secure their customers' data. Imposing prescriptive requirements deprives ISPs of the flexibility and adaptability required to address the constantly-changing threats to network security, and conflicts with both the Congressional preference for relying on voluntary mechanisms (particularly the NIST cybersecurity framework), and industry-driven best practices to secure networks embodied in Commission policy statements.

Similarly, the data breach framework proposed in the *Notice* is problematic, as it effectively imposes a strict liability regime with no harm threshold. The definition of "data breach" is overbroad, the 7-10 day reporting requirement is too inflexible, and the scope of data subject to the reporting obligation is overbroad and unnecessarily burdensome.

Rather than move forward with the prescriptive regime embodied in the *Notice*, the best option for consumers, competition, and innovation would be for the Commission to embrace the proposed industry framework.[4/] This comprehensive proposal reflects the flexible, standards-based, enforcement-oriented approach successfully applied to the entire broadband ecosystem by the FTC prior to reclassification. It is grounded in key principles such as transparency, respect for context, choice, and security, and enforced through case law. This approach effectively balances consumer choice over the use of personal information with the benefits of enabling the use of data in ways that foster innovation, competition, new services, and new capabilities.

Consumers expect and deserve to have their data governed by consistent privacy standards based upon the sensitivity of the information and the manner of its use, irrespective of which entity in the Internet ecosystem uses that data. To ensure parity throughout the Internet ecosystem, the proposed industry framework reflects the FTC's well-established deception and unfairness standard, in accordance with existing protections that consumers receive when engaging with other companies on the Internet. A consistent privacy framework also gives ISPs the necessary flexibility to adjust their privacy and data security practices to adapt to changing consumer needs and preferences, while preserving their ability to provide data-driven customized services in the same manner as all other Internet entities. In short, consumers and competition

4/ *See NPRM* at ¶¶ 280-82.

will benefit most from a reasonable, consistent framework based on the successful FTC model that has protected the privacy of broadband consumers for years.

I. THE COMMISSION LACKS THE LEGAL AUTHORITY TO ADOPT THE PROPOSED BROADBAND PRIVACY RULES

As set forth below, the Commission lacks the legal authority to establish the regime set forth in the *Notice*, because the statutory bases cited therein do not empower the Commission to proceed as proposed.

A. Congress Did Not Intend for Section 222 to Empower the Commission to Adopt a Broadband Privacy Regime

The plain language and legislative history of Section 222[5/] demonstrate that it was intended to address only telephone customer records and practices employed by providers of telephone service with respect to those records. Acknowledging that the rules adopted to implement Section 222 are not "well suited to broadband Internet access service," the Commission recognized that those regulations address "concerns that have been associated with voice service"[6/] and are "telephone-centric."[7/] In fact, Section 222 was written only with voice telephone service in mind, and the "telephone-centric" nature of the Commission's current rules reflects nothing more than the limits of the statute itself.

Congress's approach to address privacy in the communications sector is well-established in the Communications Act: it adopts specific provisions aimed at specific segments of that industry – cable, telephony, DBS. In 1984, Congress adopted the comprehensive privacy regime in Section 631 of the Communications Act designed to safeguard the privacy interests of cable

---

5/ 47 U.S.C. § 222.

6/ *Protecting and Promoting the Open Internet*, GN Docket No. 14-28, 30 FCC Rcd 5601, 5823-24, ¶ 467 (2015) ("*Open Internet Order*").

7/ Public Notice*, Enforcement Bureau Guidance: Broadband Providers Should Take Reasonable, Good Faith Steps To Protect Consumer Privacy*, DA 15-603 (rel. May 20, 2015).

television subscribers.[8/] In 1996, Congress adopted Section 222 to ensure protection for telephone customer call record and call detail information.[9/] In 2004, Congress adopted provisions as part of the Satellite Home Viewer Extension and Reauthorization Act requiring DBS providers to treat the personally identifiable information (PII) of their subscribers in accordance with the same privacy protections applicable to cable operators in Section 631.[10/] Congress has not adopted a privacy regime for broadband and the FCC cannot conjure one on its own simply because it is uneasy about one of the collateral effects of its decision to reclassify broadband service.

As the Commission itself has recognized, Section 222 has its roots in a bill sponsored by then-Rep. Markey, entitled the "Telephone Consumer Privacy Protection Act of 1993."[11/] Enacted as part of the Telecommunications Act of 1996 ("1996 Act"), Section 222 was designed to protect telephone customer privacy and promote competitive telephony by regulating telephone companies' use of their customers' call record, call detail and billing information, as well as to foster competition in the publication of telephone directories.[12/] The plain text of Section 222 contains language specific to the provision of telephony services that simply cannot

---

8/ 47 U.S.C. § 551.

9/ 47 U.S.C. § 222.

10/ 47 U.S.C. § 338(i).

11/ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information,* Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, n. 3 (1998) ("*1998 CPNI Order*").

12/ *See e.g.*, H.R. Rep. No. 204, 104th Cong., 1st Sess. 23 (1995) (defining CPNI as "information concerning the customer as is available to the local exchange carrier by virtue of the customer's use of the carrier's telephone exchange service or telephone toll services"); *id.* at 89 (noting that "LECs have total control over subscriber list information" and requiring non-discriminatory access to such information for competing "publishers of telephone directories" while also "ensuring that the telephone companies that gather and maintain such data are fairly compensated"); S. Rep. No. 23, 104th Cong., 1st Sess. 23-24 (1995) (describing rules imposed upon the "Bell companies" regarding treatment of customer-specific proprietary information); H.R. Conf. Rep. No. 458, 104th Cong., 2d Sess. 203-205 (1996) (Joint Explanatory Statement of the Committee of Conference).

map to broadband at all,[13/] thereby underscoring the absence of Congressional intent to apply those provisions to the Internet generally or to broadband Internet access service specifically.[14/] Further, Congress was aware that the Commission's pre-1996 Act CPNI rules were aimed at ensuring competition in the enhanced services business, but it deliberately chose to confine the statutory CPNI obligations to providers of voice services.[15/]

In its initial rulemakings implementing Section 222, the Commission clearly understood the services encompassed by the statute to be solely voice communications, concluding that the core CPNI provision in Section 222(c)(1)(A) should be interpreted as "distinguishing among telecommunications services based on traditional service distinctions, specifically local, interexchange, and CMRS."[16/] The Commission likewise recognized that key statutory terms were infused with telephony concepts, describing CPNI as "information that is extremely personal to customers as well as commercially valuable to carriers, such as to whom, where and

---

13/ *See e.g.* 47 U.S.C. § 222(h)(1)(B) (defining CPNI in part as "information contained in the bills pertaining telephone exchange service or telephone toll service received by a customer of a carrier"); 47 U.S.C. § 222(e)(requiring providers of "telephone exchange service" to make available subscriber list information – defined as customers' name, address and telephone number - for publication); 47 U.S.C. § 222(f) (regulating use or disclosure of wireless customer "call location information"); 47 U.S.C. § 222(g) (obligating providers of "telephone exchange service" to furnish subscriber list information to providers of emergency services); 47 U.S.C. § 222(c)(3) (conditioning use of aggregate customer information by "a local exchange carrier").

14/ Indeed, as demonstrated by the numerous references to the Internet and interactive computer services elsewhere in the 1996 Act, *see* 47 U.S.C. § 230(a)-(d), (f), Congress was fully capable of including data pertaining to customer usage of the Internet and interactive computer services within the ambit of Section 222, but opted not to do so. *See e.g.*, *Duncan v. Walker*, 533 U.S. 167, 173 (2001) ("Where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion.") (internal citations omitted).

15/ *1998 CPNI Order* at ¶ 77 (Prior to enacting Section 222, "Congress was well aware of the Commission's treatment of CMRS CPNI, and of our framework of nonstructural safeguards in connection with CPE and information services.").

16/ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Notice of Proposed Rulemaking*, CC Docket No. 96-115, 11 FCC Rcd 12513, ¶ 22 (1996); *1998 CPNI Order* at ¶ 27.

when a customer places a call."[17/] While the Commission has applied the requirements of Section 222 to new technologies that have emerged to compete with traditional telephone service,[18/] it has not, until recently, sought to apply the specific provisions of that statute to a service that is not a functional equivalent of voice service.[19/]

As the Commission itself acknowledges, several of the provisions of Section 222 have no meaning in the broadband context. Indeed, the *Notice* effectively concedes that the provisions of Section 222 cannot be interpreted to apply to broadband privacy in a coherent and holistic manner,[20/] thereby casting significant doubt on the validity of the Commission's interpretation of the statute in the *Notice*.[21/]

There is, for example, no "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer" associated with the provision of broadband service,[22/] and the Commission concedes that this portion of the CPNI definition can apply "only to" telephony service.[23/] Likewise, subjecting ISPs to the statutory directive in Section 222(e) to make subscriber name, address, and telephone number data available "to any

---

17/ *1998 CPNI Order* at ¶ 2.

18/ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, 22 FCC Rcd 6927, ¶ 56 (2007) ("*VoIP CPNI Order*").

19/ *Cf. id.* at ¶ 5 ("Practically speaking, CPNI includes information such as the phone numbers called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting").

20/ *See, e.g., NPRM* at ¶¶ 63-64, 80.

21/ *See United Savings Ass'n of Texas v. Timbers of Inwood Forest Associates*, 484 U.S. 365, 371 (1988) (Interpretation of a statute is "a holistic endeavor," and statutory language must be read in a manner that is "compatible with the rest of the law"); *Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach*, 118 U.S. 26, 36 (1998) (applying "that central tenet of interpretation, that a statute is to be considered in all its parts when construing any one of them").

22/ *See e.g.*, 47 U.S.C. § 222(h)(1)(B).

23/ *NPRM* at ¶ 38.

person" for directory publication "in any format" is wholly at odds with the basic thrust of the proposal in the *Notice*, which seeks to treat such information as personally identifiable information (PII) and bar ISPs from using or disclosing it absent customer consent.[24/]

Confronted with the Congressional decision to define customer name, address, and telephone information as "subscriber list information," the Commission simply declares – without any explanation or analysis – that "there is no subscriber list information in the broadband context."[25/] But the Commission cannot, by regulatory fiat, expunge from existence data categories and definitions in Section 222 that it deems incompatible with a regulatory framework founded upon that statute.[26/] If the Commission's proposed framework necessitates discarding data categories and definitional phrases included by Congress within the authorizing statute, that impugns the validity of the proposed framework under that statute, rather than, as the Commission supposes, the existence of those categories and definitions.[27/]

Grafting the requirements of Section 222 onto ISPs also would disregard a key limiting feature of the language of that provision. CPNI is, by definition "proprietary." Section 222 was enacted to address the sensitivity of information available only to a voice service customer's

---

24/ *See* 47 U.S.C. § 222(e); *NPRM* at ¶ 62.

25/ *NPRM* at ¶ 64.

26/ *United States v. Hood,* 343 U.S. 148, 151 (1952) ("We should not read out what as a matter of ordinary English speech is in"); *Walter v. Metropolitan Educ. Enterprises*, 519 U.S. 202, 209 (1997) ("Statutes must be interpreted, if possible, to give each word some operative effect"); *Metropolitan Life Ins. Co. v. Pettit*, 164 F.3d 857, 865 (4th Cir. 1998) (cautioning against "violating a fundamental precept of statutory interpretation" by reading statutory language "out of existence").

27/ *See Food & Drug Admin. v. Brown & Williamson Tobacco Corp*., 529 U.S. 120, 133 (2000) ("A court must . . . interpret the statute 'as a symmetrical and coherent regulatory scheme,' and 'fit, if possible, all parts into an harmonious whole'"); *Util. Air Regulatory Grp. v. E.P.A.*, 134 S. Ct. 2427, 2442 (2014) ("[A]gency interpretation that is 'inconsistent with the design and structure of the statute as a whole' does not merit deference") (internal citations omitted); *Corley v. United States*, 556 U.S. 303, 314 (2009) ("[O]ne of the most basic interpretive canons, that a statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant") (internal quotation marks and brackets omitted).

telephony provider by virtue of the carrier-customer relationship. But while call record and call detail information is "proprietary" because it is uniquely and solely held by a voice customer's telephone provider, broadband CPNI is not. Numerous third parties in the Internet ecosystem – including browser providers, search engines, app developers, operating systems, social networks, Websites and other entities – can access users' IP addresses, device identifiers, Web browsing history, and other information even if the broadband provider does not affirmatively disclose such information or take other steps to make such information available.[28/] It would be anomalous to decide that, in enacting Section 222, Congress intended to comprehensively protect a voice service customer's CPNI by imposing privacy obligations on the full scope of entities that may be able to access such data, while also – via the same statutory language – providing piecemeal protection for broadband customer data by imposing privacy requirements on only a small slice of entities that have access to such data.

The Commission's proposed broadband privacy framework also conflicts with another key purpose of Section 222 – fostering fair competition among similarly situated entities.[29/] Congress was concerned that telephone companies' singular access to customer call record data would provide them with a competitive advantage in adjacent markets.[30/] To address these concerns, Section 222 and the Commission's rules thereunder are designed to level the playing field by requiring non-discriminatory access to aggregate customer information compiled by telephone exchange companies and restricting their ability to use CPNI to win-back customers

---

28/ *See infra* § II.B.

29/ *See e.g. 1998 CPNI Order* at ¶ 52 (noting "the goals of section 222 to safeguard customer privacy and promote fair competition").

30/ *E.g.*, *id.* at ¶ 3 (suggesting that Congress aligned consumers' interests in privacy and competition such that, "where customer information is not sensitive, the customer's interest rests more in choosing service with respect to a variety of competitors, thus necessitating competitive access to the information, than in prohibiting the sharing of information.")

switching to a different provider.[31/] Not only is that concern inapposite here because numerous other entities in the broadband ecosystem have access to the same broadband activity data available to ISPs,[32/] but the Commission's proposed rules, as shown in Section II, will actually distort the competitive marketplace by hampering the ability of ISPs – compared to other online service entities – to use broadband activity data to competitively offer customized products and services to their subscribers and provide marketing and advertising messages tailored to their subscribers' interests and preferences.

The Commission cannot evade the substantive and jurisdictional limits of Section 222 simply by invoking its decision to reclassify broadband service as a telecommunications service. An agency cannot use its definitional authority to expand its jurisdiction beyond what Congress intended.[33/] As demonstrated by the language, structure, history and purpose of the provision, Congress had no intention of subjecting providers of broadband Internet access service to the constraints of Section 222, and the Commission cannot enlarge the scope of the statute to encompass entities and services which Congress deliberately chose not to include.

31/ *See, e.g.*, *id.* at ¶¶ 151-152 (finding that "[t]he aggregate rule rationally serves Congress's goal of encouraging competitive markets, through availability of aggregate customer information."); *id.* at ¶ 85 ("a local exchange carrier is precluded from using or accessing CPNI derived from the provision of local exchange service, for example, to regain the business of a customer that has chosen another provider.").

32/ *See infra* § II.C.

33/ *American Bankers Association v. SEC*, 804 F.2d 739, 754-55 (D.C. Cir. 1986) (agency cannot "change basic decisions made by Congress" or "use its definitional authority to expand its own jurisdiction"). *See also Loving v. IRS*, 742 F.3d 1013, 1021 (D.C. Cir. 2014) (invalidating agency's expansion of statutory term to encompass new class of entities not previously covered by rules due to inconsistency with the text, history, structure and context of the statute). *See also Comcast v. FCC*, 600 F.3d 642, 661 (D.C. Cir. 2010) ("[N]otwithstanding the 'difficult regulatory problem of rapid technological change' posed by the communications industry, 'the allowance of wide latitude in the exercise of delegated powers is not the equivalent of untrammeled freedom to regulate activities over which the statute fails to confer . . . Commission authority.'") *quoting National Ass'n of Regulatory Utility Commissioners v. FCC*, 533 F.2d 601, 618 (D.C. Cir. 1976).

B. Section 222(a) Is Not a Standalone Source of Authority for Regulation of Information That Does Not Constitute CPNI

Even if Section 222 empowered the Commission to regulate ISPs' use of broadband CPNI – which it does not – the statute does not grant it any authority to constrain their use of data that does not meet the definition of CPNI. The Commission's suggestion that Section 222(a) constitutes a standalone source of authority for imposing privacy safeguards on ISPs' treatment and use of "customer proprietary information" (CPI) – which would include both CPNI and PII of their customers - is contrary to law.[34/] The text and structure of Section 222 demonstrate that Congress did not intend to place use or disclosure restrictions on any information other than CPNI, or to endow Section 222(a) with authority for the Commission to regulate telecommunications carriers' use or disclosure of PII.

In contrast to other Communications Act privacy provisions,[35/] Section 222 was never intended to function as a general privacy statute protecting all forms of personally identifiable information. Nearly twenty years ago, the Commission recognized that "a customer's name, address and telephone number do not fall within the definition of CPNI,"[36/] without ever (until recently) suggesting that the privacy of such information was somehow subject to an independent source of protection under Section 222(a). To the contrary, as noted above, such information is specifically excluded from the definition of CPNI as "subscriber list information" under the statute.[37/]

34/ *NPRM* at ¶ 57.

35/ *See e.g.*, 47 U.S.C. § 551; 47 U.S.C. § 338(h).

36/ *See 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).

37/ 47 U.S.C. § 222(h)(1).

Congress established that, when acting pursuant to Section 222, the Commission could only treat "name, address, and telephone number" information as subscriber list information.[38/] Accordingly, the Commission cannot use Section 222(a) as a means to redefine subscriber name, address and telephone number information as PII for purposes of Section 222, since such information already has been defined as subscriber list information.[39/] Nor can it use Section 222(a) as a means of regulating broadband customer PII, since Congress clearly knows how to legislate protections for PII into the Communications Act, but opted not to do so in Section 222.[40/]

Until recently, the Commission consistently administered the statute as if CPNI was synonymous with the scope of customer information to be protected:

> Congress laid out a framework for carriers' use of customer information based on the sensitivity of the information. In particular, the statute allows easier dissemination of information beyond the existing customer-carrier relationship where information is not sensitive, or where the customer so directs. Thus, section 222 establishes three categories of customer information to which different privacy protections and carrier obligations apply: (1) individually identifiable CPNI, (2) aggregate customer information, and (3) subscriber list information.[41/]

38/ *See id.* (specifying that "as used in this section" name, address, and telephone number information are included as subscriber list information) (emphasis added).

39/ *Meese v. Keane*, 481 U.S. 465, 484 (1987) ("It is axiomatic that the statutory definition of [a] term excludes unstated meanings of that term"); *Gade v. National Solid Wastes Management Ass'n*, 505 U.S. 88, 100-01 (1992) (courts should avoid interpreting the text of a provision inconsistently with the necessary assumptions of another statutory provision).

40/ *See* 47 U.S.C. § 338(i); 47 U.S.C. § 551; *Russello v. United States*, 464 U.S. 16, 23 (1983) ("[W]here Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely"). Other communications-related statutes that, unlike Section 222(a), expressly protect and define "personally identifiable information" or "personal information" include the Video Privacy Protection Act, 18 U.S.C. § 2710, and the Children's Online Privacy Protection Act, 15 U.S.C. § 6501.

41/ *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, ¶ 6 (2002) ("*2002 CPNI Order*"); *1998 CPNI Order* at ¶ 2 ("Section 222 sets forth three categories of customer information to which different privacy protections and carrier obligations apply -- individually identifiable CPNI, aggregate

In 2007, the Commission reiterated that "Section 222(c) outlines the confidentiality protections applicable to customer information," again suggesting that the requirements of subsection (c) were synonymous with the scope of privacy protections accorded to customer information under Section 222."[42/]

The Commission has expressly stated that "sections 222(c)(1)(A) and (B), as well as the narrow exceptions in section 222(d), represent the only instances where customer approval for a carrier to use, disclose or permit access to personal customer information is not required."[43/] This statement cannot be reconciled with a claim that Section 222(a) constitutes a source of protection for PII, because the Commission there implicitly acknowledges that the disclosure of name and address information required by Section 222(e) is not a use or disclosure of "personal customer information" protected by Section 222, since no approval under subsection (e) is required for the collection and disclosure to third parties of such data for purposes of directory publication.

Indeed, notwithstanding the Commission's more recent statements in the *YourTel/Terracom* orders,[44/] the structure of the statute undermines claims that Section 222(a) can function as a separate, standalone source of authority to regulate PII of telecommunications customers, such as name and address information. Section 222(e) imposes an affirmative duty on carriers to enable third party directory providers to publish subscriber list information, which

---

customer information, and subscriber list information. CPNI includes information that is extremely personal to customers. . .").

42/ *VoIP CPNI Order* at n. 6.

43/ *1998 CPNI Order* at ¶ 23.

44/ *TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325 (2014) ("*YourTel/TerraCom NAL*"); *TerraCom, Inc. and YourTel America, Inc.*, Order, 30 FCC Rcd 7075 (2015).

expressly includes name, address and telephone number information.[45/] This duty is imposed "notwithstanding subsections (b), (c), and (d)" of Section 222.[46/] But Congress would not have simultaneously authorized the Commission to protect subscriber name and address information under Section 222(a), while also ordering carriers to enable the provision of such information to third parties under Sections 222(e).

It is noteworthy that Congress saw no need to establish the publication directive in Section 222(e) as an exception to any duty to protect name and address information established under subsection (a) – while also expressly excepting that same publication requirement to any duties to protect information set forth in subsections (b), (c), and (d). The most logical conclusion from the structure of the statute is that Congress did not view subsection (a) as a source of substantive regulatory authority over carriers' collection and use of information, and therefore did not deem it necessary to exempt the application of its putative constraints from the execution of the duty prescribed in subsection (e).[47/] Instead, consistent with the Commission's own approach to administering the statute for the first fifteen years of its existence, Congress treated subsection (a) as an overarching statement of purpose of Section 222, the details of which were set forth in the remaining provisions of that section.[48/]

45/ 47 U.S.C. § 222(e).

46/ *Id.*

47/ Congress replicated this same approach in 1999 in the Wireless Communications and Public Safety Act of 1999, when it adopted a duty to provide subscriber list information to emergency services providers, "notwithstanding subsections (b), (c) and (d)." Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286 (codified in 47 U.S.C. §§ 222(g)). Again, had Congress viewed subsection (a) as imposing substantive restrictions on the disclosure of subscriber name and address information, it would have had to adopt an exception for that subsection as well. That it did not demonstrates that no substantive data protection obligations (or regulatory authority to create such obligations) are present in subsection (a).

48/ *See YourTel/Terracom NAL*, Dissenting Statement of Commissioner Michael O'Rielly, at 2 ("Critically, the general duty in section 222(a) was intended to be read in conjunction with, not separate

Nor can the Commission reconcile the exceptions in Section 222(d) for using CPNI without customer approval to perform a variety of tasks, which include billing and collection, prevention of fraud, assistance to first-responders, and notification of a user's location to family members in emergency circumstances, with the position that Section 222(a) authorizes restrictions on the use of PII. Congress manifestly did not envision that conventional PII items such as customer name, address, and telephone numbers could be restricted from use by carriers pursuant to Section 222(a), or else it clearly would have authorized such information to be used in connection with activities covered by the exceptions in subsection (d). Indeed, those exceptions would be rendered ineffective and meaningless if carriers were not permitted to use name, address, and other customer "proprietary information" in order to bill, collect, deter fraud, and aid first responders and family members in emergencies.[49/] Congress clearly did not view Section 222 as imposing any restriction on the use of such information, and hence saw no need to exempt application of any restrictions on PII in connection with carrier activities covered by subsection (d).

Because the language and structure of Section 222 plainly preclude reading subsection (a) to empower the Commission to regulate a provider's use and disclosure of PII, the Commission's attempt to subject anything other than broadband CPNI to the constraints of Section 222 is unlawful.[50/]

---

from, the specific limitations in sections 222(b) and (c). And that is how the Commission viewed the provisions").

49/ *Cooper Industries, Inc. v. Aviall Services, Inc.*, 543 U.S. 157, 166 (2004) ("Aviall's reading would render part of the statute entirely superfluous, something we are loath to do.").

50/ *Cf. NPRM* at ¶ 62 (setting forth "non-exhaustive" list of "types of data that are PII").

C. The Scope of Data Covered under the Permissions Regime Exceeds the Limits of Section 222

As demonstrated below, the *Notice* disregards statutory limits on the scope of data that can be subject to use or disclosure restrictions, and erroneously identifies as CPNI and PII certain data items that cannot be classified as such.

1. Any Authority the Commission May Have to Regulate Broadband CPNI Is Limited to Individually Identifiable Information

Section 222 imposes restrictions on the use and disclosure of CPNI only to the extent that it is "individually identifiable,"[51/] and any broadband privacy regime erected under Section 222 must unequivocally adhere to this Congressional limitation on the scope of data covered by the constraints of the statute. The Commission's proposal, however, misapplies this statutory directive. Instead, the *Notice* turns cartwheels to invent a new category of data nowhere mentioned in the statute – "de-identified, non-collective data" – which, even though it is manifestly not "individually identifiable," would somehow still be covered by the use restrictions in Section 222(c).[52/] The Commission's proposed approach violates Section 222 by reading out of the statute the Congressional directive in subsection (c)(1) to impose use restrictions only on "individually identifiable" data.

The statute offers no basis for concluding, as the *Notice* does, that customer- or account-level data stripped of individual identifiers must still be considered "individually identifiable" unless and until it is grouped with other, similarly anonymized data. To the contrary, under the language of Section 222(c)(1), information can only be subject to use restrictions established under the statute if it is both (i) CPNI and (ii) individually identifiable; section 222(c)(1) does

---

[51/] 47 U.S.C. §§ 222(c)(1), (c)(3), (h)(2).

[52/] *See NRPM* at ¶ 165.

not, however, include a third prerequisite that such information must also be "aggregate." Indeed, there is nothing in Section 222 to suggest that de-identified information which is not "aggregate" somehow remains "individually identifiable." It strains credulity to conclude that a customer data record that cannot be used to identify a specific person nonetheless must be considered "individually identifiable" because it is not grouped with another similar record.

The implicit assumption in the *Notice* is that Section 222 creates a binary structure in which CPNI is either "individually identifiable" and subject to the permissions regime or "aggregate" and exempt from restrictions on use and disclosure. But this misapprehends the statute. While Section 222 establishes that "aggregate" data is *never* CPNI at all,[53/] it does not follow that "aggregate" information is the sole category of non-individually identifiable information. If Congress had intended that the use restrictions of Section 222(c)(1) should apply to all non-aggregate data, it could have easily so specified. The *Notice's* tentative conclusion to limit the carve-out from the permissions regime only to data that is both not "individually identifiable" and aggregate is legally unsustainable.

Congress's decision to limit the application of the permissions regime in Section 222 only to "individually identifiable" customer data is critical, because the bulk of the information categories proposed to be classified as either CPNI or PII in the *Notice* cannot, on their own, identify specific individuals.[54/] The failure of the *Notice* to give full effect to the plain meaning and impact of the "individually identifiable" limitation set forth in Section 222 significantly – and unlawfully – increases the compliance burdens of the regime proposed by the Commission

---

53/ *Compare* 47 U.S.C. § 222(h)(1) *with* 47 U.S.C. § 222(h)(2).

54/ *See NPRM* at ¶ 41; *id.* at ¶ 62 (including as PII items such as IP address, MAC address and device identifiers, cookies, Internet browsing history, traffic statistics, application usage data, geo-location information, shopping records, health information, and other items that cannot, on their own, identify a specific person).

by exponentially expanding the scope of data covered beyond what is permissible under the statute.

2. Neither IP Addresses nor MAC IDs Can Be Treated As CPI

Because IP addresses are assigned to customer devices by the ISP,[55/] they fall outside the statutory definition of CPNI as information "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[56/] IP addresses are not the property of customers and are not created by customers. The *Notice* itself states that a customer's IP address is "roughly analogous" to a telephone number, which also is assigned by the carrier.[57/] Importantly, Section 222 expressly defines a subscriber's telephone number as "subscriber list information," and not CPNI.[58/] The Commission's analogy thus confirms that a subscriber's IP address may not be defined as CPNI under Section 222.[59/]

For similar reasons, Media Access Control (MAC) addresses and other device identifiers also cannot be deemed to be CPNI. MAC addresses are typically native to an end user's device, and embedded by the manufacturer and thus are made available to the carrier by that device

---

55/ *See* Technical Appendix, *supra* n. 3, at 15.

56/ 47 U.S.C. § 222(h)(1)(emphasis added). IP addresses assigned to customer devices by ISPs may be temporary (dynamic IP addresses) or permanent (static). The ISP obtains blocks of IP addresses from its regional Internet registry. ISPs may provide a subscriber with a publicly routable IP address, or it may assign a non-routable IP addresses and utilize a Network Address Translation (NAT) device to route traffic to and from its intended endpoint or point of origination. Some ISPs rely upon NAT devices as a means of mitigating the effects of the potential exhaustion of IPv4 addresses. *See* Technical Appendix at 15-17.

57/ *NPRM* at ¶ 165.

58/ 47 U.S.C. § 222(h)(3).

59/ Nor should destination IP addresses of a broadband customer, by themselves, be considered CPNI, *see NPRM* at ¶ 41, absent their association with individually identifiable information about that subscriber.

maker, rather than the customer.[60/] MAC addresses of broadband customer equipment leased from ISPs, such as cable modems and wireless routers, demonstrably fail to meet the statutory criterion of being "made available to the carrier by the customer."[61/] In addition, neither IP addresses nor MAC IDs are available to ISPs "solely" as a result of the customer-carrier relationship. As noted, not only do ISPs assign IP addresses to their customers' equipment, but the American Registry for Internet Numbers (ARIN) makes its IP address range assignments to ISPs available to the public using the Whois protocol.[62/] Likewise, the IEEE makes its registry of assigned MAC/Ethernet addresses publicly available.[63/]

Nor can IP addresses or MAC IDs be treated as PII, *assuming arguendo* that Section 222 empowers the Commission to regulate ISPs' use of PII. Neither a MAC ID nor an IP address can be deemed to be "personally" identifiable information, because neither – on its own – is capable of identifying a specific person. A MAC ID can only identify a device, while an IP address typically can only identify an Internet endpoint associated with a set of devices.[64/] Further, the device endpoints associated with dynamic IP addresses change regularly, and even

---

60/ Vendors purchase from the Institute of Electrical and Electronics Engineers (IEEE) an Organizationally Unique Identifier (OUI) that is a 24-bit number that uniquely identifies the vendor/manufacturer. The vendor then appends to that another 24-bit number they generate to form a unique 48-bit number that constitutes the MAC address. *See* Technical Appendix at 24 and n. 47.

61/ 47 U.S.C. § 222(h)(1).

62/ *See* American Registry for Internet Numbers, whois.arin.net (last visited May 11, 2016).

63/ *See* IEEE Standards Association, Registration Authority Search Page, https://regauth.standards.ieee.org/standards-ra-web/pub/view.html#registries (last visited May 11, 2016).

64/ *See Pruitt v. Comcast Cable Holdings, LLC*, 100 Fed. Appx. 713 (10th Cir. 2004) (treating PII as consisting of name, address, and other subscriber-specific or individually identifiable information); *Klimas v. Comcast Cable Communications*, 465 F.3d 271, 276 (6th Cir. 2006) (treating PII as data containing the identity of "particular persons"); H.R. Rep. No. 98-934, at 79 (1984) (describing PII as "including specific information about the subscriber, or a list of names and addresses on which the subscriber is included"). *In re BitTorrent Adult film Copyright Infringement Cases*, 296 F.R.D. 80, 84 (E.D.N.Y. 2012) ("An IP address provides only the location at which one of any number of computer devices may be deployed") .

static IP addresses associated with home routers typically serve multiple devices. In addition, during the IPv4 to IPv6 transition, a single IPv6 address may denote hundreds or even thousands of endpoint devices that sit behind a local gateway. Treating IP addresses and device identifiers such as MAC IDs as inherently PII also would be out-of-step with several judicial decisions addressing that issue.[65/]

3. The Proposed Implementation of the Aggregate Data Exception Is Unlawful

As acknowledged in the *Notice*, Section 222(c)(3) permits providers to "use, disclose, or permit access to aggregate customer information" without need for customer approval.[66/] The statute expressly defines aggregate customer information,[67/] and the Commission has no authority to depart from that definition.[68/] The *Notice*, however, proposes to "expand[]" upon the "concept" of what Section 222 requires in order for data to be considered aggregate,[69/] and this

---

65/ *See e.g., Johnson v. Microsoft Corporation*, 2009 U.S. Dist. Lexis 58174 (W.D. Wash. June 23, 2009) (IP address does not constitute personally identifiable information); *In re Nickelodeon Consumer Privacy Litigation*, 2014 U.S. Dist. Lexis 91286 (D. NJ 2014) ("[M]erely acquiring an IP address does not itself identify an individual"); *Columbia Pictures Indus. v. Bunnell*, 2007 U.S. Dist. LEXIS 46364, 2007 WL 2080419 *3 n.10 (C.D. CA 2007) ("[A]n IP address identifies a computer, rather than a specific user of a computer"); *Pruitt,* 100 Fed. Appx. at 713 (10th Cir. 2004) (viewership data associated only with a converter box ID number is not PII subject to Section 631 of the Cable Act); *Malibu Media LLC v. Doe*, 2016 U.S. Dist. Lexis 45479 (D. NJ 2016) (one of several cases by the same name noting that plaintiff alleging copyright infringement and in possession of alleged infringer's IP address and the ISP with which it is associated could not, without more, ascertain the identity of alleged infringer); *Malibu Media LLC v. Doe*, 2014 U.S. Dist. Lexis 119560 (M.D. Fla. 2014) (Noting cases holding that "naming only an IP address is insufficient to identify an individual subscriber") .

66/ 47 U.S.C. § 222(c)(3); *NPRM* at ¶ 155.

67/ 47 U.S.C. § 222(h)(2).

68/ *See, e.g.*, *Burgess v. United States*, 553 U.S. 124, 129-30 (2008) ("Statutory definitions control the meaning of statutory words in the usual case. When a statute includes an explicit definition, we must follow that definition… As a rule, a definition which declares what a term 'means' excludes any meaning that is not stated.") (internal citations, brackets, and ellipsis omitted).

69/ *See NPRM* at ¶ 155.

"expansion" has the effect of narrowing the scope of the exception in a manner that contravenes the statute.

Congress specified that customer information would be considered aggregate information if it constitutes "collective data that relates to a group or category of services or customers from which individual customer identities or characteristics have been removed."[70/] The *Notice* proposes a four-part eligibility test for data to be treated as "aggregate information" that is unmoored from the statutory definition.[71/] In particular, the Commission's proposal would prevent collective customer data from being treated as "aggregate information" unless it is "not reasonably linkable to a specific . . . device." But the statutory definition of aggregate information makes no mention of linkability or association with customer "devices." It focuses only on whether collective information can be tied back to "individual customer identities and characteristics."[72/] Accordingly, the Commission's proposed implementation of the "aggregate information" exception is not permitted under Section 222.

D. The Commission Is Not Authorized by Other Provisions of the Communications Act to Adopt the Proposed Rules

The other potential sources of statutory authority cited in the *Notice* for the Commission's proposed framework are likewise unavailing. As discussed below, the additional provisions cannot be relied upon by the Commission because they are not sources of standalone authority for the proposed rules and/or would not be exercised consistently with the constraints of Section 222.

70/ 47 U.S.C. § 222(h)(2).

71/ *NPRM* at ¶ 155.

72/ 47 U.S.C. § 222(h)(2).

Section 201(b). Because Congress enacted a comprehensive privacy regime under Section 222, Section 201(b) cannot serve as an independent source of authority for the Commission to impose privacy protections on ISPs subject to Title II. The Commission itself has determined that "the specific consumer privacy and consumer choice protections established in section 222 supersede the general protections identified in sections 201(b) and 202(a)."[73/] This interpretation is consistent with Congress's stated understanding in passing specific CPNI legislation. When adding location information to the definition of CPNI, Congress did so based upon an understanding that there was no other lawful vehicle for protecting such information under the Communications Act.[74/]

While the Commission can rely upon Section 201(b) as an additional source of enforcement authority for the rules and requirements it adopts pursuant to Section 222, that provision cannot function as a basis for regulatory obligations that differ from – or are inconsistent with – the framework established by Congress.[75/] Here, however, as discussed above in Sections I.A and I.B, the rules proposed in the *Notice* exceed the Commission's authority under Section 222, and hence cannot be lawfully grounded in Section 201(b).[76/]

73/ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information,* Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, 14491, ¶ 153 (1999); *see also Appropriate Framework for Broadband Access to the Internet over Wireline Facilities*, 20 FCC Rcd 14853, ¶ 149 (2005) (noting that as a result of enactment of Section 222, "the pre-1996 Act CPNI framework . . . was eliminated in its entirety").

74/ *See, e.g.*, 145 Cong. Rec. H 9858 (Oct. 12, 1999) (statement of Rep. John Shimkus) (stating that unless protections for location information was added to the definition of CPNI, there would be "no protection for a customer's location information").

75/ *See e.g., 1998 CPNI Order* at ¶ 15 (Section 201(b) "authorize[s] the Commission to adopt any rules it deems necessary or appropriate to carry out its responsibilities under the Act, so long as those rules are not otherwise inconsistent with the Act").

76/ Likewise, Section 201(b)'s status as a repository of authority to address anti-competitive uses of customer data by carriers, *see e.g.*, *1998 CPNI Order* at ¶ 59 & n. 316, does not amount to a grant of authority to establish a broadband customer privacy regime.

Section 705. Section 705 of the Communications Act cannot serve as the basis for the rules proposed here.[77/] Section 705(a) of the Communications Act prohibits any person "transmitting or assisting in transmitting any interstate or foreign communication by wire or radio" from "divulg[ing] or publish[ing] the existence, contents, substance, purport, effect, or meaning thereof."[78/] Courts have ruled that all of Section 705(a) must be construed in harmony with the Federal Wiretap Act and its accompanying jurisprudence.[79/] Accordingly, as the Commission itself has recognized, any activity permissible under the Wiretap Act cannot be deemed to be proscribed by Section 705(a),[80/] thereby raising substantial doubt about that provision's ability to serve as a basis for the framework proposed in the *Notice*.

First, the Wiretap Act was amended in 1986 to remove any prohibition against interception or divulgence of non-content information associated with a communication – including information about the existence of, or parties to, the communication.[81/] Thus, there is a

---

77/ Indeed, the structure of the provision raises questions as to whether Congress intended to grant the Commission general rulemaking authority, since it establishes both criminal penalties and authorizes civil actions by aggrieved persons, 47 U.S.C. § 605(e)(1)-(4), while authorizing rulemaking authority only for the limited purpose of devising a universal encryption standard for private home viewing of satellite cable programming. 47 U.S.C. § 605(h).

78/ 47 U.S.C. § 605(a).

79/ *See e.g. United States v. Rose,* 669 F.2d 23, 26-27 (1st Cir. 1982) (noting that restrictions of Section 705 do "not apply to communications that may be intercepted and disclosed under" the Wiretap Act and acknowledging that "the protective shield of" Section 705 "is significantly diminished" by incorporating the provisions of the Wiretap Act); *Edwards v. State Farm Ins. Co.*, 833 F.2d 535, 540 (5th Cir. 1987); *United States v. Gass*, 936 Sup. 810, 812 (N.D. Okla. 1996).

80/ *Google Inc.*, Notice of Apparent Liability for Forfeiture, File No. EB-10-III-4055, DA 12-592 at ¶ 6 (rel. Apr. 13, 2012)("*Google Street View NAL*") ("[C]ase law supports that conduct authorized by the Wiretap Act is exempt from Section 705(a)'s prohibitions"); *Cosgrove v. Greater New Orleans Expressway Comm'n*, 1999 LEXIS 672, n. 2 (E.D. LA 1999) ("The Federal Communications Act, 47 U.S.C. § 605, also is inapplicable because it does not apply to activities 'authorized by chapter 119, Title 18'").

81/ *In re iPhone Application Litigation*, 844 F. Supp. 2d 1040, 1062 (N.D. Cal 2012) (noting that in 1986 Wiretap Act was amended to excise the phrase "information concerning the identity of the parties to such communication or the existence . . . of that communication" from the definition of the term "contents").

threshold question of whether Section 705(a) can offer any basis at all to regulate or condition ISP use and disclosure of non-content metadata pertaining to broadband customers.[82/]

Second, under Wiretap Act jurisprudence, implied consent is a complete defense to claims that a communication has been unlawfully intercepted or disclosed.[83/] Courts have held that where a person has been given actual notice of intent to intercept his or her communications, consent to the interception may be implied for purposes of the Wiretap Act.[84/] Thus, even if ISPs' use of broadband customer CPI did implicate the prohibitions of Section 705(a), the permissions regime proposed by the Commission imposes far greater restrictions on divulgence of the existence or content of broadband customer communications than is permissible under jurisprudence governing the administration and enforcement of that provision.

Third, the Wiretap Act also contains an ordinary course of business exception.[85/] Any equipment or facility used by a provider of wire or electronic communication service in the

---

82/ *See id.* (holding that "under the current version of the statute, personally identifiable information that is automatically generated by the communication but that does not comprise the substance, purport, or meaning of that communication is not covered by the Wiretap Act").

83/ *United States v. Amen*, 831 F.2d 373, 378 (2d Cir. 1987) (consent for purposes of the Wiretap Act "may be either actual or implied"); *Williams v. Poulos*, 11 F.3d 271, 281 (1st Cir. 1993) (implied consent is "inferred from surrounding circumstances indicating that the party knowingly agreed" to interception of his or her communications"); *Griggs-Ryan v. Smith*, 904 F.2d 112, 117 (1st Cir. 1990) (implied consent "ordinarily include[s] language or acts which tend to prove (or disprove) that a party knows of, [and] assents to, encroachments on the routine expectation that [communications] are private"); *see also*, *Berry v. Funk*, 146 F.3d 1003, 1010 (D.C. Cir. 1998) ("[I]t has been uniformly held that implicit consent will satisfy" consent exception).

84/ *See Amati v. City of Woodstock*, 176 F. 3d 952, 955 (7th Cir. 1999) ("If there is actual notice . . . there will normally be implied consent"). *See also, e.g.*, *Griggs-Ryan*, 904 F. 2d at 118 ("In the face of express notice, it cannot be gainsaid that plaintiff impliedly consented to what later transpired."); *Amen*, 831 F.2d at 379 ("[T]he district court properly found that the two defendants had notice of the interception system and that their use of the telephones therefore constituted implied consent to the monitoring."); *Shefts v. Petrakis*, 758 F. Supp. 2d 620, 630-31 (C.D. Ill. 2011) (finding consent where notice of logging and storage of text messages was contained in the Employee Manual provided to all employees).

85/ 18 U.S.C. § 2510(4).

ordinary course of its business does not implicate a prohibited interception under the Act,[86/] and hence would not engender a prohibited disclosure.[87/] The Second Circuit Court of Appeals has ruled that an ISP does not engage in prohibited interceptions of communications when utilizing facilities employed within the ordinary course of its business, such as "routers, servers and other computer equipment [used] as part of its email service to all customers."[88/] The court reasoned that an ISP's basic offering involves the "acquisition of the contents" of an electronic communication, and that if the ordinary course of business exception did not apply to its core facilities it would be deemed to constantly intercept communications in violation of the Wiretap Act. Thus, disclosures of CPI captured with equipment used in the ordinary course of an ISP's business arguably could not be prohibited under Section 705(a).

Fourth, the prohibitions of Section 705(a) apply to any person "receiving, assisting in receiving, transmitting, or assisting in transmitting" any wire or radio communication.[89/] Thus, if applicable to the broadband privacy context, these prohibitions arguably could cover a variety of entities in the broadband ecosystem that transmit, receive, or access data defined as broadband CPI, thereby rendering the Commission's proposed framework significantly under-inclusive.[90/] Indeed, the ready availability of broadband customer usage data to vast numbers of other entities

---

86/ 18 U.S.C. § 2510(5)(a).

87/ 18 U.S.C. § 2511(1)(c)-(d). *See Nix v. O'Malley*, 160 F.3d 343, 349 (6th Cir. 1998) (ECPA "establishes two preconditions to a finding of liability: the interception must have violated the law, and the defendant must have known or had reason to know this when he disclosed the contents of the intercepted communication").

88/ *Hall v. EarthLink Network, Inc.,* 396 F.3d 500, 504-05 (2d Cir. 2005).

89/ 47 U.S.C. § 605(a).

90/ *See infra* § II.B. *See also Online Advertising and Hidden Hazards to Consumer Security and Data Privacy*, Staff Report, Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, May 15, 2014, at 5 ("A visit to an online news site may trigger interactions with hundreds of other parties that may be collecting information on the consumer as he travels the web. The Subcommittee found, for example, a trip to a popular tabloid news website triggered a user interaction with some 352 other web servers as well.").

in the broadband ecosystem itself raises doubts about the ability to predicate the proposed rules on Section 705, since that provision would not cover communications through a system that makes the communications "readily accessible" to the public.[91/]

Section 706. Section 706 does not empower the Commission to adopt the rules proposed in the *Notice*. While the D.C. Circuit has ruled that the FCC could, if it wished, rely upon Section 706 as a legal basis for net neutrality requirements,[92/] it also made clear that whatever authority is imparted under Section 706(a) may not be exercised in a manner inconsistent with the Communications Act.[93/] As discussed above, the rules proposed by the Commission exceed the constraints imposed by Section 222 in several respects, and those transgressions cannot be rectified simply by invoking Section 706.

Further, it would be difficult for the Commission to argue that its proposed privacy rules would *eliminate* barriers to broadband investment. There is no empirical evidence that a lack of such protections has inhibited investment in broadband infrastructure. To the contrary, broadband investment thrived under an FTC-based privacy regime that applied uniformly to all online entities, and there is already evidence that the Commission's proposal to single out ISPs for more stringent rules would dampen broadband investment.[94/]

91/ 18 U.S.C. § 2511(2)(g)(i).

92/ *Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014).

93/ *Id.* at 649-50.

94/ *See e.g., FCC Internet privacy proposal could harm broadband providers - Moody's*, REUTERS (Mar. 15, 2016), *available at* http://www.reuters.com/article/usa-fcc-internet-moodys-idUSL2N16N19H.

E. Adoption of the Proposed Rules Would Be Arbitrary and Capricious

Adoption of the privacy regime proposed in the *Notice* would be arbitrary and capricious.[95/] For more than a decade, ISPs were subject to a flexible and well-balanced privacy framework applicable to all entities in the broadband ecosystem. The FTC Framework protected the privacy interests of broadband consumers while simultaneously providing all online entities, including ISPs, the opportunity to use customer data to gain more insight into the interests and preferences of their customers and, in turn, develop customized services and new content through marketing and advertising that is more relevant to their customers.

As detailed more fully below,[96/] the Commission's proposal departs dramatically from the FTC Framework in several key respects without offering a reasoned explanation for these departures or for the onerous rules that result from them. The Commission has offered no evidence that the FTC Framework was deficient in terms of protecting broadband consumers from misuses of their data by ISPs, or that there are any potential privacy harms that could not be adequately redressed through a framework that parallels the FTC model. The Commission also fails to justify the regulatory asymmetry fostered by its proposal.[97/] It sets forth counter-factual conclusions regarding ISP visibility and use of broadband consumer data relative to edge providers with access to the same information, even though those conclusions are refuted by a

---

95/ Under the Administrative Procedure Act ("APA"), agency action will be found arbitrary and capricious to the extent the agency, among other things, failed to consider an important aspect of the problem or offered an explanation for its decision that runs counter to the evidence before the agency. *Motor Vehicle Mfrs. Ass'n v. State Farm Mutual Auto Insurance Company*, 463 U.S. 29, 43 (1983). Agency action will not be upheld absent "a satisfactory explanation for its action, including a rational connection between the facts found and the choice made." *Id.* The Commission's proposed rules fail to meet these elementary standards and are therefore impermissible under the APA.

96/ *See infra* § II.

97/ *See infra* § II.B; *McElroy Electronics Corp. v. FCC*, 990 F.2d 1351, 1365 (D.C. Cir. 1993) ("we remind the Commission of the importance of treating similarly situated parties alike or providing an adequate justification for disparate treatment").

thorough and comprehensive study that the *Notice* does not even bother to discuss.[98/] Further, the Commission fails to consider the substantial costs and burdens imposed upon ISPs and the potential adverse effects of its proposed rules on consumers and the Internet ecosystem at all, and weight those against the purported benefits of the proposal.[99/]

The proposed regime also would be substantially overbroad, in relation to the problem it seeks to address, since it categorically restricts ISPs' ability to use customer data elements that do not themselves identify specific persons and therefore do not implicate potential privacy harms.[100/] The proposed rules are ill-suited to resolving the problems they are designed to address in other respects. The more restrictive limitations on ISP use of broadband customer data will not improve broadband consumer privacy because all other entities in the online ecosystem will continue to be permitted to use the same data pursuant to the less stringent FTC Framework.[101/] Indeed, the Commission's decision to subject ISPs to stricter controls on their use of broadband customer data is not reasonable in light of its previous findings that consumer privacy risks are greater when consumer data is used by entities that are not in a recurring service relationship with subscribers, rather than when it is used by companies like ISPs that are in such a recurring relationship.[102/]

98/ *See* 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, 7, 23-35 (Feb. 29, 2016) ("*Swire Paper*").

99/ *See infra* § II.C.

100/ *See infra* § II.D.

101/ *See infra* § II.C.

102/ *2002 CPNI Order* at ¶ 37 ("Because of commercial constraints required to ensure customer accountability, therefore, the carrier with whom the customer has the existing business relationship has a strong incentive not to misuse its customers' CPNI or it will risk losing its customers' business."). *See also infra* pp. 51-52.

F. Adopting a Broadband Privacy Regime for ISPs that Differs Materially from the FTC Privacy Framework Implicates Serious Constitutional Concerns

The Commission's imposition of new, more stringent restrictions on ISP commercial speech notwithstanding the proven track record and effectiveness of the less restrictive FTC Framework contravenes the First Amendment. Courts have confirmed that the government's decision to impose opt-in, rather than opt-out rules, on ISP use of customer data for marketing and advertising messages implicates the basic *Central Hudson* analytical framework for regulatory restrictions on commercial speech.[103/]

In assessing whether the proposed restrictions on ISPs' commercial speech are narrowly tailored to address specific, non-conjectural harms to consumer privacy,[104/] the Commission faces fresh challenges not at issue in *NCTA v. FCC*.[105/] In particular, the Commission must grapple with the fact that, prior to reclassification, the privacy of broadband consumers was effectively protected without resorting to the more stringent permissions regime and heightened restrictions on use of de-identified data proposed in the *Notice* for ISPs.[106/] The *Notice*, however, fails to set forth specific facts demonstrating that the privacy interests of broadband consumers were not adequately protected from harmful acts by ISPs under the pre-reclassification FTC

103/ *National Cable & Telecommunications Association v. FCC*, 555 F.3d 996 (D.C. Cir. 2009); *U.S. West v. FCC*, 182 F.3d 1224 (10th Cir. 1999); *see also Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York*, 447 U.S. 557, 566 (1980) (restrictions on commercial speech satisfy First Amendment only if "(1) there is a substantial government interest; (2) the regulation directly advances the substantial government interest; and (3) the proposed regulation is not more extensive than necessary to serve that interest").

104/ *Lorillard Tobacco v. Reilly*, 533 U.S. 525, 555-56 (2001) (*Central Hudson* requires the government to "demonstrate that the harms it recites are real and that its restriction will alleviate them to a material degree" and that the proposed restrictions are "narrowly tailored to achieve the desired objective") (internal citations omitted).

105/ *See supra* n. 103, *NCTA v. FCC,* 555 F.3d 996. *See also Sorrell v. IMS Health, Inc*., 564 U.S. 552 (2011) (holding that the process of gathering and analyzing data in preparation for speech is protected by the First Amendment and leaving open the question whether restrictions on such expression should receive stricter First Amendment scrutiny than the intermediate standard of *Central Hudson*).

106/ *See infra* §§ II and III.

Framework, or that that framework was otherwise deficient in safeguarding consumer privacy interests.

The Commission's decision to adopt a more restrictive regime than the framework applicable to edge providers also is problematic in light of its previous findings that there is a greater risk of privacy abuses or data misuses arising from entities – such as large edge providers – that are not in an ongoing business relationship with end users whose personal data is being used.[107/] Indeed, the First Amendment flaws of the proposed rules are exacerbated by the fact that other broadband entities with comparable – if not greater – access to broadband consumer CPI are subject to a more lenient set of privacy rules.[108/]

G. The FCC Lacks Authority to Adopt Prescriptive Broadband Data Security Rules

The Commission lacks authority to impose upon ISPs the specific data security regulations proposed in the *Notice*.[109/] Whatever authority the Commission may have to enforce carriers' obligation to ensure the confidentiality of CPNI in accordance with the requirements of Section 222 does not extend to adopting regulations delineating the specific procedures and measures they must take in order to meet that obligation. Where Congress seeks to impose

---

107/ *See supra* n. 102; *infra* pp. 51-52.

108/ *See Time Warner Cable, Inc. v. Hudson*, 667 F.3d 630, 641 (5th Cir. 2012) ("[A] law that targets a small handful of speakers for discriminatory treatment 'suggests that the goal of the regulation is not unrelated to suppression of expression, and such a goal is presumptively unconstitutional.' Therefore, 'we cannot countenance such treatment unless the State asserts a counterbalancing interest of compelling importance'"); *see also Verizon Northwest Inc. v. Showalter*, 282 F. Supp. 2d 1187 (W.D. WA 2003) (invalidation on First Amendment grounds State rules regulating CPNI: "[C]onsumers face different rules regarding the use of CPNI if they use wireless and interstate telecommunications services in addition to the intrastate services to which the WUTC's rules apply. Furthermore, the exclusion of wireless services from the regulations leaves a large segment of services free from the protections offered by the WUTC's restrictions. The WUTC, therefore, fails to establish that its rules are part of a substantial effort to advance a valid state interest").

109/ *NPRM* at ¶ 174.

specific, granular data security requirements, it does so expressly.[110/] Nothing in Section 222 supports the proposition that Congress intended for the Commission to dictate by regulation the steps and procedures ISPs must take in order to secure the confidentiality of CPNI.

Not only does the Commission lack legal authority to impose the specific data security requirements proposed in the *Notice*, those requirements also conflict with the Congressional preference for relying on voluntary mechanisms and industry-driven best practices to secure networks. Congress decided in the Cybersecurity Enhancement Act of 2014 to establish the NIST Framework as the preeminent Federal policy mechanism for bolstering the cyber defenses of American companies.[111/] The Act directed that NIST should "on an ongoing basis, facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost effectively reduce cyber risks to critical infrastructure."[112/] The Act also expressly provided that it did not "confer any regulatory authority on any Federal, State, tribal, or local department or agency."[113/] Congress clearly memorialized into law a policy preference to strengthen cybersecurity by eschewing regulation and relying instead upon a public-private collaboration that uses voluntary mechanisms to develop best practices and guidelines for reducing risks to cyber- and data security. The Commission's proposal to prescribe specific procedures and measures for ISPs to

---

110/ *See e.g.*, Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320-d(2)(d) (specifying requirements and factors to be considered by HHS in establishing data security standards and safeguards for health care providers); Gramm-Leach-Bliley Act, 15 U.S.C. § 6801(b) (directing agencies to establish appropriate security standards relating to "administrative, technical, and physical safeguards" to ensure the security and confidentiality of consumers' financial information); Fair Credit Reporting Act, 15 U.S.C. § 1681w(a) (directing FTC and other Federal agencies to establish regulations designed to prevent unauthorized access to consumer credit reports by specifying proper procedures for disposal of such reports).

111/ P.L. No. 113-274 (2014).

112/ 15 U.S.C. § 272(c)(15).

113/ 15 U.S.C. § 7422.

take in fulfilling their duty to protect CPNI from unauthorized access is contrary to law because it is neither authorized by Section 222 nor consistent with Congressional policy.[114/]

H. The Commission Neither Can Nor Should Harmonize Its Proposed Rules with Section 631

The Commission has no authority to "harmonize" the notice and customer approval requirements proposed in the *Notice* with the notice and approval provisions expressly adopted by Congress in Section 631 of the Cable Act.[115/] Apart from the fact that the proposed rules are themselves unlawful, the privacy obligations set forth in Section 631 "occupy the field" with respect to privacy requirements imposed upon cable operators providing cable service.[116/] Congress had no intention of authorizing the Commission to use whatever power was granted to it under Section 222 to undo the statutory scheme Congress established in Section 631.[117/] The Commission cannot use reclassification as a pretext for supplanting the privacy framework established by Congress for cable service in Section 631.[118/]

The notion of harmonizing the proposed rules with the requirements of Section 631 is legally deficient in several other respects. First, the privacy rules proposed in the *Notice* have

---

114/ As detailed below, the adoption of compulsory data security rules for ISPs also would be inconsistent with the Commission's own oft-stated policy preferences for relying upon voluntary mechanisms and industry-driven solutions to secure networks. *See infra* § II.E.

115/ *See NPRM* at ¶¶ 103, 153.

116/ *See Gorbach v. Reno*, 219 F.3d 1087, 1098 (9th Cir. 2000) (rejecting view that agency has delegated authority to adopt rules where "express statutory procedure is exclusive and fully occupies the field"); H.R. Rep. No 98-934, 98th Cong., 2d Sess. 77 (1984) (Section 631 "provides procedural safeguards to consumers for the protection of their privacy interests").

117/ H.R. Rep. No. 204, 104th Cong., 1st Sess. 90 (1995) (specifying that "new privacy rules" for CPNI adopted as part of Telecommunications Act of 1996 apply only to "telecommunications carriers").

118/ *Board of Governors of Federal Reserve System v. Dimension Financial Corp*., 474 U.S. 361, 374 (1986) (where Congress has "defined with specificity" scope and requirements of a statute, agency "has no power to correct flaws that it perceives in the statute"); *Board of Trade v. SEC*, 883 F.2d 525, 535 (7th Cir. 1989) ("When Congress establishes the rules, an agency must carry them out. A desire to keep the law 'up to date' does not justify departure from its rules").

been developed specifically to apply to a service classified as a common carrier offering by the Commission.[119/] Section 621(c) of the Cable Act, however, bars the Commission from imposing common carrier regulation on any cable service offered by a cable operator.[120/]

Second, Section 624(f)(1) of the Cable Act expressly bars the Commission from "imposing requirements regarding the provision or content of cable services except as expressly provided in" Title VI.[121/] Conditioning an operator's provision of cable service upon adherence to all or any of the rules proposed in the instant proceeding is not authorized by Title VI and hence would contravene Section 624(f)(1).

Third, the proposed "harmonization" would be inconsistent with previous statements from the FCC that Section 631 is "enforced by the courts, and not by the Commission."[122/] Indeed, Congress specifically authorized a private right-of-action as a remedy for cable operator violations of Section 631.[123/] There is no lawful basis for concluding that the Commission, acting pursuant to its putative Title II authority over ISPs, could somehow alter the Title VI privacy rights that Congress intended to be enforced by consumers themselves through private rights-of-action.

119/ *See e.g., NPRM* at Appendix A (proposing to amend part 64, "Miscellaneous Rules Relating to Common Carriers," by adding rules proposed in the *NPRM*).

120/ 47 U.S.C. § 541(c).

121/ 47 U.S.C. § 544(f)(1).

122/ *Applications for Consent to the Transfer of Control of Licenses and Section 214 Authorizations by Time Warner Inc. and America Online, Inc., Transferors, to AOL Time Warner Inc., Transferee*, CS Docket No.00-30, Memorandum Option and Order, 16 FCC Rcd 6547, ¶ 279 (2001).

123/ 47 U.S.C. § 551(f); H.R. Rep. No 98-934, 98th Cong., 2d Sess. 77 (1984)("Subscribers may enforce their rights under this subsection pursuant to terms specified in subsection (f)"); *see also Meghrig v. KFC Western, Inc.,* 516 U.S. 479, 488 (1996) ("It is an elemental canon of statutory construction that where a statute expressly provides a particular remedy or remedies, a court must be chary of reading others into it").

Even if it were not barred from doing so by statute, the Commission should nonetheless refrain from harmonizing the rules proposed here with Section 631. Cable operators have more than three decades of experience complying with Section 631 of the Communications Act,[124/] one of the most robust, long-standing, and customer-protective privacy regimes in existence. The Commission has never adopted any rules implementing the Cable Act privacy provisions, and those provisions have protected cable subscriber privacy for over 30 years. The absence of prescriptive rules enables practices and safeguards to adapt to changes in technology and the marketplace, consistent with the basic framework set forth in the statute.

Unlike broadband, there has been no reclassification or other change in the regulatory structure of cable television that requires dislodging the well-established and successful privacy framework for cable service. It makes no sense for the Commission to take a new, untested, and highly prescriptive privacy framework for broadband providers and attempt to graft it onto the demonstrably effective regime that Congress established for cable service. There is no evidence at all that consumers are demanding such an action, nor is there any basis for concluding that such an approach would materially improve the careful balance between privacy safeguards and permissive data uses embodied in the framework for cable service adopted by Congress.

Further, the Commission's proposed rules cannot be sensibly or productively harmonized with Section 631. The key statutory provisions at issue are not susceptible to easy reconciliation. While Section 631 does not limit data "use," Section 222 does. Conversely, Section 222 does not restrict any data collection, but Section 631 does. Section 631 delineates specific notice obligations, while Section 222 lacks a corresponding notice requirement. Section 631 also specifically prescribes the manner in which government entities may obtain access to PII, while

---

[124/] 47 U.S.C. § 551.

Section 222 contains no similar provision. Moreover, the specific rules proposed by the Commission are even less amenable to harmonization with Section 631. Congress established a specific and comprehensive permissions regime in Section 631 that cannot be altered by rule and which is very different from the permissions regime proposed in the NPRM.

The Commission's concern with Section 631 harmonization is particularly misplaced in light of its apparent tolerance for the substantial conflicts between the two privacy regimes that would govern broadband consumer data if the proposed rules are adopted. Under the Commission's proposal, customer data from the same category of communications service will be treated very differently by different entities in the broadband service ecosystem.[125/] There is nothing in the Commission's proposal to address this conflict or mitigate the potential confusion for consumers. By contrast, there is less potential for consumer confusion or conflict in a circumstance in which distinct services are subject to distinct sets of privacy obligations – particularly when all entities involved in the provision of such service are subject to the same rules. Rather than focus unnecessarily on harmonization across distinct service categories, the Commission should instead address the lack of harmonization concerning treatment of broadband consumer data that would be established within the same category of service by adoption of its proposed rules.[126/]

II. THE COMMISSION'S PROPOSED PRIVACY REGIME IS SIGNIFICANTLY AND UNJUSTIFIABLY MORE RESTRICTIVE THAN THE FTC FRAMEWORK

The flexibility of the FTC Framework has enabled consumer privacy to be protected while still allowing data to be a key driver of the virtuous cycle of broadband investment,

125/ *See infra* § II.C.

126/ *See infra* § III.

innovation, and service enhancement.[127/] There is widespread agreement that near-continuous innovation and advancement in the area of data analytics and applications over the last decade has been central to the growth of the Internet economy.[128/]

Broadband consumers today expect and receive graphics and settings tailored to their preferences, product and service recommendations and advertisements that reflect their interests, habits, and hobbies, and suggestions about new music, movies, video and other content that reflect their tastes.[129/] Consumers who prefer to forego such customization have access to an ample array of tools and services to do so,[130/] and the FTC Framework itself ensures that they are provided with opportunities to opt-out of having their individually identifiable data used by the online entities with which they interact. Notwithstanding the availability of these tools and

---

127/ *Protecting Consumer Privacy in an Era of Rapid Change*, FEDERAL TRADE COMMISSION, at 2 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf ("*FTC Privacy Report*"); *Report to the President, Big Data and Privacy: A Technological Perspective*, President's Council of Advisors on Science and Technology, 11-14 (May 2014), https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf ("*PCAST Big Data Report*"); *Big Data: Preserving Opportunities, Preserving Values*, Executive Office of the President, 39-41 (May 2014), https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf ("*White House Big Data Report*").

128/ *See Data-Driven Innovation: Big Data for Growth and Well-Being*, Organisation for Economic Co-operation and Development, 20 (2015), http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/data-driven-innovation_9789264229358-en#page1.

129/ *See Fact Sheet: U.S. Consumers Want More Personalized Retail Experience and Control Over Personal Information, Accenture Survey Shows*, Accenture (Mar. 2015), https://www.accenture.com/us-en/~/media/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_10/Accenture-Retail-Personalization-Survey-Fact-Sheet-March-2015.pdf; *see also* Gartner, Gartner Says Consumers Most Value Online Banking Features that Address Communication and Personalization, Press Release (Jul. 2009), http://www.gartner.com/newsroom/id/1089312 (finding that "[c]onsumers most value online banking features that address communication and personalization"); Janrain, *Online Consumers Fed Up with Irrelevant Content on Favorite Websites According to Janrain Study*, Press Release (Jul. 2013), http://janrain.com/about/newsroom/press-releases/online-consumers-fed-up-with-irrelevant-content-on-favorite-websites-according-to-janrain-study/.

130/ *See The 2015 Ad Blocking Report*, PAGEFAIR (Aug. 2015), https://blog.pagefair.com/2015/ad-blocking-report/; Rob Lightner, *Five smart ways to keep your browsing private*, CNET (Jan, 2012), http://www.cnet.com/how-to/five-smart-ways-to-keep-your-browsing-private/.

choices, consumers' behavior demonstrates, subject to appropriate safeguards, their affinity for having their broadband experience reflect and respond to their interests and preferences.[131/]

Given the success of, and support for, the FTC Framework with respect to balancing the important interests at stake here, the most logical policy choice for the FCC to make post-reclassification would be to hew as closely as possible to the FTC model. But the proposal in the *Notice* rejects that approach, notwithstanding earlier signals that the Commission intended to adhere to the FTC's framework.[132/] As demonstrated below, the end result of the Commission's rejection of key elements of the successful FTC Framework will be more consumer confusion, lowered consumer welfare, less competition, and adverse effects on the broadband ecosystem as a whole, the broadband customer experience and broadband investment and innovation.

A. The Proposed Rules Are Not Harmonized with the FTC Framework

The privacy regime proposed in the *Notice* differs from the FTC model both conceptually and substantively.[133/] The FTC Framework was designed to be flexible, harms-based,

---

131/ *See, e.g.*, *Ad-Blocking, Measured,* ClarityRay, at 4 (May 2012) (finding only 8.72% of ad impressions in the U.S. were blocked by ad blockers), *available at* http://www.slideshare.net/arttoseo/clarity-ray-adblockreport; Genesis Media Ad Blocking Survey (Aug. 7, 2015), http://www.genesismedia.com/news/survey-of-over-11500-adults-finds-76-percent-have-never-used-ad-blockers/ (finding that 76% of U.S. consumers in 2015 did not use ad blockers, despite over 60% of consumers being aware that such a product existed).

132/ *See, e.g.*, Margaret Harding McGill, *FCC, FTC Chiefs Zero In On Data Security, Privacy,* LAW360 (Jan. 6, 2016), *available at* http://www.law360.com/articles/743314/fcc-ftc-chiefs-zero-in-on-data-security-privacy (quoting FCC Chairman Tom Wheeler as saying "What the FTC has done in that regard is to build a terrific model and so I think one of our challenges is to make sure we're consistent with the kind of thoughtful, rational approach that the FTC has taken."); Kate Tummarello and Alex Byers, *Wheeler's crystal ball: Net neutrality decision soon*, POLITICO, http://www.politico.com/tipsheets/morning-tech/2016/03/wheelers-crystal-ball-net-neutrality-decision-soon-garland-a-quick-study-on-telecom-issues-a-path-forward-for-small-biz-bill-in-the-senate-213269 (quoting FCC Chairman Tom Wheeler as saying "We're following the same kind of conceptual framework that the FTC has.").

133/ Maureen K. Ohlhausen, Commissioner, U.S. Federal Trade Commission, *Privacy Regulation in the Internet Ecosystem*, Prepared Remarks at the Eighth Annual Telecom Policy Conference, Free State Foundation, at 7 (Mar. 23, 2016) ("The FCC's proposal differs significantly from the choice architecture the FTC has established.") ("*Ohlhausen 2016 Remarks*").

technology-neutral, and outcome-oriented.[134/] It focuses on preventing harmful outcomes rather than on prescribing rules and practices for companies to follow.[135/] Such an approach fosters innovation and is better-suited for the dynamic and technically complex broadband ecosystem, where technology and consumer preferences rapidly evolve and change.[136/]

In contrast, the FCC's scheme is prescriptive rather than harms-based; rigid rather than flexible; and process-based rather than outcome-oriented. While the FTC has moved over the last decade and a half from "emphasizing potentially costly notice-and-choice requirements for all uses of information" to "focus on specific consumer harms,"[137/] the FCC proposes to move in the opposite direction.[138/] The rules proposed by the FCC constitute prescriptive, *ex ante* regulation decoupled from consumer harms. The regime is highly detailed procedurally, providing granular directives to companies about how they should communicate with their

---

134/ *See FTC Privacy Report* at 9; Maureen K. Ohlhausen, Commissioner, U.S. Federal Trade Commission, *The Procrustean Problem with Prescriptive Regulation*, Prepared Remarks at the Sixth Annual Telecom Policy Conference, Free State Foundation, at 4-6 (Mar. 18, 2014) ("*Ohlhausen 2014 Remarks*"); Doug Brake, et al*., Broadband Privacy: The Folly of Sector-Specific Regulation*, Information Technology and Innovation Foundation, 1 (Mar. 2016), http://www2.itif.org/2016-broadband-privacy-folly.pdf ("*ITIF Broadband Privacy Report*").

135/ *FTC Privacy Report* at 9; *Protecting Consumer Privacy in an Era of Rapid Change*, Preliminary Staff Report, Federal Trade Commission, at 9 (2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf ("*FTC Preliminary Staff Report*").

136/ *FTC Privacy Report* at 9; *ITIF Broadband Privacy Report* at 11; Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 303 (2011).

137/ *FTC Preliminary Staff Report* at 9.

138/ *See, e.g.*, Jon Leibowitz & Jonathan Nuechterlein, *The New Privacy Cop Patrolling the Internet*, FORTUNE (May 10, 2016), http://fortune.com/2016/05/10/fcc-internet-privacy/ ("The FCC should hold ISPs to the same privacy standards to which the FTC successfully held them for many years—and to which the FTC still holds all other companies. We were disappointed, then, when the FCC recently proposed to subject ISPs to a detailed set of burdensome data-privacy rules with no precedent in the FTC's regime.") ("*The New Privacy Cop*").

customers about privacy, how they should solicit, obtain and document choices exercised by consumers, and how data should be collected and stored.[139/]

This is antithetical not only to the model offered by the FTC, but also to the approach recommended in the 2014 Big Data reports commissioned by the White House. For example, the report from the President's Council of Advisers on Science and Technology recommended that government privacy frameworks avoid compelling particular measures and processes for achieving policy objectives, and should instead broadly articulate the desired outcome without prescribing "how" to attain it.[140/] Neither is it consistent with the framework put forward by the White House, which eschewed the use of prescriptive rules to regulate privacy in favor of flexible standards.[141/]

Not only are there radical conceptual differences between the FTC Framework and the regime proposed in the *Notice*, but the substantive differences between the two approaches are stark[142/]:

First Party-Marketing/Implied Consent. The FTC Framework is predicated upon a pragmatic understanding that many uses of broadband customer data are designed to fulfill or enhance the provision and enjoyment of services and products that online entities make available to their customers. By recognizing that "first party marketing generally does not require choice"

139/ *See NPRM* at ¶¶ 16-23.

140/ *PCAST Big Data Report*, at 49-50.

141/ The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, at 23, 36 (2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf ("*White House Privacy Framework*"); *ITIF Broadband Privacy Report*, at 10-11; Doug Brake, et al*., The FCC's Privacy Foray: Privacy Regulation Under Title II*, Information Technology and Innovation Foundation, 3-5 (Apr. 2015) ("*ITIF CPNI Report*").

142/ *See* Comments of Jon Leibowitz, Former Chairman, Federal Trade Commission, WC Docket No. 16-106, at 6-12 ("Leibowitz Comments").

because it is typically consistent with the context of the provider's relationship with the customer,[143/] the FTC Framework provides online entities with considerable leeway to use customer data to facilitate the provision of service, enhance the customer experience, and market products and offerings of interest to them.[144/] The FCC framework abandons this approach, with little explanation as to why the FTC's treatment of first-party marketing was harmful to consumers or unsuitable for ISPs.[145/] Instead, the FCC regime proposes an extraordinarily narrow set of uses where consent is implied, focused chiefly on the actual provision of broadband service (which is defined very narrowly) and prevention of abusive or unlawful conduct, and permits only first-party marketing of a different level of the same service subscribed to by the consumer.[146/]

Scope of Data Covered. The FCC regime covers a broader scope of data and offers no exception from the permissions regime for data de-identified at the account or customer level. Customer data is subject to the FCC permissions regime if it can be deemed "linked or linkable" to an individual, and broad categories of information are automatically deemed to be CPI (IP addresses, MAC addresses, traffic statistics) irrespective of whether such data are being used in a manner that can reasonably be linked to an identifiable individual.[147/] Further, under the FTC

143/ *FTC Privacy Report*, at 40-44.

144/ *FTC Privacy Report* at 36-44.

145/ Leibowitz Comments at 8 (noting FCC's "baffling departure" from FTC guidance regarding first-party uses of data).

146/ *NPRM* at ¶¶ 112-114, 122.

147/ *Compare NPRM* at ¶¶ 61-62; *FTC Privacy Report*, at 20-22. *See also Internet of Things, Privacy & Security in a Connected World*, FTC Staff Report, January, 2015, at iv ("*FTC Internet of Things Report*") ("[I]f a company collects a consumer's data and de-identifies that data immediately and effectively, it need not offer choices to consumers about this collection").

model, aggregation is just one form of de-identification; in the FCC framework, it is the only form.[148/]

Permissions Regime. The FTC prudently employed an opt-out approach for use of customer data in most instances, requiring opt-in approval only for uses of sensitive data (e.g., health data, Social Security Numbers, and information about children for which opt-in would be required).[149/] Without explaining why the FTC's approach is inappropriate or unworkable for ISPs, the FCC mandates use of an opt-in approval mechanism for virtually all uses of customer data, including many uses which right now are covered by the FTC's exemption from any requirement to offer a choice for first-party uses.[150/] By dictating opt-in for a broad range of data uses which today are either not subject to a choice mechanism at all, or for which most existing broadband customers decline to exercise opt-out rights, the proposal will harm consumers by spawning notice fatigue, sowing consumer confusion (since ISP data use prohibited due to the absence of an opt-in choice will not be restricted anywhere else in the online ecosystem), and reducing consumer welfare by limiting data uses consumers already have shown they prefer.

Competitive Neutrality. The FTC Framework applied uniformly to all entities in the broadband ecosystem. The FTC considered whether large platform providers (including in that group ISPs, browsers, operating systems, and search engines) should be subject to some special set of heightened restrictions, but ultimately declined to recommend any additional

---

148/ *Compare FTC Privacy Report*, at 18-22 *with NPRM* at ¶¶ 74, 165. *See also* Leibowitz Comments at 6 ("[A]ggregation . . . is but one way to de-identify data").

149/ *FTC Privacy Report* at 48-55, 58-60.

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

constraints.[151/] By contrast, the FCC regime abandons the principles of competitive and technological neutrality and instead singles out one subset of large platform providers – ISPs – for privacy requirements that are more stringent and restrictive than those imposed upon any other category of online entity.[152/] As demonstrated below, the perfunctory justifications for such disparate treatment proffered in the *Notice* lack any firm empirical basis and cannot withstand scrutiny.[153/]

Data Security. The FTC's "approach in data security cases is a flexible one."[154/] Companies must provide reasonable data security relative to the sensitivity of the data collected.[155/] The FCC, by contrast, proposes both a general security standard and several specifically delineated data security obligations regardless of the sensitivity of the data collected.[156/]

Publicly Available Information. The FTC Framework calls for greater transparency when companies combine online information about customer behavior with data that is publicly available to all entities in the broadband marketplace from third parties.[157/] In contrast, the FCC proposal contemplates prohibiting ISPs from engaging in such a practice, notwithstanding the absence of any such restraint on other online entities.

The FTC's framework radically departs from the core principles which reflect consensus forged after years of input from a wide range of stakeholders, including consumers, ISPs, edge

---

151/ *FTC Privacy Report* at 55-57.

152/ *NPRM* at ¶ 4.

153/ *See infra* § II.B.

154/ *FTC Privacy Report* at 21, n. 108.

155/ *FTC Privacy Report* at 24-32.

156/ *NPRM* at ¶¶ 170-255. *See infra* § II.E.

157/ *FTC Privacy Report* at 46.

providers, advertisers, privacy advocates, academics and social scientists. That departure threatens to harm consumers because, as FTC Commissioner Ohlhausen notes, by "set[ting] the privacy baseline too high, the privacy preferences of the few are imposed on the many."[158/] By taking a dramatically different approach than the FTC, the FCC imposes an asymmetrical regulatory framework that will regulate a particular set of entities in the Internet ecosystem differently from the vast majority of online entities that collect, use, and share consumers' online information. Given the substantial success of the FTC Framework in balancing the broad array of interests at stake here, it is incumbent upon the Commission to clearly call out – and justify – its departures from the FTC's framework. The *Notice* fails to do that.

B. The Arguments Set Forth For Subjecting ISPs to a More Stringent Set of Rules Are Unsound and Unsupported by Empirical Evidence

In contrast to unproven assertions in the *Notice*,[159/] ISPs do not have more visibility over broadband consumer data than others in the Internet ecosystem. The types of broadband customer and usage information implicated by the Commission's proposed rules are hardly unique to ISPs. Other broadband entities, including search engines, browsers, operating systems and content providers, may have even more comprehensive access to broadband consumer network usage data, by virtue of the fact that they interact with users across multiple broadband platforms and providers.[160/] The Electronic Privacy Information Center (EPIC) has criticized the proposal's "narrow focus on ISPs," noting that "many of the largest email, search, and social

---

158/ *Ohlhausen 2016 Remarks*, *supra* n. 133, at 4.

159/ *NPRM* at ¶ 4.

160/ *See Swire Paper*, *supra* n. 98, at 7, 23-35 (showing that "ISP access to user data is not unique – other companies often have access to more information and a wider range of user information than ISPs.").

media companies exceed the scope and data collection activities of the ISPs."[161/] The FTC recognized this as well in crafting its framework, noting that "ISPs are just one type of large platform provider" and "operating systems and browsers may be in a position to track all, or virtually all, of a consumer's online activity to create highly detailed profiles."[162/]

As Professor Peter Swire has demonstrated, ISP visibility of broadband customer data is not greater than that of other broadband entities, and is in fact rapidly diminishing. ISPs do not see nearly as much data about their subscribers' Internet activity as the FCC assumes,[163/] nor is the data that they do see unique or uniquely concerning. Changes in technology and consumer behavior over the last 20 years have severely decreased the amount of information about subscribers' online activity available to ISPs.[164/] Broadband subscribers are likely to access the Internet from multiple devices over several ISPs – one in the home, one at the office, several at WiFi hotspots, and more through mobile devices such as mobile phones and tablets – meaning that no single ISP has comprehensive access to its subscribers' online activity.[165/]

Technology also has changed such that pervasive encryption and increasing use of proxy services have limited the ability of ISPs to actually "see" the data they carry. The widely used HTTPS encryption standard blocks ISPs from seeing the full detailed URL[166/] and content of websites visited by their subscribers.[167/] And this encryption standard has been increasing in use

---

161/ Memorandum, *FCC Communications Privacy Rulemaking*, EPIC, 1 (Mar. 18, 2016), *available at* https://epic.org/privacy/consumer/EPIC-Draft-FCC-Privacy-Rules.pdf ("*EPIC Memorandum*")

162/ *FTC Privacy Report* at 56.

163/ *See ITIF Broadband Privacy Report* at 8-10.

164/ *Swire Paper* at 7, 23-35.

165/ *Swire Paper* at 24-25; *ITIF Broadband Privacy Report* at 10.

166/ *I.e.*, the subpage that a subscriber is visiting (for example, what comes after the ".com/"). HTTPS still gives ISPs access to the host name of the websites visited (what comes before the ".com").

167/ *Swire Paper* at 26; *ITIF Broadband Privacy Report* at 9.

– going from 13% of Internet traffic in 2014 to 49% by 2016 and expected to outpace unencrypted HTTP traffic this year.[168/] All told, the percentage of Internet traffic employing some form of encryption is expected to reach 70% by the end of this year.[169/] As Swire concludes, "For all of the encrypted links and content, ISPs are technically blocked from seeing user data." Similarly, increasing use of proxy services, such as Virtual Private Networks (VPNs), go a step further than even HTTPS and eliminate ISPs' ability to see even the host name[170/] of the websites their subscribers' visit.[171/] As of 2014, 30 million Americans used a proxy service and that number has likely been climbing, as major third parties such as Google have introduced free proxy servers and encouraged their users to activate those services.[172/]

Chairman Wheeler suggests that "even when data is encrypted," ISPs can piece together significant amounts of information.[173/] While ISPs still receive some information about the websites their customers visit even when encryption is employed,[174/] that information can be difficult to parse.[175/] A "typical web page entails 40 different IP addresses" with no readily

---

168/ *Swire Paper* at 3, 28. This increase contrasts with the study's authors earlier concerns "that pervasive encryption was developing but was not yet in place in 2012, the year when the FTC Privacy Report stated that ISPs could develop "comprehensive profiles" of their customers." *Swire Paper* at 30.

169/ *Swire Paper* at 3.

170/ *See supra*, n. 166.

171/ *Swire Paper* at 30; *ITIF Broadband Privacy Report* at 9.

172/ *Swire Paper* at 34. In addition to Google, Facebook purchased a proxy service for mobile devices. *Id.* at 35.

173/ Statement of Chairman Tom Wheeler, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* WC Docket No. 16-106, Notice of Proposed Rulemaking, FCC 16-39 (2016).

174/ Encryption can be performed at other layers in the stack and can obscure both content payload and metadata. Work is underway at the IETF to add encryption support to additional Internet control protocols, such as domain name system and time.

175/ Richard Bennett, *FCC Confused about Privacy*, High Tech Forum, http://hightechforum.org/fcc-confused-about-privacy.

apparent means of ascertaining which reflect user activity and which represent ad networks or other third-party service providers.[176/]

Browsers, search engines and social media are in a much better position to create comprehensive views of Internet users' activities.[177/] ISPs' increasingly limited view contrasts sharply with the increasingly extensive view of customer data that is available to edge providers with a substantial ability to track users across devices.[178/] For example, 92 of the 100 most popular websites contain Google tracking infrastructure and a user visiting those 100 most popular sites would collect over 6,000 cookies, granting edge providers significant ability to track users across websites.[179/] And large edge providers are also in a better position than ISPs to track users across devices, whether through users logging in to a service on several devices or through probabilistic tracking that uses data analytics to assess the probability that a device belongs to a particular user.[180/]

176/ *Id.*

177/ Timothy Libert, *Exploring the Hidden Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites*, International Journal of Communications 9 (2015), at 2 http://ijoc.org/index.php/ijoc/article/view/3646/1503 ("Although many companies track users online, the overall landscape is highly consolidated, with the top corporation, Google, tracking users on nearly 8 of 10 sites in the Alexa top 1 million").

178/ *Swire Paper* at 116-118.

179/ Ibrahim Altaweel, Web Privacy Census, Presentation at PrivacyCon, Federal Trade Commission, at 11, 15 (Jan. 14, 2016), https://www.ftc.gov/system/files/documents/videos/privacycon-part-1/part_1_privacycon_slides.pdf; *see also* J. Howard Beales & Jeffrey A. Eisenach, *Putting Consumers First: A Functionality-Based Approach to Online Privacy*, NAVIGANT ECONOMICS, 19 (Jan. 2013) ("75 percent of the top 1,000 web sites include code from one or more social networks.") .

180/ *Swire Paper* at 116-118. Google also is entering the home network space, offering its "Google OnHub" wireless router which could provide it with additional visibility into customer device types and usage activity. *See e.g.* "Google Appeases Privacy Hounds by Detailing OnHub Router Data Collection Routines and Opt-Out Procedures," HotHardware, August 21, 2015, http://hothardware.com/news/google-appeases-privacy-hounds-by-onhub-router-data-collection-routines-and-opt-out-procedures ("[I]f you use the OnHub, you're sharing information about your online activities with a device designed by one of the most data-hungry companies in the world"); "Google details OnHub data collection and opt-out instructions," TechReport August 20, 2015, http://techreport.com/news/28872/google-details-onhub-data-collection-and-opt-out-instructions (Noting

Not only do ISPs lack a unique view of consumer online activity, they have not been a significant – or even a minor – source of misconduct with regard to the broadband customer data they do have. ISPs' track record with respect to their privacy and data use practices does not warrant imposition of a special set of rules that differ from those applicable to others in the broadband ecosystem. As EPIC noted,

> 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.[181/]

Indeed, while the FTC has brought privacy enforcement actions several edge providers, including Google, Facebook and Twitter,[182/] there have been relatively few actions brought against ISPs, particularly in recent years.

There is no evidence that consumers are clamoring for a new and different set of privacy rules for ISPs or that ISP privacy practices pre-reclassification inflicted harms which necessitate the establishment of a new privacy regime that is radically different from the FTC Framework.

---

that information collected and used by OnHub's associated cloud services includes "data usage statistics, and some information about nearby networks, like access points' network names, MAC addresses, supported wireless standards, and channel usage").

181/ *EPIC Memorandum, supra* n. 161, at 1.

182/ *E.g.*, Press Release, Fed. Trade Comm'n, *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser* (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented; Press Release, Fed. Trade Comm'n, *Facebook Settles FTC Charges That It Deceived Consumers by Failing To Keep Privacy Promises* (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep; Press Release, Fed. Trade Comm'n, *Twitter Settles Charges that it Failed to Protect Consumers' Personal Information; Company Will Establish Independently Audited Information Security Program* (June 24, 2010), https://www.ftc.gov/news-events/press-releases/2010/06/twitter-settles-charges-it-failed-protect-consumers-personal.

In fact, studies show that consumers trust their ISP more than edge providers to protect the privacy and security of their data.[183/] One study from the Pew Research Center found that trust levels with respect to safeguarding consumers' personal data are more than twice as high for ISPs than for online entities such as search engines, social media platforms, online video sites and online advertisers.[184/] Other studies likewise found that consumers trust their ISPs to protect their data significantly more than many other entities in the Internet ecosystem.[185/] NTIA's 2014 Digital Nation report states that "only 1 percent of households expressed privacy concerns . . . as their primary reason for not using the Internet at home."[186/]

ISPs have a built-in incentive to respect the privacy of their subscribers given their ongoing business relationship. This relationship strengthens incentives to win and retain consumers' trust by appropriately safeguarding their privacy. Indeed, the FCC explicitly recognized in its CPNI Orders that communications service providers in direct privity with end users are more trustworthy data custodians than third parties due to the ongoing customer-carrier

---

183/ *See* Pew Research Center, *American Attitudes about Privacy, Security and Surveillance*, 7 (May 20, 2015), *available at* http://www.pewinternet.org/files/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf (finding that edge providers "are among the least trusted entities when it comes to keeping information private and secure" with consumers rating cable and telephone companies as more trustworthy than most edge providers) ("*Pew Study*"); *See ITIF Broadband Privacy Report*, *supra* n. 134, at 4-5 *citing* TRUSTe and Harris Interactive, "2011 Consumer Research Results Privacy and Online Behavioral Advertising," (July 25, 2011) (after themselves, people expressed more trust in ISPs to protect their privacy than any other entity or regime, including government regulation, search engines, and browsers).

184/ *Pew Study* at 7.

185/ *Perceptions of Privacy Online and In the Digitally Connected World*, NATIONAL CYBER SECURITY ALLIANCE, at 5 (Jan. 28, 2015); *Consumer Privacy: What are Consumers Willing to Share*, PRICEWATERHOUSECOOPERS, at 9 (2012); Matthew Quint & David Rogers, *What is the Future of Data Sharing: Consumer Mindsets and the Power of Brands*, COLUMBIA BUSINESS SCHOOL & AIMIA, at 12 (Oct. 2015).

186/ U.S. Dep't of Commerce, Nat'l Telecomms. & Info. Admin., *Exploring the Digital Nation: Embracing the Mobile Internet*, 37 (Oct. 2014), https://www.ntia.doc.gov/files/ntia/publications/exploring_the_digital_nation_embracing_the_mobile_internet_10162014.pdf ("*Exploring the Digital Nation*")

relationship.[187/] These incentives have led most ISPs to incorporate "privacy by design" into their everyday business practices and consider privacy at all stages of the development of any product or service that involves the collection or use of customer data.[188/]

Finally, the putative switching problem identified by the Commission does not justify differential treatment.[189/] Broadband customers utilize multiple paths to the Internet and enjoy competitive choices.[190/] Any switching constraints that may exist for broadband service are no worse – and in several respects are less severe – than switching constraints for core edge offerings: Google has 70% of the search market,[191/] 60% of the mobile OS market,[192/] and is the largest advertiser[193/] and second largest browser provider,[194/] while Facebook has over 60% of social media log-ins.[195/]

187/ *2002 CPNI Order* at ¶¶ 37, 51 (finding that "[the] likelihood of any potential privacy harm from an inadvertent approval under opt-out is significantly reduced in the intra-company context by the carrier's need for a continuing relationship with the customer… whereas "third parties have no incentive to honor the privacy expectations of customers with whom they have no relationship.").

188/ *See* Comments of NCTA, *Information Privacy and Innovation in the Internet Economy*, Docket No. 101214614–0614–01, Nat'l Telecomms. & Info. Admin., at 16 (filed Jan. 28, 2011).

189/ *See NPRM* at ¶¶ 4, 33.

190/ *See, Swire Paper*, *supra* n. 98.

191/ NETMARKETSHARE, Desktop Search Engine Market Share (April 2016), https://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0.

192/ NETMARKETSHARE, Mobile/Tablet Operating System Market Share (April 2016), https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=1; *see also* Vindu Goel, *Making the Move to iPhone From Android*, NEW YORK TIMES, B8 (Apr. 7, 2016) (describing the difficulty of switching mobile phones, operating systems, and apps and concluding that "given the headaches of switching, most people avoid it.").

193/ AOL*, Millennial Face Uphill Battle to Capture Mobile Ad Dollars* (Sep. 8, 2015), http://www.emarketer.com/article.aspx?R=1012954.

194/ NETMARKETSHARE, Desktop Browser Market Share (April 2016), https://www.netmarketshare.com/browser-market-share.aspx?qprid=0&qpcustomd=0.

195/ Frederic Lardinois, *Facebook Continues To Dominate Social Logins, Expands Lead To 61% Market Share*, TechCrunch (Jan. 27, 2015), http://techcrunch.com/2015/01/27/facebook-dominates-social-logins/.

Imposing new privacy and security rules under Section 222 that focus only on ISPs would address the issue of broadband privacy in an asymmetrical and under-inclusive way. ISPs should not be subject to more granular regulation or more stringent restrictions than all other broadband entities that collect and use the same type of data from broadband consumers, particularly when there is no sound basis for such differential treatment.

C. The Proposed Rules Will Fail to Incrementally Improve Privacy Protection, Cause Consumer Confusion, Reduce Consumer Welfare, and Thwart Competition and Innovation

Consumers experience broadband Internet service as an integrated whole. Under the FCC's proposed rules, however, broadband consumers will have one set of privacy rights that apply to how their data is handled by their Internet access providers, and then an entirely different set of rights that apply when the exact same data is handled by anyone else in the broadband ecosystem. Data associated with sending an email, requesting a Web page, entering a search request, receiving a marketing offer or an advertisement, or engaging in other common Internet activities will be subject to materially different legal and regulatory regimes during the milliseconds in which such transmissions are initiated, transmitted, processed and responded to – depending upon the identity of the entity handling such data.[196/] Consumers do not want – nor do they benefit from – substantial differences in privacy regulation between different parts of what they regard as an integrated Internet experience.[197/] The increased customer confusion arising from asymmetric regulation will lead to less use of the Internet, not more.

196/ *E.g.*, *NPRM* at ¶¶ 132, 206.

197/ *See* Comments of Progressive Policy Institute, WC Docket No. 16-106, at 1 (citing recent survey of Internet users by Public Opinion Strategies and Peter D. Hart showing that: "By an overwhelming margin, 94% v 5%, Internet users agree that 'All companies collecting data online should follow the same consumer privacy rules so that consumers can be assured that their personal data is protected regardless of the company that collects or uses it'").

The NPRM fails to explain why consumers consider such divergence to be necessary or desirable. Despite the very real possibility of consumer harm due to confusion, frustration, and more complicated privacy disclosures, the NPRM fails to cite any empirical evidence to support the notion that consumers believe there should be different privacy and data protection regimes depending upon whether their data is used by an ISP rather than by a search engine, Web site, app provider, or any of the advertising, analytics or other third party entities working with such edge providers.

The upshot of the asymmetry embraced by the Commission is that the granularity and burdens of its proposed regime will not materially improve privacy, because every other entity in the ecosystem with access to the same data as ISPs will be subject to less stringent restrictions on their use of such data. The end result will be increased regulatory burdens and costs and greater consumer confusion - with no material improvement in privacy.[198/]

Consumers do not expect their basic privacy protections will vary substantially based on the type of broadband entity they are interacting with at any particular time. Many consumers may erroneously believe that an opt-out choice made with their ISP will apply across the Internet, and, perversely, may be more willing to share information with third parties believing that such disclosures would be protected by the privacy choices made with their ISP. This will lead to confusion and frustration when, for example, they continue to receive targeted ads from

---

198/ *See* Leibowitz & Neuchterlein,*The New Privacy Cop*, *supra* n. 138 ("Ironically, the proposed rules would do very little to promote the cause of "privacy" in the first place. If they are adopted, all other participants in the Internet ecosystem will remain exempt, will continue collecting all of the same information that the ISPs would have collected, and may continue selling the same information as before to the same data brokers. The Big Data marketplace will carry on—except, ironically, the FCC will have insulated its largest players from ISP competition. Meanwhile, the rules would simply confuse all but the savviest consumers about what data is, and is not, subject to collection and use.").

third-party networks.[199/] Explaining the difference between the privacy rules applicable to ISPs and those applicable to edge providers, and the very limited part of their interaction with the Internet that is covered by their ISP's privacy notice, will require even longer and more detailed privacy disclosures. Indeed, while the NPRM suggests that privacy notices should be simplified and standardized to make them "more accessible to consumers,"[200/] the regulatory asymmetry created by the Commission's regime is likely to make privacy notices more complex and confusing.

While failing to incrementally enhance privacy protection and sowing increased confusion, the regime proposed in the *Notice* also will decrease consumer welfare. The dynamism of the broadband marketplace stems from the personalized offerings available to broadband users from a vast array of companies providing broadband-related content, products, services, apps, and tools.[201/] Across the Internet ecosystem, companies such as Facebook, Amazon, Netflix, and countless others have relied upon data-driven customization and

---

199/ *E.g.*, Rosa Mendoza, "The FCC's consumer privacy order could lead to consumer confusion," Hispanic Telecommunications and Technology Partnership, March 29, 2016, http://httponline.org/2016/03/the-fccs-consumer-privacy-order-could-lead-to-consumer-confusion/, (By writing "rules only for ISP [and] exempting online entities such as Facebook and Google that keep a much deeper, richer profile of online activity, the FCC risks consumer confusion and regulating the industry in an unbalanced way").

200/ *NPRM* at ¶¶ 90-95.

201/ *See e.g.*, Liraz Margalit, "The Psychology of Online Customization," *Tech Crunch*, Nov. 11, 2014, http://techcrunch.com/2014/11/11/the-rise-of-online-customization/ (Customization has become increasingly significant to brand-name companies because it's now part of a broader trend that shifts from viewing customers as recipients of value to co-creators of value. Rather than being passive, the customer is now becoming a part of the "product development" process"); Bain Insights, Having It Their Way: The Big Opportunity in Personalized Products, FORBES, November 5, 2013, http://www.forbes.com/sites/baininsights/2013/11/05/having-it-their-way-the-big-opportunity-in-personalized-products/#2ba26d970363 ("[T]those customers who had customized a product online engaged more with the company. They visited its website more frequently, stayed on the page longer and were more loyal to the brand. Equally, customization helps companies differentiate their products from those of their competitors at a time when the Internet is rapidly making it easier for customers to compare the prices of products with standard features. Customization helps companies gain insights from customized designs and fine-tune products to stay one step ahead of the competition").

personalization in order to grow their businesses, expand their service offerings and retain and strengthen their relationships with their customers. By imposing highly prescriptive restrictions on broadband service providers, the Commission's rules will reduce opportunities for consumers to benefit from customized offerings and services while raising their costs.[202/] Remarkably, however, the Commission appears to have engaged in no cost-benefit analysis with respect to the impact of its regime on consumer welfare, or with regard to the utility of its specific – and material – departures from the FTC Framework.

Both the White House and PCAST Big Data Reports acknowledge the substantial consumer benefits associated with Big Data, including greater customization of products and services, the subsidization of Internet content and capabilities, new offerings, and improvements in fraud detection, health care delivery, and automated conveniences.[203/] The behavior of consumers demonstrates their support for having Internet graphics, capabilities, and content subsidized by relevant advertising and marketing messages and enhanced by analysis of – and responsiveness to – their interests and preferences.[204/] The rigid permissions regime proposed in the *Notice*, which prophylactically restricts data uses and analytics employed today by broadband providers (and a host of other Internet entities) that improve service quality, enhance the customer experience, and promote awareness and consumption of new products and services, is fundamentally incompatible with data-driven growth, investment and innovation. Making it

---

202/ *ITIF Broadband Privacy Report* at 7 ("[T]he rigidity of up-front regulation – as opposed to a more FTC harms-based approach – will slow new services that depend on data").

203/ *White House Big Data Report* at 5, 39, 58; *PCAST Big Data Report*, at 49-50. *See also See Fact Sheet: U.S. Consumers Want More Personalized Retail Experience and Control Over Personal Information, Accenture Survey Shows*, Accenture(Mar. 2015), https://www.accenture.com/us-en/~/media/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_10/Accenture-Retail-Personalization-Survey-Fact-Sheet-March-2015.pdf.

204/ *See supra* n. 129.

harder and more expensive for ISPs to offer data-driven services, capabilities, advertising and marketing will worsen, rather than improve, consumers' broadband experience.[205/]

The proposed rules also will harm consumer welfare by engendering reductions in investment, innovation and competition due to the significant disparities in privacy and data use burdens for ISPs compared to everyone else in the ecosystem. By burdening broadband providers, the rules will slow broadband deployment and increase costs for consumers.[206/] While a unified privacy framework provides a level playing field for all participants in the broadband marketplace and enables all companies to have the same opportunity to utilize data in ways that improve the products and services they offer, the asymmetry embraced in the *Notice* will distort competition and lead to marketplace outcomes dictated by regulatory disparities rather than market forces and consumer preferences.[207/] There is no evidence to suggest that consumers are willing to endure less relevant advertising and marketing messages, and higher-priced broadband service, in exchange for one-sided privacy rules that apply only to ISPs.

205/ *See ITIF CPNI Report*, at 3 ("this is not a zero-sum game… with carriers getting all the benefits of being able to use data and consumers getting none. In fact, consumers can get direct benefits through lower priced and more customized offerings, and society in general benefits from greater levels of efficiency in advertising."); *Ohlhausen 2016 Remarks*, at 8 (FTC framework sets a baseline by prohibiting practices the vast majority of consumers would not embrace. *Mandating* practices above this baseline reduces consumer welfare because it denies some consumers options that best match their preferences") (emphasis in original).

206/ *ITIF Broadband Privacy Report* at 13 (rules that depart from the FTC framework "would reduce the efficiency of the broadband industry, with resultant loss of broadband network investment and higher prices for broadband consumers").

207/ *See e.g., ITIF Broadband Privacy Report* at 3("[I]f the FCC treats broadband providers as fundamentally different from other Internet actors, it would disrupt a nascent area of competition in the Internet ecosystem; government would be putting its thumb on the scale"). *See also* Leibowitz & Neuchterlein, *The New Privacy Cop*, *supra* n. 138 ("The rules would further subject all ISPs—and ISPs alone—to unprecedented compliance costs and keep them from efficiently monetizing online data in the same way that Google and Facebook have long done, with astounding consumer benefits. Such restrictions would exert upward pressure on broadband prices and undercut the FCC's central mission of promoting broadband investment and adoption.").

To the extent that other online entities depend upon ISPs for access to data elements now miscast as CPI by the Commission's proposal in order to fulfill broadband customer requests for content and services, the proposed regime will severely disrupt these arrangements and introduce considerable friction that will make it much harder for ISPs and edge entities to work together to meet consumer needs.[208/] Edge providers themselves have expressed concern that, even though the proposed rules would apply only to ISPs, the conflicting requirements of the different privacy regimes will create unwanted and adverse downstream effects that could slow their innovation.[209/] As the Information Accountability Foundation states: "It seems to us that the proposed rulemaking that impacts one player creates a very awkward governance system and that awkwardness overshadows the entire ecosystem."[210/]

The default opt-in regime proposed by the Commission also will inhibit the emergence of new competition in the online advertising market, which is already dominated by a handful of large edge providers.[211/] Tying the hands of ISPs will eliminate one of the most plausible

---

208/ *See ITIF Broadband Report* at 10 ("Treating broadband providers as fundamentally different from other online actors would harm, not help, the Internet ecosystem."). The FTC Framework was much less prone to creating unwanted friction in the ecosystem because (i) the metadata elements involved did not, on their own, automatically constitute CPI, as is the case under the FCC proposal (ii) the context of the transaction with the consumer was understood as conceptually broader than the narrow definition of broadband Internet access service established in the *Open Internet Order* and relied upon in the *NPRM* and/or (iii) the metadata use at issue was at most subject to an opt-out approval mechanism.

209/ *See, e.g.*, Notice of Ex Parte Communication, ACT: The App Association, WC Docket No. 16-106, at 3 (filed Apr. 22, 2016) ("[T]he Commission's proposal to require an opt-in approach for uses of data that have traditionally been permitted under the FTC with an opt-out model could create inconsistent federal agency approaches to the same data, confusing consumers and presenting conflicting requirements that will flow through the Internet ecosystem and disrupt the vibrant app economy, both within the United States and globally").

210/ Comments of Information Accountability Foundation, WC Docket No. 16-106, at 4.

211/ AOL*, Millennial Face Uphill Battle to Capture Mobile Ad Dollars* (Sep. 8, 2015), http://www.emarketer.com/article.aspx?R=1012954. ([I]n 2016, Facebook and Google are expected to comprise over 50% of U.S. digital ad revenues, with the top ten companies, all edge providers, combining for 70% of revenues).

sources of competition for large digital advertisers,[212/] and thereby inhibit the emergence of competition that could lower costs for consumers.

D. The Scope of Data Covered by the Proposal is Overbroad and the Permissions Regime is Overly Restrictive

1. The Scope of Data Included as CPI and Subject to the Permissions Regime Is Far Too Broad

Use or Disclosure of CPI Should Be Subject to the Permissions Regime Only When Used or Disclosed in Combination With Individually Identifiable Data. Each of the several categories of data proposed as broadband service CPNI (as well as many of the data items proposed as PII) cannot, by themselves, identify any specific individual.[213/] For example, the *Notice* proposes to identify broadband service plan and traffic statistics data as CPNI, even though there is no way to identify a subscriber simply by knowing, in isolation, that he or she subscribes to 50Mbps Internet service or consumes a particular number of bytes per month.[214/] The *Notice*, however, fails to make clear that these items can be considered CPNI subject to the permissions regime only if they are combined with individually identifiable information.[215/] Instead, it leaves the impression that any one of the CPNI data categories enumerated in the

---

212/ *See e.g., FCC Internet privacy proposal could harm broadband providers - Moody's*, Reuters (Mar. 15, 2016), *available at* http://www.reuters.com/article/usa-fcc-internet-moodys-idUSL2N16N19H ("Moody's said Internet providers could be 'severely handicapped' in their ability to compete with digital advertisers such as Facebook Inc. and Google").

213/ *See NPRM* at ¶ 41 (e.g. service plan information, traffic statistics, IP addresses, MAC addresses, and device identifiers).

214/ *See NPRM* at ¶¶ 42, 47.

215/ There is no indication that the "linked or linkable" standard for PII, *see NPRM* at ¶ 62 (which is itself vague and overbroad and could still encompass information that cannot plausibly be used to identify an individual) qualifies or limits the circumstances in which an item of data identified as CPNI is subject to the permissions regime. *See NPRM* at ¶¶ 41-47. It is likewise unclear whether that standard qualifies or limits the circumstances in which data items specified in the *Notice* as PII would be covered by the permissions regime. *See NPRM* at ¶ 62 (listing "the types of data that are PII"). *See infra* at text accompanying notes 243-249.

NPRM, on its own and without any additional identifying information, is subject to the permissions regime.

This omission is noteworthy because Section 222(c) makes clear that use restrictions may only be imposed on "individually identifiable" CPNI.[216/] Thus, to the extent that any of the data categories in the NPRM proposed as CPNI – whether gathered or maintained at the customer, account, or aggregate level - are not combined with information that identifies a specific individual, there is, as a policy matter, no reason to restrict their use and, as a legal matter, no authority to do so.[217/] Any Commission conclusion to the contrary would be erroneous and could lead to absurd results.

For example, as noted, IP address ranges assigned to ISPs are published by ARIN.[218/] Not only would treating IP addresses, on their own, as CPI preclude such publication absent opt-in approval,[219/] it also would potentially interfere with implementation of CSRIC III recommendations relating to Border Gateway Protocol (BGP).[220/] CSRIC III's Working Group 6 BGP noted that "all techniques for improving the security of inter-domain routing rely on authoritative, accurate, and timely information about which [network operators] are authorized to

---

216/ 47 U.S.C. § 222(c).

217/ *See supra* § I.C.

218/ *See supra* § I.C.2.

219/ Such an outcome, however, would appear to be contrary to Congressional intent, however. H.R. Rep. No. 104-204, 104th Cong., 1st Sess., at 90 (1995)("[A] carrier is not required to obtain the approval of customers to use customers to use customer information in the provision of . . . services . . . such as the publishing of directories").

220/ BGP is the protocol utilized to prevent Internet route hijacking and identify the best available paths for packets to take between points on the Internet at any given moment. Technical Appendix, at 4, 31.

originate routes for each IP address block."[221/] IP address blocks can be as granular as a single IP address, so the restriction against use or disclosure of IP addresses could interfere with the IP address publishing and updating activities required to implement this recommendation. In a similar vein, the Internet Engineering Task Force (IETF) considers "DNS data and the results of a DNS query" obtained by or initiated from an ISP's end user to be "public."[222/] The Commission should consider whether its proposed treatment of DNS information as CPI would disrupt DNS-related expectations and data flows in the Internet ecosystem.[223/]

Likewise, the proposal to include "geo-location" data as both CPNI and PII is vague and overbroad.[224/] The *Notice's* failure to provide any detail regarding the granularity of location information that would fall within the definition of "geo-location" subject to the proposed rules potentially renders ISP server location inclusion in the ARIN registry of IP addresses, and made available via whois.net, as impermissible disclosures of CPNI.[225/] For example, ISP authentication of a customer's entitlement to OTT content offered by that provider (or through the provider in conjunction with a content partner) might depend upon the location of the

---

221/ The Communications Security, Reliability and Interoperability Council IV Working Group 6 Final Report, *Secure BGP Deployment*, at 4 (March 2013), http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG6_Report_March_%202013.pdf.

222/ "DNS Privacy Considerations," Internet Engineering Task Force, August 2015, at 5. Basic Internet functionality depends upon a set of complex routing protocols and host name resolution protocols that translate Website queries typed by Internet users into their numerical IP address on the network to ensure proper routing. The network relies on IP address and DNS protocol data to keep routing tables accurate and up to date, and in some instances to resolve the host name request from computers. *See* Technical Appendix, at 19-23.

223/ There is also a potential competitive impact that should be considered by the Commission, since third-party DNS services such as those offered by Google, *see e.g.,* Swire Paper at 34; *Open Internet Order* at ¶ 370, would be exempt from the constraints on DNS look-up potentially imposed by the Commission's proposed privacy rules for ISPs.

224/ *NPRM* at ¶ 43.

225/ Location data made available via whois.net is used for a variety of purposes including investigating SPAM, incident response, contacting network administrators, and obtaining the location of and contact information for businesses for common commercial purposes. Technical Appendix at 21-22.

customer.[226/] ISPs should not be required to solicit customer approval in order to ensure that content the customer wishes to receive via a broadband transmission is furnished consistent with any applicable geographic restrictions.

Use Cases. There is no logical rationale for automatically treating IP addresses, MAC IDs and other device identifiers, domain information, location information, and service plan and traffic statistics data as CPNI since such items are generally decoupled from information that defines a specific person.[227/] For example, IP addresses, device identifiers or other data elements subject to the rules may be used by broadband providers to facilitate email traffic routing; undertake DNS look-up (forward and reverse); manage the network and the functionality and services thereon; provide cloud storage and retrieval services; assess network usage patterns; inform caching decisions; operate and execute parental controls and content filters requested by customers; load third-party apps and tools associated with a subscriber's preferred landing page; investigate or research potential security concerns in conjunction with third-party security and tool vendors and academic researchers; and assist in measuring the performance of advertising and marketing campaigns.[228/] In each of these instances, the broadband provider has no interest in, or need for, the actual identity of the person associated with the IP address or other data

---

226/ Netflix today restricts content to certain geographies given its content rights.

227/ *See supra* § I.C.2. *See also* NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, § 3.3.2 (2010)("*NIST Guide to Protecting PII*") (IP address + URL information, without more, is not "directly identifiable data."); "Are IP Addresses Personal," Google Public Policy Blog, Feb. 22, 2008 ("A black-and-white declaration that all IP addresses are always personal data incorrectly suggests that every IP address can be associated with a specific individual. . . The reality is though that in most cases, an IP address without additional information cannot [identify you]"); Office of Privacy Commissioner of Canada, Interpretation Bulletin, Dec. 11, 2015 (IP address "can be considered personal information if it can be associated with an identifiable individual")(emphasis added); *Pruitt*, *supra* n. 64, 100 Fed. Appx. at 716 (Agreeing that device ID number "without more - provides nothing but a set of numbers" and that "[w]ithout the information in the billing or management system one cannot connect the unit address with a specific customer").

228/ *See generally* Technical Appendix.

elements being used to facilitate these basic functions. Yet under the Commission's proposed regime, each of these uses would need to be assessed against the application of the permissions regime and some, if not all, could require opt-in consent. This is a sea change from the *status quo*, and would likely result in considerable disruption of current practices and capabilities, notice fatigue and consumer frustration.[229/]

As explained in the attached Technical Appendix,[230/] the breadth of data subject to the proposed permissions regime could significantly interfere with common practices and customer expectations, including

Email transmissions to and from ISP email accounts. In accordance with the SMTP protocol, ISPs and other email providers may append IP addresses associated with end points or devices to email headers in order to facilitate proper routing, assist with trouble-shooting, or mitigate spam and junk mail.[231/] All emails include IP addresses of the end points or devices in the header's "Received:" field, and most also include an IP address for the end point or device in the "X-Originating-IP" field. Under the *Open Internet Order*, email service is expressly separate from broadband Internet access service.[232/] Thus, if IP addresses are considered CPNI, the broadband provider's disclosures of IP addresses attendant to transmission of an email to or from an ISP email account holder would need to be assessed against the permissions regime, for each potential use and disclosure of the IP addresses associated with the sender or recipient's end points/devices sending or receiving an email transmission.[233/] Not only would that be impractical, it also could disadvantage ISP-provided email service relative to third-party email providers, which would harm both consumers and competition.

229/ *See* Leibowitz Comments at 6 (noting that over a fifteen month period, FTC staff "conducted extensive 'stress testing'. . . to test the proposed rules against specific use cases in order to determine whether the desired outcome was achieved. As a result of these meetings, changes were made to account for normal business operations and to encourage innovation in new products and services. Similarly the FCC should conduct meetings to fully understand the effects of its proposed requirements before potentially causing disruption to an entire industry and the Internet ecosystem.").

230/ *See* Technical Appendix at 11-37.

231/ *See* Technical Appendix at 11-14.

232/ *Open Internet Order* at 5757-58, ¶ 356.

233/ As part of the process for sending email, the sending email server queries the receiving server to ask if an email address exists. The receiving server would then disclose the email address, which is CPI, to the sending server.

DNS look-up. The Open Internet Order makes clear that broadband providers' DNS look-up capabilities are separate from broadband Internet access service,[234/] and hence IP address and other CPI uses or disclosures associated with DNS look-up would not be covered by the proposed exception for "provision of BIAS."[235/] Under RFC 1011,[236/] a network operator is supposed to populate the DNS server with the hostname and associated IP address for each endpoint on their network to facilitate look-up by others. Moreover, to facilitate routing and optimize service from authoritative servers, the IETF has been developing a DNS update that will include the IP address information associated with the originating domain query, but the Commission's proposal could scuttle this upgrade.[237/]

IPv6. The NPRM proposes that MAC addresses should be viewed as CPNI and PII and therefore require a customer's consent prior to their disclosure to third parties. IPv6 was designed to re-emphasize the end-to-end principles of the Internet and enable each device on the network to have a unique address globally reachable from any other location on the Internet. This objective led to IPv6's reliance on including a device's MAC ID number as part of the unique IP address assigned pursuant to IPv6 protocols. Thus, even in circumstances where disclosure of an IP address might be permitted under an exception to the Commission's rules, broadband providers might still be unable to take advantage of that exception due to the inclusion of the MAC ID in the IPv6 address.[238/]

Authenticating or delivering products and services offered by ISPs with affiliates or third-party partners. ISPs that provide online products or services to their customers (either on their own or in conjunction with affiliates or third-party partners) may use or disclose to those affiliates' or partners' IP addresses in order to deliver such offerings to specific Internet endpoints or rely upon subscriber log-in credentials for authentication purposes. These offerings might include anything from music and other content, software, home security and energy management systems, Internet of Things devices, and other products and services capable of being provisioned over the Internet. [239/] Under the Commission's proposed permissions regime, such uses or disclosures could be subject to customer approval, notwithstanding the fact that the customer already has assented to the receipt of such products or services.[240/]

234/ *Open Internet Order* at 5765-70, ¶ 366-71.

235/ *NPRM* at ¶ 113.

236/ J. Reynolds & J. Postrel, RFC 1011 – Official Internet Protocols (May 1987).

237/ *See* Technical Appendix at 19-23.

238/ *See* Technical Appendix at 15-18.

239/ *See* Technical Appendix at 35. *See also id.* at 18-19, 33-34.

240/ Even the basic authentication process for customer service calls is potentially constrained by the proposed rules. If broadband customers fail to remember their PIN – a frequent occurrence – the MAC address of the customer's modem may be used to authenticate. If multi-factor authentication is employed for customers that lack access to their mobile device (and therefore cannot receive a text message), use of other CPI may be needed to complete authentication. While customer service for broadband might be considered "necessary to" the provision of broadband service, or a "closely related service," App. A, § 64.7002(a)(1)-(2), there is nothing in the *Notice* to suggest that. To the contrary, the *Notice* asks whether broadband providers should be permitted a "one-time usage" of CPI during a customer service call (which

Thus, the *Notice* introduces considerable regulatory uncertainty, compliance burdens, and potential penalties with current uses of IP addresses, device identifiers, domain information, and other proposed CPI that are commonly employed today throughout the broadband ecosystem.[241/] The examples provided here and in the Technical Appendix also highlight the extent to which items the Commission proposes to define as CPNI – such as IP addresses, MAC addresses and device identifiers, domain information, etc. – have been used by engineers to drive technological development on, and innovation for, the Internet. By tethering these data elements to a rigid permissions regime and erroneously treating them as inherently identifiable, the *Notice* essentially disables their function as lynchpins of innovation. [242/]

The Linkability Standard for PII Is Highly Flawed. The *Notice* proposes to define PII as "any information that is linked or linkable to an individual."[243/] Information is considered "linked" or "linkable" to an individual if it "can be used on its own, in context, or in combination to identify an individual or to logically associate with other information about a specific individual."[244/] As a threshold matter, it is unclear whether this standard qualifies and limits the circumstances in which items listed in the *Notice* as PII would be subject to the permissions regime. As with the data categories listed as CPNI, many of the items delineated as PII – including IP addresses, MAC addresses, persistent identifiers, Internet browsing history, traffic

---

would still require approval to be "granted") - thereby implying that usages of CPI related to customer service would, absent changes, be covered by the permissions regime. *NPRM* at ¶ 148.

241/ The uncertainty associated with the use cases flagged here and in the Technical Appendix cannot be mitigated by simply invoking the exception for the provision of broadband Internet access service or "closely-related services" or reiterating without explanation that the Commission's proposed rules do not apply to "other services" provided by broadband providers. *See infra* § II.D.2; Technical Appendix at 36-37.

242/ *See* Technical Appendix at 1, 5-6, 38.

243/ *NPRM* at ¶ 60.

244/ *Id.* at ¶ 61.

statistics, app usage data, geo-location, medical and health information, shopping records and other data items listed – cannot, on their own, "identify an individual."[245/] But the *Notice* purports to list them as "non-exhaustive" examples of "the types of data that are PII," without anywhere clarifying that they "are PII" only when used or disclosed in a manner that satisfies the "linked or linkable" standard.[246/]

As proposed, the "linkability" standard set forth in the *Notice* is highly overbroad. While purporting to be consistent with the FTC's approach, the standard omits inclusion of the important "reasonableness" qualifier employed by the FTC.[247/] The unqualified "linkability" standard proposed by the FCC takes no account of the distinction between the theoretical possibility that an item of information could be linked to an individual and the reasonable plausibility that it actually is or will be so linked. The FCC's proposal inflexibly binds to a permissions regime any data that could possibly be used by a technically sophisticated expert with sufficient resources and tools to identify a specific individual.[248/] This approach eliminates providers' incentives to calibrate their practices to impose the most stringent protections for the most sensitive data. The FTC opted to place data sets that are "not reasonably identifiable" outside of its framework in order to provide "companies an incentive to collect and use data in a form that makes it less likely the data will be linked to a particular consumer or device, thus

---

245/ *Id.* at ¶ 62. Notably, NIST does not appear to consider many of the items listed as PII by the FCC to be identifiable unless they are maintained in combination with other more specific identifying information such as name, address, SSN, etc., *see NIST Guide to Protecting PII*, *supra* n. 227, at § 2.2, or combined with other information about an individual. *See Id.* at §§ 2.2, 3.3.2 (characterizing IP address + URL information as not "directly identifiable data").

246/ *See NPRM* at ¶ 62.

247/ *FTC Privacy Report*, at 20-21.

248/ Treating as PII information that "can be used . . . in context, or in combination . . . to logically associate with other information about a specific individual" has no grounding in the FTC's 2012 Report and is unmoored from any concept of plausible or reasonable risk of identification. *See NPRM* at ¶ 62

promoting privacy."[249/] The FCC's approach extinguishes these incentives, thereby reducing privacy protections and making consumers worse off.

The Aggregate Data Exception Is Too Narrow. The Commission proposes to treat broadband provider use of aggregate customer data as outside the permissions regime only if they are not reasonably linkable to a specific device.[250/] Not only is such a proposal in conflict with the statute,[251/] it also renders the exception for aggregate information unduly narrow and counterproductive. Aggregate information that is potentially linkable to a "device" does not implicate the same privacy risks as aggregate information potentially linkable to an individual. As the Commission itself recognizes, the NIST PII Guide defines "linked information" only as "information about or related to an individual that is logically associated with other information about the individual."[252/] There is no need to predicate the "reasonable linkability" standard for aggregate information upon a tie to a specific device. If a tie to a device is capable of identifying an individual, then it would be captured by the NIST formulation; if such a tie cannot identify an individual, then there is no reason why it should be excluded from treatment as aggregate data. The Commission does not need to preemptively determine that any data linkable to a device is automatically linkable to an individual, and its proposed narrowing of the exception for aggregate information is counterproductive because it does just that.

By unduly narrowing the scope of the aggregate data exception, the Commission also risks harming consumer welfare and the public interest.[253/] Broadband consumers benefit from

---

249/ *FTC Privacy Report* at 22.

250/ *See NPRM* at ¶¶ 154-59.

251/ *See supra* § I.C.3.

252/ *See NPRM* at ¶ 158*; NIST Guide to Protecting PII* at § 2.1 (emphasis added).

253/ *See* "Comments to the FCC on Broadband Privacy," Peter Swire, Huang Professor of Law and Ethics, Georgia Tech Scheller College of Business, April 28, 2015, at 14 ("[T]he Commission should be

the use of aggregate data for purposes of analyzing usage and consumption patterns and metrics, service popularity, technical performance, potential product enhancements and a host of other valid uses aimed at understanding and improving the services provided to – or developed for – them. In addition, the Commission's approach could harm the public interest by reducing the scope of data available for analysis by academic and product researchers. Aggregate data sets have been utilized by researchers for a wide range of social beneficially uses, and it makes little sense to prophylactically exclude from such sets information that could be linked to devices.[254/] Ensuring a level of anonymization sufficient to meet the FCC's unnecessarily high standard could inadvertently thwart the development and publication of important and beneficial data-driven insights and innovations.[255/]

The Proposal Discourages De-Identification Practices that Reduce the Risk of Privacy Harms. The *Notice* apparently intends to exempt from the permissions regime only data that is both de-identified and aggregated.[256/] In contrast, data aggregation is just one form of rendering data de-identified under the FTC Framework.[257/] The FTC model does not require de-identified data to be aggregated as a condition of exemption from the choice framework, and thus the FCC regime would disadvantage ISPs relative to all others in the ecosystem in the use of de-identified,

---

cautious about an over-expansive definition of what counts as individually identifiable CPNI, or an overly narrow definition of aggregate information. There is considerable utility from analysis of data for many consumer service, consumer protection, and other purposes").

254/ Jane Yakowitz, Tragedy of the Data Commons, 25 HARV. J. L. & TECH. 1, 9-10 (2011).

255/ *Id.* at 13-17. *See generally* Ann Cavoukian & Daniel Castro, Information and Privacy Commissioner Ontario, Canada, Big Data and Innovation, *Setting the Record Straight: De-Identification Does Work* (June 16, 2014), http://www2.itif.org/2014-big-data-deidentification.pdf ("*De-Identification Does Work*").

256/ *NPRM* at ¶ 165.

257/ *FTC Privacy Report* at 21 ("[A] variety of technical approaches to de-identification may be reasonable, such as deletion or modification of data fields, the addition of sufficient 'noise' to data, statistical sampling, or the use of aggregate or synthetic data")(emphasis added).

non-aggregate data. The FCC's approach also would create confusion, since edge providers may utilize data de-identified at the customer level, without soliciting advance approval, for marketing, advertising, or other purposes.[258/]

The FCC's treatment of "non-collective," de-identified data is counterproductive and harms consumer welfare. De-identification can work effectively to reduce risks to consumer privacy while preserving beneficial uses of data.[259/] By discouraging anonymization of individual account and household data in favor of data aggregation as the only approach to de-identification, the Commission actually puts consumer privacy at greater risk.[260/] The FCC's approach will simply prompt companies to forego investing in tools, resources and protocols that reduce the identifiability of data they employ for purposes of enhancing the customer experience, marketing services, or delivering advertising, and instead seek permission to maintain data sets and profiles in a more individually identifiable form.[261/]

258/ *See, e.g.*, Google Inc., Privacy Policy, https://www.google.com/policies/privacy/; Facebook, Inc. Data Policy, Sharing With Third-Party Partners and Customers https://www.facebook.com/policy.php; The New York Times, Privacy Policy, http://www.nytimes.com/content/help/rights/privacy/policy/privacy-policy.html.

259/ Cavoukian & Castro, *De-Identification Does Work*, at 9-11. *See also FTC Internet of Things Report* at 37 (Noting that "maintaining data in de-identified form . . . helps minimize the individualized data companies have about consumers, and thus any potential consumer harm").

260/ Cavoukian & Castro, *De-Identification Does Work*, at 9-11; *see also* Stuart S. Shapiro, Homeland Security Systems Engineering and Development Institute, *Situating Anonymization Within a Privacy Risk Model*, at 3 (2012), https://www.mitre.org/sites/default/files/pdf/12_0353.pdf, ("[A]nonymization is more accurately viewed as reducing the ability to associate information with specific individuals. To the extent the implicated characteristics of risks involve identity information and sensitive attributes, anonymization can serve to reduce privacy risk").

261/ *See* Letter from American Association of Advertising Agencies, et. al. to Senator Jeff Flake and Senator Al Franken, May 10, 2016, at 2-3 ("[T]he FCC would expand the definition of personally identifiable information to data elements that are not, and have not been considered, individually identifiable, such as application usage data, persistent online identifiers (cookies), device identifiers and Internet browsing history. Many companies have developed service models that focus on collecting such data instead of PII").

An appropriately tailored privacy framework should distinguish between the risks posed by use and disclosure of de-identified data – even if it is "non-collective" – and PII, recognizing that different types of data usage practices create different risks of harm. The privacy risks presented by the use of data that do not contain PII are not the same as those associated with personal data that identify a particular broadband customer.[262/] There is no empirical evidence to support the proposition that consumers accord the same level of concern over the privacy of information that cannot be identified with them, as they do toward information that can be identified with them. The danger of conflating the risks and harms associated with the use of PII and use of anonymized data is it effectively deters companies from committing resources to anonymizing data, thereby depriving the public of the benefits of de-identification.[263/] Instead of dampening investment in, and use of, de-identification tools and techniques, the Commission's privacy framework should promote existing and future privacy-enhancing technologies that minimize or eliminate the association of data with individuals.

2. The Customer Approval Framework Proposed in the NPRM Dramatically Departs from the Status Quo and Will Harm Consumer Welfare

The permissions regime proposed in the *Notice* is overly restrictive, will interfere with existing practices, will place broadband service providers at a competitive disadvantage, and be a drag on development of new services and capabilities. By marginalizing the concept of context

---

262/ Simson L. Garfinkel, *De-Identification of Personal Information*, NISTIR 8053, National Institute of Standards and Technology, at iii, 5 (2015)("De-identification can reduce the privacy risk associated with collecting, processing, archiving, distributing, or publishing information. . . .all data exist on an identifiability spectrum. At one end (the left) are data that are not related to individuals . . . and therefore pose no privacy risk. At the other end (the right) are data that are linked directly to specific individuals. Between these two endpoints are data that can be linked with effort, that can only be linked to groups of people, and that are based on individuals but cannot be linked back").

263/ *FTC Privacy Report*, at 22. *See also FTC Internet of Things Report*, at 43 ("[R]obust de-identification measures can enable companies to analyze data they collect in order to innovate in a privacy-protective way. Companies can use such de-identified data without having to offer consumers choices").

which was at the core of the FTC Framework, specifying only a narrow set of exemptions for first-party data uses, and establishing opt-in consent – rather than opt-out – as the default choice mechanism for virtually all uses of customer data, the FCC's proposed permissions regime radically departs from the FTC Framework's choice architecture applicable to all other Internet ecosystem entities.

The FCC's Approach to Context Differs Substantially from the FTC's Model. The FTC makes "context" the fulcrum of the choice architecture under its framework, establishing that the need to seek customer approval for a particular data usage depends on the relationship between the customer and the business or the context of the specific transaction in which the two are engaged.[264/] The FTC's notion of context starts from the basic premise that a business' relationship with its customer can evolve over time and encompass products, services and capabilities that may differ from those involved in the initial transaction with the consumer.[265/] It is also predicated upon the recognition that managing customer relationships involves more than simply furnishing service, but also entails understanding the manner in which services are consumed, identifying areas for improvement, and offering customers product enhancements and services of interest to them.[266/] By recognizing both that the context of a company's interaction with consumers is an organic and evolving concept and that data uses that are consistent with that context do not require approval, the FTC allows customer relationships to develop and

---

264/ *FTC Privacy Report* at 38-39.

265/ *See id.*

266/ *See ITIF Broadband Privacy Report* at 3 ("Analyzing data is essential for ISPs to understand patterns and trends in Internet traffic and allows for informed adjustments to network functions and capacity, both in the long and the short term. Customer data is also important to help diagnose problems within the network and facilitate responses to customer requests for assistance with various issues").

grow.[267/] The use of context as the lynchpin for whether or not to solicit customer approval renders the choice architecture of the FTC's framework far more flexible and agile. Indeed, the FTC's reliance upon the context standard is aimed at ensuring that its framework is "sufficiently flexible to allow for innovation and new business models."[268/]

In contrast, the FCC's conception of "context" is far more narrow and rigid - and much less central to the operation of its proposed permissions regime - than the manner in which context is understood under the FTC Framework.[269/] Because the FCC proposal is more restrictive and less flexible and nuanced than the FTC Framework, data uses that would be considered consistent with the context of a provider's relationship with the consumer under the FTC model would instead trigger approval solicitations under the FCC's regime. The end result will be increased notice fatigue, increased customer annoyance and service disruption, and greater obstacles to providing customized services and offers that consumers want in order to obtain approval for data uses that the FTC model today treats as permissible.

Implied Consent/First-Party Uses. The FTC recognized that "most first-party marketing practices are consistent with the consumer's relationship with the business and thus do not necessitate consumer choice."[270/] Accordingly, the FTC guidance treated most first-party uses as within the context of the customer's interaction with the service provider, including

---

267/ *See also White House Privacy Framework* at 16 (While context principle "emphasizes the importance of the relationship between a consumer and a company at the time consumers disclose data, it also recognizes that this relationship may change over time in ways not foreseeable at the time of collection. Such adaptive uses of personal data may the source of innovations that benefit consumers").

268/ *FTC Privacy Report* at 38.

269/ *FTC Privacy Report* at 36-44. *See also White House Privacy Framework*, *supra* n. 141, at App. A. (proposing a Respect for Context principle in the Consumer Privacy Bill of Rights).

270/ *FTC Privacy Report* at 40.

cross-channel marketing and most affiliate sharing.[271/] The White House's 2012 Privacy Framework likewise contemplates a reasonable sphere of first-party use of personal data based on inferred consent, including for marketing, analytics, fraud prevention, and protection of intellectual property.[272/]

The FCC, however, discards the FTC's well-established and successful approach and instead narrowly defines the context of a subscriber's interaction with her ISP as exclusively the provision of broadband Internet access service, meaning that virtually all first-party marketing is outside the context of the relationship and subject to the permissions regime. Indeed, the FCC's proposal allows only one first-party marketing practice to occur without seeking some form of customer approval: the marketing of another level or tier of broadband services.[273/] Any other first-party marketing-related use of customer data is prohibited absent some form of consent. For example, the proposed rules would restrict ISPs from marketing their video services to broadband cable subscribers absent some type of consent, even though tens of millions of households today reap the savings associated with bundling their broadband service with video service.[274/]

This is wholly at odds with the FTC and White House frameworks, as well as customer expectations. Consumers are accustomed to receiving marketing offers from companies with which they have an ongoing service relationship, [275/] and those companies are careful not to

---

271/ *Id.* at 41-44.

272/ *White House Privacy Framework* at 17.

273/ *NPRM* at ¶ 114.

274/ *See Annual Assessment of the Status of Competition in the Market for the Delivery of Video Programming*, Sixteenth Report, 30 FCC Rcd 3253, at ¶¶ 2, 101 (2015).

275/ *FTC Privacy Report* at 42 ("[R]eceipt of a message from a company with which a consumer has interacted directly is likely to be consistent with the consumer's relationship with that company").

inundate the subscriber with unwanted messages in order to preserve and strengthen that relationship.[276/] There is no justification for requiring ISPs to seek permission from their customers to market other products and services furnished by the provider or its affiliates, when all other entities in the broadband ecosystem are not subject to any approval obligation to market their full portfolio of services without customer approval. Such a disparity will only distort the marketplace and unnecessarily interfere with the ability of consumers to learn about services and products of interest to them.

The small set of implied consent exceptions authorized in the *Notice* are themselves narrow and vague. The breadth of data subject to the CPI permissions regime – coupled with the narrowness and vagueness of the implied consent exceptions to the approval framework – will make it much harder to provide a seamless and frictionless customer experience. The first-party exceptions permitted in the *Notice* are limited to broadband service fulfillment, initiating or rendering broadband service or "closely related services," marketing of different forms or tiers of broadband service, legal compliance, and the protection of property/prevention of spam and other abusive uses (which includes uses of CPI for sharing of cybersecurity threat indicators).[277/]

Under the Commission's rules, broadband service is defined narrowly as little more than packet routing, decoupled from any processing or other information service capabilities associated with a broadband service offering or transmission.[278/] Thus, CPI uses necessary for,

---

276/ *2002 CPNI Order* at ¶ 37 (noting carrier's "strong incentive not to misuse its customers' CPNI or it will risk losing its customers' business.")

277/ *NPRM* at ¶¶ 113-121.

278/ *NPRM* at ¶ 29. The *Open Internet Order* defines broadband Internet access service expressly to exclude related capabilities typically bundled with broadband Internet access service, such as email and DNS look-up. *See Open Internet Order* at ¶ 356. As a result, the implied consent exemption for CPI used in the "provision of the broadband Internet access service from which such information is derived, or in its provision of services necessary to, or used in, the provision of such broadband service," *NPRM* at App. A, § 64.7002(a)(1), does not on its face encompass CPI used by an ISP to provide integrated

or incidental to, transmitting or providing services or capabilities that customers have requested or purchased from or through the ISP could be subject to the permissions regime.[279/] The simple act of an ISP furnishing via broadband transmission a capability offered with an affiliated home security service could involve a use or disclosure of an IP address or MAC ID that would trigger the permissions regime. Likewise, the purchase and delivery of anti-virus or desktop software programs or applications sold by ISPs (or by third-party vendors or affiliates through ISPs) may entail the use disclosure of an IP address, MAC ID, or other CPI.[280/] There are numerous potential examples in which an ISP may need to use or disclose an IP address or other CPI in conjunction with fulfilling, via a broadband service transmission, a task requested of that ISP by a customer – but because that task is not itself broadband Internet access service, there is considerable uncertainty as to whether the ISP can do so without soliciting approval.

The uncertainty around these uses cannot be resolved by reference to the *Notice's* cryptic statement that the proposed regime does not apply to "the provision of other services by broadband providers."[281/] The *Notice* provides no guidance as to whether or when a broadband service provider offering an integrated suite of services and capabilities in conjunction with the provision of broadband Internet access service should be considered furnishing "other services" not subject to the permissions regime. Likewise, while the draft rules proposed in the NPRM suggest that implied consent would be available where CPI is used to initiate, render, bill or collect for "closely related services," no guidance at all is provided with regard to the meaning of

---

services and capabilities characterized in the *Open Internet Order* as information services that ride on top of BIAS.

279/ *See supra* § II.D.1.

280/ *See* Technical Appendix at 35.

281/ *NPRM* at ¶ 13. *See id.* at n.35 ("For example, the activities of an online advertising company or social media site owned by a broadband provider are not part of the broadband Internet access service").

that term other than the suggestion that it would encompass "tech support related to" broadband service.[282/] But that could encompass little more than an installer unavoidably encountering the MAC ID on a subscriber's router.

Even where the *Notice* provides some guidance regarding uses of CPI that may be exempt from customer approval, upon further scrutiny and checked against actual day-to-day practices, the exception turns out to reinforce the overbreadth of the permissions regime and disregard for flexibility.[283/] For example, the *Notice* suggests that Section 222(d)(2) should be read to permit broadband providers to use or disclose CPNI to protect against cybersecurity threats or vulnerabilities.[284/] As reflected in recent guidance from the Department of Justice and Department of Homeland Security in connection with implementation of the Cybersecurity Information Sharing Act of 2015 (CISA),[285/] IP address information and other metadata categorized as CPI – pertaining to suspect domains, threat vectors, sources of botnets and malware - are a common form of cyber threat information.[286/] However, because use or disclosure of IP addresses is generally prohibited under the FCC's proposed rules absent opt-in approval, companies seeking to share cyber threat information in order to deal with a real-time attack will need to ensure that any IP address they disclose is "reasonably necessary to protect" their network or others, or risk penalties. This will introduce layers of review and delay into

---

282/ *NPRM* at App. A, § 64.7002(a)(2). *See also NPRM* at ¶ 117 (permitting broadband providers to "use CPNI without customer approval in the provision of inside wiring installation, maintenance, and repair services").

283/ *See* Technical Appendix at 26-30.

284/ *NPRM* at ¶ 117.

285/ *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015*, Department of Justice & Department of Homeland Security, at 5-6 (Feb. 16, 2016).

286/ Cyber threat indicators also include email addresses, domain names, and URLs, *Id.*, each of which is also proposed to constitute CPI. *NPRM* at ¶¶ 46, 50, 62.

addressing real-time threats. Further, until the boundaries of this exemption are clearly understood, common cybersecurity-related uses of IP addresses that may not be considered linked to an imminent threat – such as sharing IP addresses with third-party security vendors and academic researchers studying threat vectors, tools performance, and threat intelligence capabilities – may be deferred pending further guidance and review.[287/] Attempting to delineate a laundry list of circumstances in which use of CPI data elements may be considered "reasonably necessary to protect" against cybersecurity threats will fail to protect against new types of threats and provide cyber criminals with a blueprint for devising strategies that would deter sharing of threat information. Further, the risk of enforcement action for even accidental disclosures of CPI potentially could deter voluntary sharing with law enforcement, security specialists, and other networks.

In short, the first-party exceptions proposed in the *Notice* are inadequate and ill-defined, and fail to consider the impact of the Commission's proposed regime on network performance and service functionality, the seamlessness of the broadband customer experience, and the Internet ecosystem as a whole.

Permissions Regime. Not only does the Commission's proposed regime enumerate a very limited range of practices covered by implied consent, it limits ISP use of CPI pursuant to

---

[287/] For example, some botnets function as peer-to-peer applications, and do not operate pursuant to a traditional command-and-control structure emanating from a single location. Instead, the bots operate interdependently, which expands both the number of potential threat vectors as well as the number of potential intelligence gathering points. As a result, just a handful of infections on a given network from a peer-to-peer botnet can yield a large trove of useful intelligence concerning the IP addresses of potential victims across the Internet. But in the absence of a specific and imminent threat to a particular network, the Commission's proposal raises a caution flag about whether a broadband provider is authorized to compile IP addresses for this purpose, or to share such compilations with other networks providers, third-party security specialists, and law enforcement.

opt-out approval to only a narrow set of practices.[288/] By contrast, the FTC privacy framework employs opt-out as the default mechanism for most disclosures of data to third parties, reserving opt-in or affirmative express consent only for uses of "sensitive" data and material changes to privacy policies that propose to use data in ways not previously encompassed within the company's privacy notice.[289/]

Under the FCC approach, opt-out is allowed solely for use of CPI for cross-marketing by a provider or affiliate of "communications-related services" – which are not defined but appear to mean only services regulated by the Commission.[290/] As noted above, such uses typically would be considered permissible first-party practices under the FTC's Framework, and therefore make it easy for consumers to learn about products and offers of interest to them. It makes no sense, for example, that those ISP customers who today routinely receive and take advantage of an ISP's bundled offerings of broadband, video, voice, and alarm monitoring services at substantial discounts would now have to opt-in in order to receive information about these lower-priced offerings because the FCC unreasonably determines that one of these services does not qualify as a "communications-related service." As proposed, the Commission's regulations potentially could exclude from the rubric of communications-related services home security, home energy management and other "Internet of Things" offerings from ISPs, CPE, smart devices and related peripherals offered by or through an ISP, and any content, games, software or

288/ *NPRM* at ¶¶ 122-23.

289/ *FTC Privacy Report* at 48-55, 58-60.

290/ *NPRM* at ¶¶ 122-23.

other services offered by an ISP or its affiliates or partners that is delivered via a broadband service transmission.[291/]

By making it harder for ISPs to apprise their customers of products, services and offers of interest to them, the Commission's approach would harm consumer welfare. It also would severely disadvantage ISPs relative to other Internet entities in terms of their ability to market related services, rendering them the sole entity in the broadband ecosystem that must obtain opt-in approval in order to engage in such activity.[292/] Handcuffing ISPs in this manner relative to all other Internet entities will undermine competition, dampen investment and thwart innovation.

Research shows that individuals are significantly more likely to choose to participate in a given activity when offered an opt-out choice rather than being asked to opt-in.[293/] The FCC itself previously has recognized the significant variance between participation rates for a given data usage activity based upon whether an opt-in or opt-out choice is offered.[294/] Further, opt-out

---

291/ *See e.g.,* Leibowitz Comments at 8 (Noting that FCC's proposal could be read to restrict an ISP from marketing "a home security system, cloud services, or music streaming . . . to its own customers without their prior opt-in consent . . . despite the fact that this type of first-party marketing is certainly consistent with consumer expectations").

292/ The restriction on sharing information with third party partners also would limit the ability of ISPs to integrate their services with other providers.

293/ *See, e.g.*, Thomas M. Lenard & Paul H. Rubin, *In Defense of Data: Information and the Costs of Privacy*, TECHNOLOGY POLICY INSTITUTE, 46 (May 2009) ("[C]onsumers have a tendency not to change the default, whatever it might be."); Eric J. Johnson, et. al., *Defaults, Framing and Privacy: Why Opting In-Opting Out*, 13 MARKETING LETTERS 5, 7-9 (2002) (finding that opt-out choices led to participation by up to twice as many people as opt-in choices) *available at* https://www0.gsb.columbia.edu/mygsb/faculty/research/pubfiles/1173/defaults_framing_and_privacy.pd; Mindi Chahal, *Consumers less likely to 'opt in' to marketing than to 'opt out'*, MARKETING WEEK, May 7, 2014, https://www.marketingweek.com/2014/05/07/consumers-less-likely-to-opt-in-to-marketing-than-to-opt-out/ (study found that 29 percent of respondents would opt-in compared to 51 percent who would not opt-out).

294/ *2002 CPNI Order* at ¶ 62 ("Testimony submitted to the Federal Trade Commission (FTC) shows that opt-out results in disclosure rates of 95 percent, but when the default is opt-in, 85 percent of consumers would choose not to provide their data"); *see also* Lenard & Rubin, at 45-46 (citing findings that initial participation in opt-in 401(k) plans was 20% and never rose above 65%, whereas participation in opt-out 401(k) plans reached as high as 98%).

regimes lead to better privacy outcomes by incentivizing companies to offer consumers feature-by-feature choices; conversely, opt-in regimes spur companies to seek expansive permissions for data use from their customers.[295/] Thus, rather than enhancing consumer choice, opt-in effectively takes choices away from consumers.

Opt-in regimes also lead to missed opportunities for enhancing consumer welfare. For example, "[m]any users who would otherwise have benefited from using services that collect information may be deterred simply by a subjective feeling or inability to evaluate the initial costs of the offer as it stands."[296/] And at a societal level, "[e]conomists have theorized that opt-in regimes do not maximize social welfare because they discourage participation that could lead to increased economic value and activity."[297/] If the FCC mandates opt-in for a range of data uses for which consumers have declined to exercise opt-out rights, that obligation invariably will harm consumer welfare by reducing data usage in circumstances in which consumer behavior under the FTC Framework already has indicated a preference for such uses.[298/]

The mere decision by the Commission to reclassify broadband services as a common carrier offering does not warrant changing the approval mechanism that ISPs must obtain for use

---

295/ Nicklas Lundblad & Betsy Masiello, *Opt-In Dystopias*, 7 SCRIPTED 155, 160-62 (2010), http://www2.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.pdf.

296/ *Id.* at 162.

297/ *Id.*; *see also* H.A. Degryse and J. Bouckaert *Opt In versus Opt Out: A Free-Entry Analysis of Privacy Policies*, CESifo Working Paper Series No 1831, CentER Discussion Paper No 2006-96, at 20-22 (Sep. 2006), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=939511.

298/ *See* Lenard & Rubin, *supra* n. 293, at 46-7("Surveys show that most consumers would be willing to trade information for something specifically useful to them. As discussed above, the purpose of obtaining information about consumers is to provide them with targeted advertising—advertising of products likely to be of use to them—as well as with services, such as free search and email. These are the types of transactions consumers indicate they would like to engage in. . . . efficiency would argue for giving the initial right to businesses—that is, for opt-out. . . . If the default were opt-in, then information would be lost—it would not flow to its highest-valued uses. This loss of information would be quite costly and would lead to price increases as firms attempt to compensate for the loss of information.").

of customer data, particularly when the consequence of such a decision will be to hinder their ability to offer data-driven customized services, advertisements, and marketing offers in relation to all other Internet entities. The Commission's putative concern with switching ISPs does not compel requiring an opt-in rather than an opt-out choice, because an opt-out regime does not put any consumer in a "take-it-or-leave-it" trade-off between privacy and Internet access service. Conversely, the FCC's previous statements that communications services providers should be regarded as more trustworthy and reliable stewards of consumers' personal data than third party entities that have no recurring business relationship with subscribers underscore the anomaly of imposing a more restrictive permissions regime on ISPs than edge providers.[299/]

The Commission's proposal will be particularly detrimental to ISPs' ability to use customer data for matters such as interest-based advertising, analytics for purposes of developing and offering new products and services, and first-party marketing of related Internet-enabled services and products.[300/] These are key elements of data-driven competition and innovation on the Internet, and the Commission's decision to encumber ISPs' ability to engage in these activities relative to their peers will harm consumer welfare. The White House Big Data Report notes the "enormous benefits associated with the rise of profiling and targeted advertising and the ways consumers can be tracked and offered services as they move through the online and physical world," and acknowledges that "advertising and marketing effectively subsidize many free goods on the Internet, fueling an entire industry in software and consumer apps."[301] Advertising that is more relevant for consumers is likely to be of greater practical value to them. When broadband consumers see tailored information about services and offerings that better

---

299/ *2002 CPNI Order* at ¶¶ 37, 46, 48

300/ *NPRM* at ¶ 127.

301/ *White House Big Data Report* at 50.

reflect their interests, instead of a barrage of ads that may be of little interest to them, it enables them to make more accurate purchasing decisions in the marketplace. Interest-based advertising has been shown to generate more than twice as much revenue as conventional ads,[302/] so the Commission's decision will clearly have competitive consequences.[303/] The *Notice* offers no justification as to why it should be more difficult for ISPs to engage in interest-based advertising than all other entities in the broadband ecosystem.

The new restrictions on use of CPI in connection with data analytics performed by – and on behalf of – ISPs is particularly short-sighted. The PCAST Report cautions against policies that constrain data analysis, questioning their efficacy for improving privacy and warning of their potential adverse economic effects.[304/] Further, the Report maintains that data analysis, on its own, does not directly impinge upon individuals.[305/] Data analytics help to provide consumers with more relevant marketing and advertising, graphics, settings and capabilities configured to their preferences, customized services and applications, free promotional items, and discounted service offerings. The *Notice* does not explain how consumers benefit from policies that make it harder for ISPs to engage in these activities.

302/ J. Howard Beales & Jeffrey A. Eisenach, *Putting Consumers First: A Functionality-Based Approach to Online Privacy*, NAVIGANT ECONOMICS, 7-8 (Jan. 2013) (finding "the price of behaviorally targeted advertising to be 2.68 times higher than the price for run-of-network advertising, and that behaviorally targeted advertising also had higher conversion rates."); Press Release, Network Advertising Initiative, (Mar. 24, 2010), http://www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf ("Study finds behaviorally-targeted ads more than twice as valuable, twice as effective as non-targeted online ads.").

303/ Beales & Eisenach, at 30 (The potential harm from limiting entry by ISPs and other potential competitors into the market for online advertising is significant. . . the market for online advertising is characterized by relatively high concentration and, for the last few years at least, stable market shares.).

304/ *PCAST Big Data Report* at xiii.

305/ *Id.* at 49-50.

Rather than single out ISPs for more stringent limitations on their ability to use customer data, the FCC should instead mirror the default opt-out regime employed by the FTC, reserving opt-in only for uses and disclosures of sensitive data such as health and children's information.[306/]

The NPRM is also vague on how frequently opt-in approval must be obtained. The NPRM envisions its opt-in rule to function similarly to consent requests in circumstances where mobile applications ask for permission to use geo-location information, contacts, lists or photographs on a consumer's smartphone.[307/] That approach may not map well to broadband, particularly given the broad scope of data, such as IP addresses and device identifiers, whose use triggers a notice obligation under the proposal. It is also likely that any approach akin to mobile consents will frustrate and annoy customers – users expect that their ISP will not redirect or delay their access to a webpage, but the moment at which a user attempts to connect to the Internet or send an email potentially triggers a covered data use for an ISP under the proposed rules. To the extent this is what the *Notice* envisions as "just-in-time" approval solicitation proposed in the NPRM,[308/] it is likely to result in frequent and repeated interruptions that are more apt to aggravate than reassure customers.

Lastly, the requirements for documenting compliance with the permissions regime[309/] are excessive, and far more onerous than that imposed on others in the Internet ecosystem. Likewise, the proposal to subject publicly available data obtained from third parties to the

---

306/ *NPRM* at 136; *FTC Privacy Report* at 47-48.

307/ *NPRM* at ¶¶ 140-143.

308/ *NPRM* at ¶ 142.

309/ *NPRM* at ¶ 149.

proposed default opt-in permissions regime[310/] should be rejected, because it would be far more stringent than what others in the ecosystem are subject to under the FTC Framework.

3. The NPRM Proposes Excessive Notice Requirements and Potentially Onerous Access Rights

As discussed below, specific elements of the notice requirements in the NPRM are potentially problematic and the sheer volume of notices contemplated could lead to consumer notice fatigue and confusion.

First, the Commission should not adopt a standardized format for ISPs' privacy policies.[311/] ISPs have devoted substantial resources to developing the language and formatting of their privacy policies that may reflect unique considerations regarding their customer base and preferred method of communicating with subscribers. There is no need for a government-directed, standardized privacy notice, which might quickly become obsolete or otherwise be incompatible with the manner in which some (or most) providers communicate with their customers.

Second, the Commission also should refrain from requiring ISPs to create a consumer-facing privacy dashboard.[312/] Such a mandate would force providers who do not engage in profiling at a household or account level to begin doing so, and would compel all providers to expend resources on consumer-facing mechanisms to provide consumers with the ability to access and revise such profiles. The decision about whether to offer a dashboard should be left to a company's business discretion, rather than compelled by regulatory fiat.

310/ *E.g.*, *NPRM* at ¶ 19.

311/ *See NPRM* at ¶ 90.

312/ *See id.* at ¶ 95.

Third, the Commission fails to afford ISPs sufficient flexibility with regard to the manner in which they provide notice required under the rules proposed in the *Notice*, including for material changes and data breaches.[313/] Broadband service providers should be able to solicit a customer's preference with regard to required notices, and send such notifications to their customers in accordance with those preferences – which may include a text message to a mobile phone number.[314/] Under the Commission's proposal, however, ISPs would be required to furnish notice of material changes (i) by email or another electronic means of communication agreed upon by the customer and ISP; (ii) on customers' bill for broadband service; and (iii) via a link on the provider's home page.[315/] An ISP should be required to provide notice of material changes on its home page and via either email/other electronic means or the customer's bill – but not both. The goal is to provide notice to the customer and the ISP is in the best position to know how best to reach its customers. Further, because of space limitations, it should be sufficient for customer bill notices to advise customers that the provider's privacy policies have materially changed and to direct them to a Web landing page for more information.

In addition, the NPRM's suggestion that the Commission rely upon the *Open Internet Order's* definition of "material change" should be rejected, since that definition encompasses "any change that a reasonable consumer or edge provider would consider important to their decisions on their choice of provider, service, or application."[316/] The reference to "edge

---

313/ *NPRM* at 96-101.

314/ Additionally, the BIAS provider should be able to set a reasonable default for this preference, such as relying upon an email address of record, in the event that a customer does not provide a preference.

315/ *Id.* at 96.

316/ *Open Internet Order* at 5671-72, ¶ 161.

providers" should be removed, since the rules proposed in the NPRM are aimed at protecting the privacy interests of broadband service customers, not edge providers.

Fourth, the Commission's suggestion that ISPs should, upon request, provide customers free of charge and within 30 days, a list of all of their PII that has been disclosed to third parties and how to contact those third parties,[317/] would – given the broad scope of data included as CPI under the proposal – impose broad and onerous access rights. NCTA is unaware of any privacy statute or regulatory framework that would – as here – afford customers access rights to information that is not subscriber-specific or linked directly to an identifiable individual. Moreover, the NPRM's broad definition of customer – which includes "former customers"[318/] – would potentially require retention of customer data for an unspecified period of time after the customer has terminated service in order to ensure compliance with the proposed access obligations.[319/] Such *de facto* retention obligations could actually increase, rather than mitigate, customer privacy and security risks.

E. The Data Security Requirements Proposed in the NPRM Are Excessive and Counterproductive

The NPRM proposes both a general obligation to protect the "security, confidentiality, and integrity of Customer PI" that the ISP receives from any unauthorized uses or disclosures,[320/]

317/ *NPRM* at ¶ 85.

318/ *NPRM* at ¶ 32. The *Notice* incorrectly suggests that customers must be defined to include "former" customers because consumers will otherwise be hesitant to switch ISPs due to concerns that their data will be misused. *See id.* at ¶ 33. There is no evidence to support this proposition. In fact, ISPs have strong incentives to seek to win-back customers that switch providers, and therefore would derive little benefit from misusing the data of former subscribers. Moreover, this proposition proves far too much. If the absence of an ongoing business relationship with end users heightens privacy risks, then the Commission should not be erecting a privacy regime that results in edge providers that have no recurring business relationship with consumers are subject to less stringent privacy obligations than ISPs.

319/ *NPRM* at ¶¶ 85, 205-09.

320/ *NPRM* at ¶ 170.

as well as several specific regulations delineating particular procedures and measures broadband providers must employ in order to secure customer data in compliance with the FCC's regime.[321/] Broadband providers have strong incentives to take robust measures to protect their customers' data. A "reasonableness" standard administered on a case-by-case basis makes sense, since it provides companies with the flexibility to adapt and innovate with regard to the manner in which they safeguard data.

The proposed data security regulations present another instance in which the breadth of data proposed to be included as CPI yields an overbroad and unnecessarily onerous obligation. Consistent with the scope of data afforded protection under Section 222(c), a data security obligation imposed upon ISPs should cover only "individually identifiable" information.[322/] In addition, companies should be permitted to employ a risk-based approach to securing customer data and addressing potential vulnerabilities, calibrating use of the most protective measures upon the sensitivity of the data.

The specific safeguards enumerated in the NPRM are unnecessary and counterproductive.[323/] They are out-of-step with the preference for flexible, voluntary, mechanisms for securing networks and data residing on networks, as articulated by the White House, National Institute of Standards and Technology (NIST), Congress, and the Commission itself through Communications Security, Reliability, and Interoperability Council (CSRIC). The White House's core cybersecurity policy initiative was memorialized in a 2013 Executive Order that directed NIST to establish a cybersecurity framework for voluntary use by industry that

---

321/ *Id.* at ¶ 174.

322/ 47 U.S.C. § 222(c).

323/ Leibowitz Comments at 11 ("Companies are better positioned to assess evolving risks to their systems; rules requiring specific processes or special treatment of certain data are often not adaptable to diverse and changing business models or technologies and quickly become outdated").

would "incorporate voluntary consensus standards and industry best practices to the fullest extent possible."[324/] NIST implemented this policy directive by establishing a voluntary cybersecurity framework that relied upon "business drivers to guide cybersecurity activities" and sought to "manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses."[325/] Congress codified this reliance upon voluntary mechanisms for securing networks in the Cybersecurity Enhancement Act of 2014.[326/] And the Commission itself embraced this approach with its support for the CSRIC IV Working Group 4 Report.[327/]

The delineation of specific, compulsory data security measures and procedures in the *Notice* also is wholly inconsistent with the approach previously charted by Chairman Wheeler. Indeed, Chairman Wheeler has stated that, in addressing risks to network cybersecurity, the Commission cannot "hope to keep up if we adopt a prescriptive regulatory approach" and that it must "harness the dynamism and innovation of competitive markets" and utilize a "new regulatory paradigm of business-driven cybersecurity risk management."[328/] Chairman Wheeler also made clear that, with respect to securing networks, the Commission would rely "on industry

---

[324/] Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, at Section 7 (Feb. 12, 2013).

[325/] *Framework for Improving Critical Infrastructure Cybersecurity*, Nat'l Inst. of Standards & Tech., at 1 (Feb. 12, 2014).

[326/] Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971.

[327/] The Communications Security, Reliability and Interoperability Council IV, Working Group 4, *Cybersecurity Risk Management and Best Practices*, Final Report, at 11 (March 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf ("The U.S. government has clearly endorsed development of a voluntary, risk-based model that enables organizations to prioritize and implement solutions based on informed, enterprise-tailored, business-driven considerations").

[328/] Remarks of FCC Chairman Tom Wheeler, American Enterprise Institute (June 12, 2014), https://apps.fcc.gov/edocs_public/attachmatch/DOC-327591A1.pdf.

and the market first while preserving other options if that approach is unsuccessful."[329/] Nowhere in the *Notice* does the Commission suggest that its preference for voluntary, business-driven solutions to network security has failed or warrants being discarded in favor of prescriptive rules.

The *Notice* recognizes that "most BIAS providers already have robust data security measures in place"[330/] and many of those incorporate the five specific practices the FCC proposes to mandate.[331/] But inscribing those practices into law risks freezing into place a certain set of data security practices that may become quickly outdated in the future. Network and data security poses a unique set of challenges, characterized by rapidly changing technology, continuous innovation and a dynamic threat landscape that often must be addressed in real-time. A flexible policy framework is critical to preserve the business and technical agility ISPs need to address real-time and rapidly changing security threats. Adoption of the compulsory data security obligations proposed or discussed in the *Notice* would not enhance data security,[332/] due to the inherently backward-looking nature of regulation. Instead, they would foster checklist compliance and make data security lawyer-driven and process-based, instead of technology-driven and focused on addressing the latest iteration of security threats and attack vectors.

In connection with its data security proposals, the NPRM also asks about data minimization and constraints on data collection,[333/] even though Section 222 – in contrast to

---

329/ *Id.*

330/ *NPRM* at ¶ 177.

331/ *Id.* at ¶ 174.

332/ *See id.* at ¶¶ 174-216.

333/ *NPRM* at ¶¶ 221-32.

Section 631 and 338(i)(3) – has no restrictions on data collection.[334/] Further, the lead recommendation of the PCAST Big Data Report finds that "policies focused on the regulation of data collection, storage, retention . . . and analysis" are unlikely to be effective mechanisms for improving privacy, and may be enforceable only through measures that are "severe and economically damaging."[335/] The FCC should refrain from imposing data collection and data minimization requirements, and recalibrate its data security proposal to reflect the preference for voluntary mechanisms favored by Congress, the White House, and other policy-makers.

F. The Data Breach Framework Proposed in the NPRM Should Not Be Adopted

Even though data breach rules notification rules already are present in 47 of the 50 states, the *Notice* proposes a special set of data breach obligations that would apply only to broadband service providers. ISPs already have strong, market-based incentives to detect and deter potential data breaches, and minimize the damage from successful incursions. The rules proposed by the Commission are unnecessary, highly cumbersome, and counter-productive.

As a threshold matter, the definition of data breach proposed in the *Notice* is extraordinarily overbroad.[336/] There is nothing in the definition that limits broadband provider responsibility for data breaches only to instances in which CPI has been exfiltrated due to a penetration of, or unauthorized access to, data residing on a broadband service provider's network or storage facilities. Read literally, the rule could require a broadband service provider

---

334/ *See* 47 U.S.C. §§ 551(b); 338(i)(3). *See also NPRM* at ¶ 222 ("We recognize that while the Cable and Satellite Privacy Acts prohibit operators from using the cable or satellite systems to collect PII concerning any subscriber without prior written or electronic consent of the subscriber concerned, Section 222 does not contain an analogous provision regarding the collection of customer information").

335/ *PCAST Big Data Report* at xiii, 50.

336/ *NPRM* at ¶¶ 75 (Defining breach as "any instance in which 'a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information'").

to furnish notice of a breach anytime that anyone anywhere gains unauthorized access to CPI of the provider's customers – regardless of whether or not the broadband provider had anything to do with the breach.[337/] Under a strict reading of the Commission's proposed breach definition, broadband providers would be responsible for furnishing notice to affected consumers of a data breach in circumstances in which customer CPI residing on PCs is stolen from subscribers that unwittingly opened malware transmitted to them by their third-party email provider or downloaded from a third-party Web site they frequent.[338/]

Aside from the absence of common-sense and necessary limits to the breach definition and the notification obligation, the breach rules proposed in the *Notice* are still far too excessive and burdensome. Broadband providers should be required to assess whether a breach notice is required only in instances in which "individually identifiable" CPI in the possession or control of the ISP is breached. By contrast, the proposed rules require notification in the event of all breaches of CPI, whether or not individually identifiable. But there is no harm to consumers if the data accessed or acquired without authorization is not individually identifiable.

Further, in contrast to nearly all other data breach notification laws and proposals, the *Notice* does not propose any "trigger" for notification – such as causing economic harm or

---

337/ There are also unique constraints associated with potential breaches of data in transit. ISPs transport trillions of communications each day without knowing or examining the content transiting their systems. In order to identify whether a breach of their transport networks contains CPI, and ascertain the affected parties requiring notice, ISPs would need to overlay and continuously operate a massive traffic content monitoring and logging apparatus. Further, ISPs do not have a customer relationship with many persons whose data flows through their network, and therefore lack the means to give notice of a breach to such persons.

338/ The Commission appears to have reflexively lifted the definition of "breach" (minus the *scienter* limitation) from its current CPNI rules, *see* 47 U.S.C. § 2011(e), without accounting for the fact that, in contrast to telephone customer call record information – which is a very specific and narrow set of data that only telephone companies have access to – broadband customer CPI is possessed by, and accessible to, innumerable entities. Likewise, the Commission's definition fails to reflect the fact that the data elements defined as broadband CPI can be obtained by cyber criminals from consumers and other sources "without authorization" without any involvement with those consumers' broadband service provider.

identity theft to customers whose data is affected.[339/] Because the types of data included in the definition of CPI are so broad and the proposed rules' lack of any harms-based limitation on when a breach requires notification, the FCC has left open the possibility that broadband providers will be obligated to provide notice of a breach for instances in which there is no harm – because the breached data is not individually identifiable or where the breach occurs through no fault of the provider.[340/] The Commission's proposal also lacks an exception from the notification obligation in circumstances where the breached information is encrypted or otherwise unusable.[341/]

The 7-10 day notice timeframe proposed by the Commission is inflexible and unreasonable and would not give ISPs sufficient time to investigate and determine the nature and

---

339/ *See, e.g.*, Alaska Stat. § 45.48.010(c)(individual notification not required if "there is not a reasonable likelihood that harm… has resulted or will result from the breach."); Ariz. Rev. Stat. § 44-7501(L)(1)("Breach" requiring notification defined as only that which "causes or is reasonably likely to cause substantial economic loss to an individual."); Conn. Gen Stat. § 36a-701b(b)(1)(notification not required if "the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed."); Ark. Code § 4-110-105(d)(notification not required if "no reasonable likelihood of harm to customers."); Del. Code tit. 6, § 12B-102(a)(notice not required if "misuse" of personal information is not "reasonably likely" to occur); Fla. Stat. § 501.171(4)(c)(notification not required if "the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed."); Iowa Code §§ 715C.2(6)(notification not required if "o reasonable likelihood of financial harm to the consumers whose personal information has been acquired has resulted or will result from the breach."); Mich. Comp. Laws § 445.72(1)(notification not required if breach "has not or is not likely to cause substantial loss or injury to, or result in identity theft" of an individual.).

340/ For example, domain name information is to be considered CPNI, *NPRM* at ¶ 41, but domain name searches are typically done "in the clear" such that anyone in possession of a sniffer or other eavesdropping device could acquire domain name information from searches performed by ISPs customers through no fault of the ISP. IETF RFC 7626, *DNS Privacy Considerations*, at 7 (2015). Likewise, a wireless router automatically broadcasting its SSID and MAC address to compatible devices within range could potentially implicate the data breach definition as drafted in the *NPRM*. *See* Technical Appendix, at 24-26.

341/ *See, e.g.*, Alaska Stat. § 45.48.090(7); Ariz. Rev. Stat. § 44-7501(A); Ark. Code § 4-110-105(a)(1); Conn. Gen Stat. § 36a-701b(a); ."); Del. Code tit. 6, § 12B-101(1),(4); Fla. Stat. § 501.171(1)(g)(b)(2); Mich. Comp. Laws § 445.72(1)(a),(b); Data Security Act of 2015, S. 961, 114th Cong. § 3(3)(B) (2015); Data Security and Breach Notification Act of 2015, H.R. 1770, 114th Cong. § 5(10)(B).

scope of a breach before notice would be required. Such a timeframe would be among the most aggressive in any State or Federal law.[342/] Rather than impose a specific timeframe, the Commission should instead require that notice be provided to customers as expeditiously as practicable and without unreasonable delay - consistent with the time necessary to determine the scope of the breach, identify individuals affected, notify law enforcement and restore the reasonable integrity of the system. Further, any delays in notification requested by law enforcement in connection with its investigation should not be counted against the notice timetable.

G. The Commission Should Not Preemptively Bar Any Data Use Practice by ISPs

The *Notice* asks whether there are ISP privacy and data use practices that should be prohibited or subject to heightened privacy protections, and specifically calls out variable pricing based on data use permissions.[343/] It is fundamentally inconsistent with a harms-based framework for the Commission to prophylactically ban or uniquely restrict any otherwise lawful data use practice. By definition, the Commission lacks a record demonstrating the harm associated with such a practice and the justification for banning it under all circumstances – irrespective of the type of choice offered to consumers for engaging in the practice or the benefits that it provides. As ITIF notes, "[t]he opportunity to offer variable pricing based on data collection policies is potentially a boon for those looking for a lower-cost option to either get

---

342/ No state data breach notification law requires individual notification within less than 30 days of discovery of the breach. *See, e.g.*, Ark. Code § 4-110-105(a)(2)("in the most expedient time and manner possible and without unreasonable delay, consistent with… any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system"); Conn. Gen Stat. § 36a-701b(b)(1)(90 days notification); Ohio Rev. Code § 1349.19(B)(2)(45 days notification); Fla. Stat. § 501.171(4)(a)(30 days notification).

343/ *NPRM* at ¶¶ 256-62.

online or move towards a faster speed connection."[344/] Prophylactic restrictions lock in current business models and restrict new pricing offers and promotional discounts based upon data usage that could spur broadband adoption.

The *Notice* asks whether AT&T's Gigapower offering – which offers a discount from the monthly subscription fee in exchange for use of Internet activity data for purposes of serving ads and marketing offers – should be "permitted under the Communications Act."[345/] While implicitly conceding the popularity of the AT&T offering – noting that a "substantial majority" of customers have chosen to participate – and acknowledging the prevalence of such offers in the offline world, the Commission nonetheless proposes to weigh whether it should be banned.[346/]

It is ironic that the NPRM would suggest prohibiting this practice given Chairman Wheeler's observation, while voting to adopt the *Notice*, that: "Most of us understand that the social media we join and the websites we visit collect our personal information and use it for advertising purposes."[347/] This is, of course, nothing more than a discount regime - in which free use of social media, search, and Web content is exchanged for access to data for marketing and advertising purposes. There is simply no justification to prevent or restrict ISPs from engaging in conduct which the Commission finds otherwise acceptable when engaged in by large edge providers that dominate their segment of the market.[348/]

344/ *ITIF Broadband Privacy Report* at 6.

345/ *NPRM* at ¶ 259.

346/ *Id.* at ¶¶ 259-61.

347/ Statement of Chairman Tom Wheeler, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* WC Docket No. 16-106, Notice of Proposed Rulemaking, FCC 16-39 (2016).

348/ *See supra* at text accompany nn. 191-192 (noting Google controls 70% of the search marketplace while Facebook's share of social media log-ins exceeds 60%). Nor is there any justification for the Commission to prohibit mandatory arbitration clauses in their contracts with broadband service customers. Arbitration clauses are a common feature of consumer terms of service agreements across the

H. The Commission Should Not Adopt Special Rules Regulating ISPs' Use of the Content of Customer Communications

The *Notice* asks whether the Commission should prohibit, or adopt heightened restrictions for, use of deep packet inspection ("DPI") for purposes other than providing broadband services and reasonable network management of such services.[349/] There is no need to adopt special rules restricting use of DPI, or any other network management technology. While acknowledging that concerns had been raised about potentially problematic uses of DPI, the FTC decided not to adopt any specific recommendations,[350/] recognizing that "any privacy framework should be technology neutral" and other entities in the Internet ecosystem have access to similar data obtainable via DPI.[351/] DPI already serves a number of pro-consumer purposes, including detection and prevention of spam, malware, and phishing attacks and execution of parental controls and content filters requested by subscribers.

DPI also plays an integral role in network diagnostics and capacity planning. ISPs cannot plan for network growth, whether through new deployments or upgrades to existing infrastructure and technologies, without understanding how Internet traffic is growing and the uses to which it is put. DPI allows ISPs to analyze aggregate growth and usage changes in network traffic patterns over time, allowing for smarter, more cost effective, and more efficient network growth. Special rules for DPI are unnecessary.

---

economy and throughout the Internet ecosystem, and there is no equitable or legal basis for singling out ISPs and prophylactically banning arbitration clauses in broadband service agreements.

349/ *NPRM* at ¶ 264.

350/ *FTC Privacy Report* at 55-57.

351/ *Id.* at 56.

Nor is there any need to adopt special rules restricting ISP use of the content of customer communications.[352/] To the extent that customer content is linked to individually identifiable information, it would be protected under the regime adopted by the Commission, and hence special rules are not necessary. In any event, there is a well-established body of law under the Electronic Communications Protection Act (ECPA) regulating the circumstances under which ISPs and other electronic communications service providers can access the content of customer communications.[353/] There is no reason for the Commission to replace or supplement that body of law, and doing so would impose unnecessary regulatory burdens and risk consumer confusion through imposition of conflicting regimes.

III. THE COMMISSIONSHOULD HARMONIZE ANY PROPOSED BROADBAND PRIVACY RULES FOR ISPS WITH THE EXISTING FTC POLICY FRAMEWORK THAT GOVERNED THE BROADBAND SERVICES MARKETPLACE PRIOR TO RECLASSIFICATION

Assuming arguendo that the FCC has authority to erect broadband privacy rules, the Commission should establish a flexible, principles-based regime similar to the framework applied by the FTC to the rest of the broadband ecosystem. Under this approach, the new FCC regime would mean less disruption for both the marketplace and consumers, and the Internet ecosystem as a whole would be subject to comparable regimes – albeit enforced by different agencies. This approach also would dovetail with prior Commission admonitions against subjecting the broadband service marketplace to prescriptive rules that would stifle technological development, innovation, and new business models.[354/]

352/ *NPRM* at ¶ 137.

353/ Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (restrictions on ISP access and disclosure of stored content codified at 18 U.S.C. §§ 2701-2712).

354/ *Open Internet Order* at ¶¶ 246-47 ("[T]he process for providing and promoting an open Internet must be flexible enough to accommodate the ongoing evolution of Internet technology . . . . flexible rules,

A. The Internet Has Thrived Under a Unified Privacy Framework Applicable to All Entities in the Broadband Ecosystem

The virtuous cycle of investment and innovation in the broadband Internet ecosystem lauded by the Commission[355/] emerged under a uniform privacy framework applicable to all entities collecting and using online consumer data.[356/] The FTC Framework is technology-neutral and effectively balances the interest in safeguarding consumer privacy with promoting competition, investment, innovation, and consumer welfare. It is, as Chairman Wheeler described, a "terrific model" and "thoughtful, rational approach."[357/] By focusing on the context of a consumer's relationship with a business, the FTC model ensures not only that consumers' privacy expectations are met but also that businesses have the flexibility to compete and innovate both with their products and with their privacy protections.[358/]

The Commission should adopt a framework that replicates the FTC's successful approach to preserve uniformity of privacy obligations in the broadband ecosystem. The benefits of maintaining a unified privacy framework were recognized by the White House,[359/] which emphasized the following principles: (1) avoid "inconsistent standards for related technologies" that could dampen innovation;[360/] (2) foster a "level playing field for companies;" and, most

---

administered through case-by-case analysis, will enable us to pursue meaningful enforcement, consider consumers' individual concerns, and account for rapidly changing technology.").

355/ *Preserving the Open Internet*, Report and Order, 25 FCC Rcd. 17905, 17911, ¶ 14 (2010).

356/ *See FTC Privacy Report*; *see also FTC Preliminary Staff Report*, *supra* n. 135, at 3 (detailing the FTC's work from the 1990s onward to develop privacy frameworks, using a "flexible and evolving approach to privacy protection designed to keep pace with a dynamic marketplace").

357/ Margaret Harding McGill, *FCC, FTC Chiefs Zero In On Data Security, Privacy,* Law360, Jan. 6, 2016, *available at* http://www.law360.com/articles/743314/fcc-ftc-chiefs-zero-in-on-data-security-privacy (quoting FCC Chairman Tom Wheeler).

358/ *See FTC Privacy Report* at 27.

359/ *White House Privacy Framework*, *supra* n. 141, at 36.

360/ *Id.* at 6.

importantly, (3) create "a consistent set of expectations for consumers."[361/] A unified approach with consistent application of standards across the entire broadband ecosystem is the best way to implement these principles. Chairman Wheeler himself stated that consumers deserve "a uniform expectation of privacy"[362/] and that the Commission's approach should be "consistent with the kind of thoughtful, rational approach that the FTC has taken."[363/] The FCC and FTC can achieve the stated goal of their recent Memorandum of Understanding to avoid "duplicative, redundant or inconsistent oversight" by working in concert to administer and enforce the same basic framework throughout the entire Internet ecosystem.[364/]

A broadband privacy framework designed to preserve and enhance the virtuous cycle also must be dynamic and flexible; it cannot be composed of a set of static rules, but must instead be able to evolve and adapt to changes in technology, business models and consumer preferences.[365/] The FCC recognized the advantages of a "light-touch regulatory framework" in reclassifying broadband service as a Title II service by "expressly eschew[ing] the future use of

---

361/ *Id.* at 36.

362/ Hearing before the U.S. House of Representatives Subcommittee on Communications and Technology, "Oversight of the Federal Communications Commission," Preliminary Transcript at 141 (Nov. 17, 2015).

363/ Margaret Harding McGill, *FCC, FTC Chiefs Zero In On Data Security, Privacy,* Law360, Jan. 6, 2016, *available at* http://www.law360.com/articles/743314/fcc-ftc-chiefs-zero-in-on-data-security-privacy (quoting FCC Chairman Tom Wheeler).

364/ FCC-FTC Consumer Protection Memorandum of Understanding, at 1 (2015), https://apps.fcc.gov/edocs_public/attachmatch/DOC-336405A1.pdf. *See* Leibowitz & Neuchterlein, *The New Privacy Cop*, *supra* n. 138 (former FTC Chairman encouraging the FCC to "adopt a less rigid, more FTC-like approach to the privacy practices of ISPs.").

365/ Bamberger & Mulligan, *supra* n. 136, at 63 ("The shortcomings of command-and-control governance, however, are well recognized. Rules are notoriously both under- and over-inclusive, identifying certain relevant factors that can easily be codified, while ignoring others. Specific rules often cannot reflect the large number of variables involved in achieving multifaceted regulatory goals… For these reasons, reliance on compliance with a set of detailed provisions may frustrate, rather than further, underlying regulatory ends. Rule systems are inevitably incomplete, failing to provide guidance in a host of contexts, especially as circumstances change. At the same time, they can have detrimental effects on decisions within the organizations they govern").

prescriptive industry-wide regulation," and highlighting that such an approach has "facilitated the tremendous investment and innovation on the Internet."[366/] A prescriptive approach would adapt more slowly – if at all – to the rapidly changing Internet ecosystem, leading inevitably to unanticipated harms and lost innovation as technologists struggle to assess whether some new, heretofore unimagined, product or service complies with static rules that can become obsolete almost as soon as they are adopted.[367/]

A framework predicated upon flexibility, and in alignment with the approach applicable to the rest of the Internet ecosystem, would chiefly identify the primary privacy and security objectives to be achieved, while affording providers a wide range of latitude in achieving those goals. It would avoid dictating the specific methods and processes for compliance. This flexibility is "critical to the shaping of consumer-protection, rather than compliance-oriented, approaches to privacy" and allows the FCC to respond to "harmful outcomes… as the market, technology, and consumer expectations change."[368/]

366/ *Open Internet Order* at 5603, ¶ 5. *See also* Jon Sallet, *The Jurisprudence of Innovation*, Prepared Remarks at the FCBA Year in Review (June 23, 2014) ("Case-by-case enforcement offers a potentially more dynamic approach, permitting the Commission to respond to and learn from the rapid pace of change in the communications market.").

367/ *Ohlhausen 2014 Remarks*, *supra* n. 134, at 7-8 (highlighting the negative consequences that result from "prescriptive *ex ante* regulation['s]… knowledge-gathering challenges, including (1) "statutory, procedural, and resource constraints make it impossible for the regulator to continually update the rules, it is difficult for ex ante regulation to keep up with technological change;" (2) "ex ante regulations are an attempt at the almost impossible task of predicting the future, some harms will occur that were unanticipated;" and (3) "prescriptive ex ante regulations can hinder innovation.").

368/ Bamberger & Mulligan, *supra* n. 136, at 273.

B. The Proposed Industry Framework Represents the Best Approach to Harmonizing FCC Broadband Privacy Rules with the FTC's Framework

As the NPRM recognizes, 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."[369/] ISPs have strong incentives to earn and maintain their customers' loyalty by protecting their data,[370/] and the proposed industry framework reflects their considerable experience in adapting the well-established FTC privacy regime to the rapidly evolving online marketplace.[371/]

The aim of the industry approach is to combine strong protections for consumers with the flexibility that allows ISPs to satisfy their customers' expectations of continued access to innovative new services and customized offerings that enhance their experience. The industry framework also avoids consumer confusion by closely aligning with the FTC's approach to privacy, and therefore to the privacy regime applicable to other online services that consumers use. Consumers expect that their data will be subject to consistent privacy standards based on the sensitivity of their information and how it is used, regardless of which entity uses that data. The industry framework consists of the following elements:

369/ *NPRM* at ¶ 10. In fact, the FTC's approach has been so successful that "nearly all legitimate companies currently make detailed promises about their privacy practices." *Ohlhausen 2016 Remarks* at 8.

370/ *See supra* § II.B.

371/ *See NPRM* at ¶¶ 280-82. *See also* Letter from American Cable Association, Competitive Carriers Association, CTIA, National Cable & Telecommunications Association, & USTelecom to Chairman Tom Wheeler, Mar. 1, 2016 (attaching industry framework), *available at* https://www.ncta.com/sites/prod/files/Letter-PrivacyPrinciples-3-1-16.pdf.

Customer-Provider Relationship. The industry framework would apply only to CPNI made available by the customer to an ISP solely by virtue of the customer-provider relationship and only in connection with the provision of broadband service.[372/]

Individually Identifiable Data. Consistent with the express language of Section 222,[373/] restrictions would be imposed only upon ISPs' use or disclosure of "individually identifiable" CPNI.[374/] Any data that is de-identified, aggregated or does not otherwise identify a known individual is exempt from the framework. This includes de-identified data that is not part of a set of aggregated data.

Prohibits Unfair and Deceptive Practices. The proposed industry framework achieves parity across the Internet ecosystem by being grounded in the well-established prohibition against unfair and deceptive practices,[375/] in accordance with the existing protections consumers receive when they engage with other companies in the Internet ecosystem.[376/]

Under the industry framework, ISPs would adhere to the following principles in connection with their collection and use of broadband service customer data:

Transparency. ISPs should provide notice, which is neither deceptive nor unfair, describing the CPNI that they collect, how they will use the CPNI, and whether and for what purposes they may share CPNI with third parties.

372/ This effectuates Section 222's limitation that CPNI only includes information that is "made available to the carrier by the customer solely by virtue of the carrier-customer relationship." 47 U.S.C. § 222(h)(1).

373/ 47 U.S.C. §§ 222(c)(1), (c)(3), (h)(2).

374/ 47 U.S.C. § 222(c)(1).

375/ 15 U.S.C. § 45(a)(1).

376/ *See, e.g.*, *FTC Privacy Report* at 14, 21-22.

Respect for Context. ISPs will offer customers choice when intending to collect and use broadband service customer data in a manner that is not consistent with the context of the transaction in which the customer provides the data or when outside the context of the relationship between the ISP and customer. As the FTC has recognized, "companies do not need to provide choice before collecting and using consumers' data for practices that are consistent with the context of the transaction, consistent with the company's relationship with the consumer, or as required or specifically authorized by law."[377/] Consistent with the flexible choice mechanisms available to all other entities in the Internet ecosystem, ISPs would give consumers easy-to-understand choices for non-contextual uses and disclosures of their CPNI, where the failure to provide choice would be deceptive or unfair. The provider would be required to take account of the sensitivity of the data and the context in which it was collected when determining the appropriate choice mechanism.[378/]

Security. ISPs will maintain physical, technical, and administrative security safeguards, appropriate to the sensitivity of the information and the size and complexity of their data operations, to protect broadband service customer data that they collect or store.

Data Breach Notifications. ISPs should notify customers whose CPNI has been breached when failure to notify would be unfair or deceptive. ISPs are afforded flexibility to determine how and when to provide such notice, depending upon the facts and circumstances of the breach.

377/ *FTC Privacy Report* at iv, 48.

378/ *See FTC Privacy Report* at 49-50 (choice mechanisms "may differ depending on such considerations as the nature or context of the consumer's interaction with a company or the type or sensitivity of the data at issue.").

Consistent with the FTC's approach, the Commission can ensure compliance with these principles by pursuing reasonable enforcement actions against ISPs that violate these principles. In coordination with other privacy regulators, the FCC could, like the FTC and various states like California, provide additional guidance on how it interprets its framework through workshops or reports. The FCC also could encourage and support the development and implementation of industry guidelines.

CONCLUSION

For the reasons set forth herein, the Commission should decline to adopt the rules proposed in the NPRM. *Assuming arguendo* the Commission has any authority to adopt broadband privacy rules, it should adopt an approach similar to the industry model discussed *supra* in Section III, which is closely aligned with the successful and effective FTC Framework.

Respectfully submitted,

/s/ Rick Chessen

Rick Chessen
Loretta P. Polk
Jennifer K. McKee
National Cable & Telecommunications Association
25 Massachusetts Avenue, N.W. – Suite 100
Washington, D.C. 20001-1431

William A. Check, Ph. D
Senior Vice President
Matthew Tooley
Vice President of Broadband Technology
Science & Technology

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

May 27, 2016

APPENDIX A

TECHNICAL REVIEW OF THE PROPOSED CPNI RULES FOR BROADBAND

William A. Check, Ph.D. and Matt Tooley

May 27, 2016

APPENDIX

TECHNICAL REVIEW OF THE PROPOSED CPNI RULES FOR BROADBAND

William A. Check, Ph.D. and Matt Tooley[1]

EXECUTIVE SUMMARY

This paper provides a technical analysis of the proposed Customer Proprietary Network Information (CPNI) rules for broadband. In particular, it examines the proposed parameters and types of information being considered as CPNI by the Commission, and discusses, from a network engineering and operations perspective, the impact to the Internet Service Providers (ISPs) and end-users.

In examination of this topic, the history of the evolution of privacy within the Internet is reviewed with the corresponding work of the Internet Engineering Task Force (IETF). In the early days of the Internet, the IETF's focus was on operational issues such as routing, TCP performance and network management. The IP address was often at the heart of solutions and innovations in these areas because it was ubiquitously employed as the means of defining origination points and end points across the network. Privacy and security were deemed to be in the domain of applications and end-user protocols. The rigid privacy rules that the Commission proposes to impose on ISPs – and, by extension Internet network architecture as a whole – do not encourage the kind of innovation that has taken place within the IETF and are not in line with the manner in which the Internet was founded and has evolved.

---

[1] William A. Check, Ph.D. is Senior Vice President, Science and Technology and Chief Technology Officer at the National Cable & Telecommunications Association (NCTA). Matt Tooley is Vice President, Broadband Technology at the NCTA.

In the *Privacy NPRM*, a broad range of information is proposed by the Commission to meet the statutory definition of CPNI; some of which – such as IP addresses and MAC IDs – are at the core of basic Internet functionality.[2] This Appendix provides a number of use cases illustrating the effects of such a categorization and includes: email, IPv6, Internet of Things, DNS, MAC addresses, cybersecurity, peer-to-peer networking, network routing, bundled services and applications, and future technologies. The use cases illustrate the following:

- ***Email*** – Whenever a user sends an email, their email provider must append the client IP address in the email header. The FCC's proposed rules could require ISPs to solicit and obtain approval to share the IP addresses to send email from an ISP-provided email account.
- ***IPv6*** – The Commission's proposed privacy rules conflict with how IPv6 addresses are created and assigned. IPv6 devices can rely on using a device's MAC address to derive a unique IPv6 address.
- ***Internet of Things (IoT)*** – Cybersecurity is going to be key to the management of compromised IoT devices. Much of it will be based on the device's IP and MAC addresses, as well as traffic analysis. Moving forward, IoT devices will likely have both IPv4 and IPv6 addresses, and therefore will also experience many of the previously noted problems with IPv6. ISP-provided IoT services (for example home security) are supported through a proxy server. Complying with the Commission's proposed rules could require ISPs to solicit and obtain approval to

[2] *See* 47 C.F.R. § 222 (h)(1). CPNI is defined to mean "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship" and "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer or a carrier", except it does not include "subscriber list information".

share IP and MAC address for the devices from their customers as part of delivering the service.

- ***DNS*** – The Commission is proposing that the domain names that an end user communicates with be treated as CPNI. But ISPs must disclose in the directory service for each end-point on their network the IP address assigned and the assigned hostname. The proposed rules potentially could require ISPs to solicit and obtain their customer's approval to share this information with third parties to make DNS work properly.
- ***MAC Addresses*** – There are several issues with treating MAC addresses as CPNI: 1) The MAC address is changeable by a user and therefore does not always uniquely identify a device. Conversely, it is incorrect to assume that a MAC address can be used to uniquely identify a device. 2) It is incorrect to state categorically that ISPs use MAC addresses to route data packets; they use MAC addresses to forward datagrams at the link-layer in the last hop to the end-user's device. 3) Devices disclose and share their MAC address as part of the link-layer protocols when communicating with many other devices, and therefore information about MAC addresses is not unique to ISPs. 4) MAC addresses are broadcast by all WiFi devices (such as iPhones, Android devices) and WiFi access points.
- ***Cybersecurity*** – The *Privacy NPRM* does include a proposed carve-out for cybersecurity, but even with this carve-out, the Commission's broad definition of CPNI is counter to President Obama's recent cybersecurity Executive Order and the Cybersecurity Information Sharing Act (CISA). The proposed rules would make it harder to share cybersecurity information with researchers and partners.

Further, it would make it harder for ISPs to bundle anti-malware software with their Internet service. Cybersecurity information sharing would effectively be discouraged due to the lack of clarity regarding when and what cybersecurity information can be shared under the proposed definitions of CPNI and PII. Fundamental to cybersecurity practices is the ability to share data on how the network is being used, and the proposed rules could weaken many effective defensive mechanisms for preventing spam and botnets, as well as impeding information sharing practices.

- ***Peer-to-Peer Networking*** – Peer-to-peer (P2P) networking is a distributed application architecture that divides the work across multiple peers, in contrast to client-server architecture, which divides the work by assigned function. For any application that relies on a P2P overlay network to communicate, the device must share its IP address so that others can communicate with it directly. As a result, ISPs potentially could be required to solicit and obtain approval from end-users before they could utilize an ISP's P2P application that the end users wants to run.
- ***Network Routing*** – Routing between networks is fundamental to the operation of the Internet and is accomplished using the Border Gateway Protocol (BGP). When networks interconnect, they announce their routers to each other using BGP, which contain blocks of IP addresses that are reachable via the network. Network route announcements using BGP could clearly be affected by the Commission's broad definition of CPNI which includes IP addresses.
- ***Multiplayer Games*** – An extremely popular class of applications is multi-player gaming. These applications can be based on different designs such as local servers, quasi-peer-to-peer, or centralized architectures, which could result in the

users affected by the proposed CPNI. Further, as games progresses, the host server may be dynamic and change during a game. The assumptions of what CPNI would be needed at the start of a game may change during the game. ISP gaming offerings available to broadband customers could be inhibited by the proposed rules.

- ***Bundled Services*** – ISPs often provide additional products and services that complement the Internet service they are offering. These services may be tied to the location where the Internet service is being delivered and rely upon the MAC address or IP address that is assigned to the modem terminating the Internet service, which needs to be shared with the third party delivering the service. In their current form, the privacy rules proposed by the Commission could require a ISP to solicit and obtain the customer's approval to provide these kinds of services.
- ***Future Services and Applications*** – How networks are architected, designed, and deployed are on the cusp of some revolutionary changes. Software Defined Networks (SDN), Network Function Virtualization (NFV), and Information-centric networking are but a few of the new concepts. The *Privacy NPRM* is silent on the evolution of any new technologies. Rigid rules rarely have the effect of spurring innovation and, as a technical matter, it is concerning how rigid CPNI rules could impact the innovation of new features. The Commission does not address or account for the inevitability of such evolution in its proposed broadband privacy rules.

General trends can be observed from the foregoing use cases. First, from an engineering perspective, for those operating broadband Internet access networks there would be uncertainty

over what uses are subject to customer approval under the Commission's CPNI rules and what are not. Second, end-users could be adversely impacted, as they would be suddenly required to make decisions on low-level technical details about which end users have little knowledge. This would result in complexity and confusion to end-users who would be required to decide how their data is used for base-level technical functionality without understanding the consequences. For the general public, confusion would abound with such questions as:

- The difference between the rules for ISP's email and edge-user email like Hotmail and Gmail?
- Which IPv6 algorithm should the end-user choose to get an IPv6 address for their laptop?
- The difference between the rules for an ISP's DNS service and a third-party DNS provider?
- Why there are rules for how a ISP's Wi-Fi operates and a none for a non-BIAS provider's Wi-Fi?
- How is an end-user to know if the application they are using is based on Peer-to-Peer networking and covered by the new rules?
- How the rules impact routing practices (i.e. BGP) and the use of their IP address block?

While these questions may sound far-fetched, they are, in reality, the potential impact of the proposed rules that network engineers and operators must grapple with. And, it raises additional problems. For instance, the general public would likely not know who to even contact with questions that may arise about the issues: the device manufacturer, the ISP, the retail store where the CPE equipment was purchased, or a third-party company's application or service they are trying to access or use via a broadband transmission.

It should be emphasized that the use cases presented in this paper are not exhaustive. While it lists a number of functions as use cases, it simply is not feasible to identify every current or future use case – there will be many more. Similarly, and more troubling, in the NPRM the Commission itself delineates a broad list of data elements subject to the proposed CPNI rules, but states that they are just "non-exhaustive examples" of the types of information that could be considered CPNI in the broadband context. While the Commissions does state that its proposed broadband privacy rules are based upon the narrow definition of BIAS in the *Open Internet Order*, the term "closely-related service" is not defined in this context and the Commission does not explain whether and when an ISP providing an integrated bundle of BIAS and non-BIAS services and capabilities to its customers should be viewed as acting as a BIAS provider subject to the rules and when it should be seen as a provider of "other services" not subject to the rules.

Moreover, an item-by-item exemption of specific cases for the purposes of CPNI would be technically risky and would be relying upon "freezing" the Internet in its current state today, picking case-by-case from a non-exhaustive list of potential parameters, and implicating any future innovation to be covered under CPNI. This would only have the effect of creating rigid rules that would hinder certain use cases, while encouraging others – in other words – picking winners and losers on the direction of current and future technologies of the Internet.

BACKGROUND

"The Internet architecture, the grand plan behind the TCP/IP protocol suite, was developed and tested in the late 1970s by a small group of network researchers."[3] The architecture was based upon an open-system approach to the development of the protocols and

[3] D. Clark, L. Chapin, V. Cerf, R. Braden, R. Hobby, *Towards the Future Internet Architecture - RFC 1287*, DOI 10.17487/RFC1287 (Dec. 1991) *available at* http://www.rfc-editor.org/info/rfc1287.

upon the end-to-end principles of system design with the primary areas of focus being routing, TCP performance, and network management.[4] At the time, the Internet was small and assumed a level of trust by all those connected and therefore privacy and security were not the focus. The first privacy guidelines were published by the Internet Engineering Task Force (IETF) in 1987 in Request for Comment (RFC) 989[5] and the first real Internet security guidelines were published in 1991 in RFC 1281,[6] nearly 20+ years after the Internet was developed.

As noted in RFC 6274, the Internet protocol inherently "leaks" information.[7] The leakage of information is not limited to the underlying Internet protocols but also in the applications themselves. A study released in 2011 asserts that edge providers need to take greater responsibility for privacy protection.[8] In January 2016 at the FTC's Privacy Con, Sarthak Grover and Nick Feamster of Princeton University gave a presentation stating that information leakage was not limited to the Internet protocols and applications, but also could be traced to the way in which many Internet of Things (IoT) devices operate.[9]

What has made the Internet successful has been its openness and free-market approach to development that is best captured in the IETF's credo: "We reject: kings, presidents, and voting.

---

[4] B. Carpenter, *Architectural Principles of the Internet - RFC 1958*, DOI 10.17487/RFC1958 (Jun. 1996), *available at* http://www.rfc-editor.org/info/rfc1958 (*"RFC 1959")*.
[5] J. Linn, *Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication procedures - RFC 989*, DOI 10.17487/RFC0989 (Feb. 1987), *available at* http://www.rfc-editor.org/info/rfc989.
[6] R. Pethia, S. Crocker, and B. Fraser, *Guidelines for the Secure Operation of the Internet - RFC 1281*, DOI 10.17487/RFC1281 (Nov. 1991) *at* http://www.rfc-editor.org/info/rfc1281.
[7] F. Gont, *Security Assessment of the Internet Protocol Version 4 - RFC 6274*, DOI 10.17487/RFC6274 (Jul. 2011), *available at* http://www.rfc-editor.org/info/rfc6274.
[8] B. Krishnamurthy, K. Naryshkin, and C. Wills, *Privacy leakage vs. Protection measures: the growing disconnect* (2011), *available at* http://w2spconf.com/2011/papers/privacyVsProtection.pdf.
[9] S. Grover, N. Feamster, *The Internet of Unpatched Things* (2016), *available at* https://www.ftc.gov/system/files/documents/public_events/776191/part_5_privacycon_slides.pdf.

We believe in: rough consensus and running code."[10] Innovation in applications has been a result of application developers and network engineers having the latitude to explore and try new things. Central planning, top-down directives, and government-mandated processes were antithetical to this spirit. Instead of trying to develop one set of security and privacy rules for all users of the Internet, the Internet opted to leave that up to the end-users themselves as noted by the Internet Architecture Board (IAB) in RFC 1958: "confidentiality and authentication are the responsibility of the end users and must be implemented in the protocols [and applications] used by the end users."[11] Applications carrying sensitive information that needed to be protected took measures to protect the data. Examples of this include email (Secure SMTP),[12] secure browsing (HTTPS),[13] and secure packet delivery (IPSEC).[14]

Many applications and protocols such as email, IPv6, domain name system, and cybersecurity applications that end-users make use of today may not have come to fruition if rigid privacy rules impeding the disclosure of information as proposed in the FCC's *Privacy NPRM* had been in place. In this Appendix, use cases are presented to illustrate the harmful effects of the FCC's proposed categorization of certain information as CPNI.

The Internet Society's paper, "The Internet and the Public Switched Telephone Network" discusses the differences between a Public Switched Telephone Network (PSTN) and the Internet. In the paper, they describe the aspect of "Innovation without requiring permission (by anyone):

---

[10] A. Russell, *IEEE Annals of the History of Computing*: Rough Consensus and Running Code and the Internet–OSI standards War (Jul. 2006).
[11] RFC 1958 at 5.
[12] P. Hoffman, *SMTP Service Extension for Secure SMTP over TLS - RFC 2487*, DOI 10.17487/RFC2487 (Jan. 1999), *available at* http://www.rfc-editor.org/info/rfc2487.
[13] E. Rescorla, and A. Schiffman, *The Secure HyperText Transfer Protocol - RFC 2660*, DOI 10.17487/RFC2660 (Aug. 1999), *available at* http://www.rfc-editor.org/info/rfc2660.
[14] R. Atkinson, *Security Architecture for the Internet Protocol - RFC 1825*, DOI 10.17487/RFC1825 (Aug. 1995), *available at* http://www.rfc-editor.org/info/rfc1825.

> **Internet:** Any person or organization can set up a new service that adheres to open and collaborative standards, and make it available to the rest of the Internet, without requiring special permission. The best example of this is the World Wide Web – which was created by a researcher in Switzerland, who made his software available for others to run, and the rest, as they say, is history.
>
> **PSTN:** Only telecoms companies can define and deploy new services within their networks."[15]

This illustrates the fundamental ability of the Internet to be open and collaborative. By specifying rigid CPNI parameters, the proposed FCC Privacy NPRM does not support an open and innovative Internet, but rather forces a PSTN framework on the Internet.

In the *Privacy NPRM*, the Commission considers various types of information to constitute CPNI in the broadband context:[16]

- Broadband service plans
- Geo-location
- Media Access Control (MAC) addresses and other device identifiers
- Internet Protocol (IP) addresses and Domain Name information
- Traffic statistics
- Port information

The Commission also asks for additional comment on what other information should be considered CPNI, such as:

- Application headers (including for Web browsing and email)
- Application usage

---

[15] Internet Society, *The Internet and the Public Switched Telephone Network*, *available at* http://www.internetsociety.org/sites/default/files/The%20Internet%20and%20the%20Public%20Switched%20Telephone%20Network.pdf.

[16] *In re Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, WC Docket No. 16-106, FCC 16-39 ¶ 41-55 (rel. April 1, 2016) ("*Privacy NPRM*").

- Customer premise equipment (CPE) information
- Anything else they missed

TECHNCIAL IMPLICATIONS

The following are technical use case examples showing the consequences of defining a number of parameters as CPNI information. This is not intended to be an exhaustive list – there will be others. But, it provides insight into the complexities and implications of the proposed classifications to ISPs and end-users.

1. Email

Email was the first "killer application" of the Internet. Email is a messaging system based on the store and forward concept. Conceptually email is modeled after postal mail. Just as with postal mail, every message has a destination or "To:" address and a return or "From:" address in the form of *end-user@example.com*. Instead of post-offices that process the mail, email relies on email servers and clients. An end-user makes use of a client to send email messages and the recipient end-user relies on her server to receive the email. Clients use the Simple Mail Transfer Protocol (SMTP) [17] to send the email messages to from the end-user's email provider, when can be the end users ISP of choice. Servers rely on the Post Office Protocol (POP) or Internet Message Access Protocol (IMAP)[18] to receive the emails from the email server.

[17] J. Klensin, *Simple Mail Transfer Protocol - RFC 5321*, DOI 10.17487/RFC5321 (Oct. 2008), *available at* http://www.rfc-editor.org/info/rfc5321.
[18] M. Crispin, *INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1 - RFC 3501*, DOI 10.17487/RFC3501 (Mar, 2003), *available at* http://www.rfc-editor.org/info/rfc3501.

To properly route an email, the email server then examines the example.com portion (in the generic example of *end-user@**example.com**)* of the "To:" address to determine the name of the email server of the recipient and then uses the DNS protocol to lookup the IP address of the recipient's email server that is known as the MX record. The SMTP client then establishes a direct connection to the destination SMTP server and asks if the server has a mailbox for the recipient's local address (in the example, the local address is the "end-user" in the **end_user**@example.com). If there is a mailbox for the recipient, then the email message is forwarded to the recipient's email server for it to be stored until the recipient reads it with their email client of choice.

For this all to occur, a number of things must happen behind the scenes within the email servers. Every email includes a header and a body with the actual message. The header is not normally displayed by the email client, but contains important information used by the email servers to ensure the proper delivery of the email message. Figure 2 is a sample email header, and Figure 3 is a sample email header via Webmail. There are many fields that can be in the email header – some are mandatory and others optional. Every email header includes one or more "Received:" lines that show the path the email took from the sending server to the destination server. Per the SMTP protocol, an email server is required to append the email client's IP address in the email header. This is very much the same way the post office postmarks every piece of mail that it receives. The inclusion of the client's IP address in the header aids in the proper routing of the email and authentication of the email.

The sender's IP address may also be added in a field called X-Originating-IP or one of its derivatives (i.e. X-AOL-IP, X-EIP, X-SENDER, X-SENDER-IP). This field is an extension to the original SMTP protocol and is to mitigate SPAM.

Figure 1 E-Mail Header

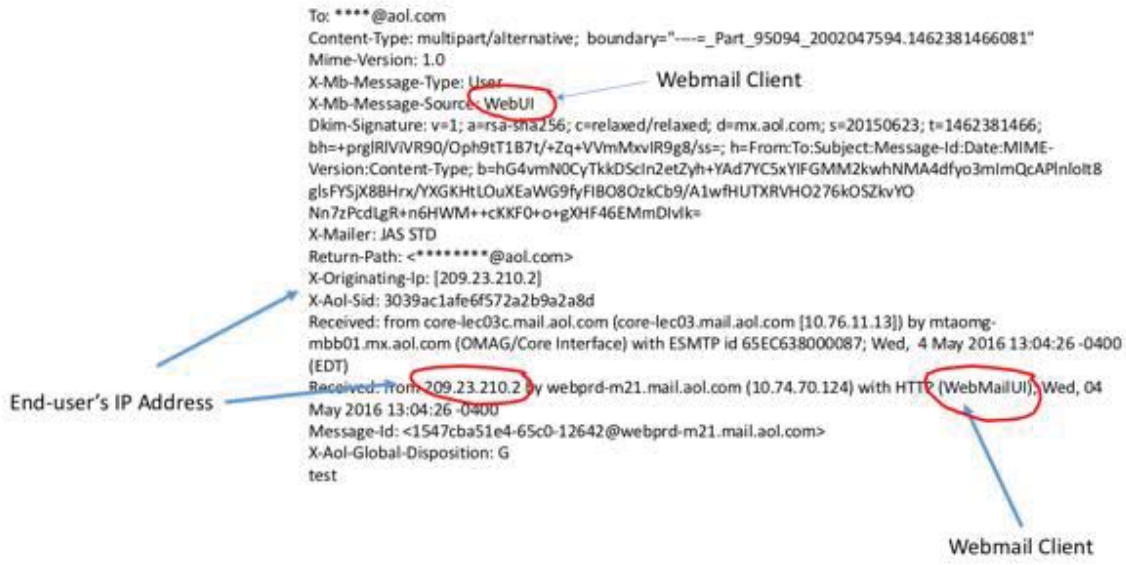

Figure 2 E-Mail Header via Webmail

There are two significant points to note about email:

1) The ISP must append the client IP address in the email header whenever a user sends an email using the ISP's email service. This is true regardless of whether they are using a standalone client (e.g. Outlook, Thunderbird) or webmail client.
2) The ISP's email server must disclose whether an email address exists to the sending email server as part of the sending process. Every destination email server as part of the email delivery process must disclose the existence of the email address on the server.

The rules proposed in the *Privacy NPRM* potentially would require soliciting and obtaining an end-user's approval for common uses of IP addresses associated with ISP email service, and significantly change the way millions of end-users using ISP email are accustomed to making use of email today.

2. IPv6

IP addresses locate endpoints on the network[19] and are assigned by the ISP to the customer devices. The Commission's proposed privacy rules are in conflict with how IPv6 addresses are assigned and used. IPv6 is the most recent version of the Internet Protocol (IP).[20] IPv6 is an update to the widely used IPv4. IPv6 was officially adopted by the IETF in 1998 and greatly expands the number of IP addresses available by using 128-bit addresses instead of the 32-bit addresses used by IPv4. In addition to a needed increase in the number of IP addresses, IPv6 was designed to simplify address assignment, streamline IP packet header processing by routers, and support mobility.

[19] J. Postel, *Assigned numbers - RFC 770*, DOI 10.17487/RFC0770 (Sept. 1980), *available at* http://www.rfc-editor.org/info/rfc770.
[20] J. Postel, *Internet Protocol, STD 5 - RFC 791*, DOI 10.17487/RFC0791 (Sept. 1981), *available at* http://www.rfc-editor.org/info/rfc791.

The Commission's proposed broadband privacy rules could interfere with how IPv6 addresses are created and assigned. In the *Privacy NPRM* the Commission proposes that MAC addresses should be viewed as CPNI and PII and therefore require a customer's consent prior to their disclosure to third parties. IPv6 was designed to re-emphasize the end-to-end principles of the Internet[21] and for each device on the network to have a unique address globally reachable from any other location on the Internet. This underlying goal in turn led to IPv6 relying heavily on using a device's MAC address to derive a unique IPv6 address.

IPv6 supports four different methods for assigning IP addresses to end-points:

- *Static address assignment* – Each end-point is assigned a permanent unique IP address. Often this is done manually by configuring the device with the IP address.
- *Stateless Address Auto Configuration (SLAAC)*[22] – An end-point generates its own IP address by first listening to the network and learning the network portion of the address, the upper 64 bits; and appending to that a unique 64-bit number. The initial version of SLAAC (RFC 2462[23]) suggested that this unique number be based upon the end-point equipment's MAC address. Since then SLAAC was updated by RFC 4941[24] to allow the end-point to choose its own method for generating a unique identifier, but many implementations still derive it from the end-point equipment's MAC address. The 64-bit network number together with the device generated 64-bit number together form a unique 128-bit IPv6 address.

[21] B. Carpenter, *Architectural Principles of the Internet - RFC 1958*, DOI 10.17487/RFC1958 (Jun. 1996), *available at* http://www.rfc-editor.org/info/rfc1958.
[22] S. Thomson, T. Narten, and T. Jinmei, *IPv6 Stateless Address Autoconfiguration - RFC 4862*, DOI 10.17487/RFC4862 (Sept. 2007), *available at* http://www.rfc-editor.org/info/rfc4862.
[23] S. Thomson and T. Narten, *IPv6 Stateless Address Autoconfiguration - RFC 2462*, DOI 10.17487/RFC2462, (Dec. 1998), *available at* http://www.rfc-editor.org/info/rfc2462.
[24] T. Narten, R. Draves, and S. Krishnan, *Privacy Extensions for Stateless Address Autoconfiguration in IPv6 - RFC 4941*, DOI 10.17487/RFC4941 (Sept. 2007), *available at* http://www.rfc-editor.org/info/rfc4941.

- *Stateless DHCPv6* – Similar to SLAAC, except that the Dynamic Host Control Protocol (DHCP) is used by the end-point to get other configuration options such as DNS server, network time server, trivial file transfer protocol (TFTP) server, etc.
- *Stateful DHCPv6*[25] – The end-point is assigned an IPv6 and other configuration options from an IPv6 address server, the DHCP server. The DHCP server manages all the IP address assignments for a network. End-points identify themselves to the DHCP server by sending a unique identifier to the server. This unique identifier can be in one of three forms: 1) MAC address plus a time value, 2) a vendor assigned unique number (e.g. MAC, EMEI, etc.), or 3) a MAC address. The DHCP server uses this unique ID to authenticate and assign a unique temporary IPv6 address.[26]

SLAAC was updated by RFC 4941 to address two privacy concerns with IPv6. The first was the use of the MAC address in the IPv6 address. The second was the concern with a persistent globally unique address being associated with a device. The first was addressed by allowing devices to choose their own method for generating a unique identifier instead of using their own MAC address in their self-generated IPv6 address. The second concern was addressed by modifying SLAAC to have the device periodically auto-generate a new IPv6 address for itself to make it more difficult for websites to track devices by their IP addresses.

Most consumer equipment defaults to using SLAAC for its IPv6 assignment. Therefore, for many ISPs the common practice is that residential users' CPEs defaults to use SLAAC to auto-generate their IPv6 addresses after their home gateway has obtained its IPv6 addresses from

[25] J. Arkko, G. Kuijpers, H. Soliman, J. Loughney, and J. Wiljakka, *Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts - RFC 3316*, DOI 10.17487/RFC3316 (Apr. 2003) ("*RFC 3316*"), *available at* http://www.rfc-editor.org/info/rfc3316.

[26] IP addresses assigned or leased by a DHCP server are referred to as dynamic and must be periodically updated. They are also temporary as they can and do change every time they are updated. The update period can be as short as a few minutes to as long as days or weeks.

the ISPs DHCPv6 server. As noted earlier, many of today's operating systems default to using IPv6 privacy extensions.[27] But there are still many operating systems deployed in the field that do not, and the privacy extension feature can be disabled.

The Commission's proposal to treat IP addresses as CPNI could create a conflict with how IPv6 works. Even with the codification of RFC 4941 by the IETF, there are still a number of instances in which IPv6 addresses will be auto-populated with IDs – and therefore disclosed automatically – under the address assignment protocol since not all devices are guaranteed to comply with RFC 4941.

This is a difficult situation to resolve without devices being "Plug and Play", which consumers expect their devices to be, to address this issue. It is hard to imagine that the general public would be able to understand the issue, and determine what corrective action to take. Indeed, the general public would likely not know whom to even contact about the issue: the manufacturer, the ISP, the retail store where the CPE equipment was purchased, or the web applications company.

3. Internet of Things

A related issue with IPv6 is the Internet of Things (IoT). As the growth of IoT devices rapidly increases, it is noted that these devices will experience at least the same challenges as in the IPv6 section above. IoT devices, like many evolving devices on the Internet, will have both IPv4 and IPv6 addresses. Typically, IoT devices tend to be more "Plug and Play" and simplify any setup interaction with the user as many IoT devices do not and will not have a user interface that supports complex user interactions. Asking users what method they want to use to assign

[27] The fact that devices that do comply with RFC 4941 and change their IPv6 addresses periodically would also draw into question whether an IPv6 address is something that can be linked to a user.

IPv6 addresses in their IoT device is contrary to the simplicity and the "Plug and Play" intent of these devices, resulting in a less consumer-friendly and consumer-oriented interaction. Examples of IoT devices with simple or no user interface include such items as door bells, wireless network attached cameras, thermostats, garage door openers, and pet feeders.[28]

IoT and Cybersecurity

Going forward, IoT is also going to present issues around privacy and security. For example, detection of devices is going to be key to the management of compromised IoT devices. That may be based on the device's IP address and MAC address, as well as traffic analysis. The effectiveness of detection will be also based on the sharing of data between service providers. It is already hard enough to get vendors of IoT devices to conform to any standards, and getting them to offer opt-in mechanisms will be difficult.[29] Many consumers will have no idea that the IoT devices are in fact devices that communicate and compute, they largely think they are "Plug and Play." To the extent ISP-provided IoT devices rely on uses or disclosures of IP addresses or other identifiers for operational or security monitoring purposes, they may trigger application of the privacy rules.

4. DNS

In the *Privacy NPRM*, the Commission is proposing that the domain names with which an end user communicates with be treated as CPNI.[30] The domain name system (DNS) is the

[28] *See* Ring Electronic Door Bell, at https://ring.com/setup; Nest Cam, at https://nest.com/camera/meet-nest-cam/ (security camera); Nest Thermostat, at https://nest.com/thermostat/meet-nest-thermostat/; Chamberlain MyQ Garage, *MyQ Garage, at* http://www.chamberlain.com/smartphone-control-products/myq-garage/model-myq-g0201 (connected garage door opener); FeedAndGo, *Automatic Pet Feeder, at* http://www.feedandgo.com/.

[29] Christopher Null, The state of IoT standards: Stand by for the big shakeout (Sept. 2, 2015), *available at* http://techbeacon.com/state-iot-standards-stand-big-shakeout.

[30] Privacy NPRM ¶ 46.

directory service for the Internet[31] and provides three key functions for the operation of the Internet:

1) *Forward DNS* - Forward DNS is the function most commonly associated with DNS. Forward DNS is the lookup of an IP address for a hostname or domain.
2) *Reverse DNS* – Reverse DNS is the lookup of a hostname or domain by IP address.
3) *DNS Load Balancing* – Distributing Internet traffic across multiple hosts all with the same hostname.

The IETF considers the DNS data itself and the results of a DNS query to be public[32] and a single or sequence of transactions to be private.

It is not always well understood how DNS actually works and how these three functions are used for more than just simple lookups. First, all DNS transactions today are in clear-text, meaning they can easily be viewed by any eavesdropper[33] (i.e. the equivalent of having a conversation with someone while walking down a public street), though work at the IETF is close to standardizing a method to protect the privacy DNS queries.[34] Second, devices have local DNS resolvers that cache DNS requests, meaning that not all DNS requests by a device are actually sent to the end user's DNS server. And with the Commission's proposal in the *Privacy NPRM* to expand the definition of CPE to include computers, routers, smartphones, and tablets,[35] it is unclear whether the domain name information that is cached on the end user's device would be covered.

---

[31] See, e.g. James. F. Kurose & Keith W. Ross, *Computer Networking* at page 130 (6th ed. 2013).
[32] S. Bortzmeyer, *DNS Privacy Considerations - RFC 7626*, DOI 10.17487/RFC7626 at 5 (Aug. 2015), *available at* http://www.rfc-editor.org/info/rfc7626.
[33] *Id.* at 7.
[34] Z. Hu, L. Zhu, J. Heidemann, A. Mankin, D. Wessels, and P. Hoffman, *Specification for DNS over Transport Layer Security (TLS) - RFC 7858*, DOI 10.17487/RFC7858 (May 2016), *available at* http://www.rfc-editor.org/info/rfc7858.
[35] Privacy NPRM ¶ 52.

A recommended best practice is every IPv4 Internet host should have a matching reverse DNS lookup as applications like email use something called Forward-confirmed reverse DNS

-**--*-ip-static.---.biasprovider.net

Figure 3 Example Encoded DNS Hostname

(FCrDNS) or full-circle reverse DNS as a form of authentication as part of the Sender Policy Framework (SPF)[36] to ensure there is a valid relationship between the owner of a domain name and the owner of the network. Further, there is a common host naming convention described in RFC 1011, DNS Encoding of Network Names and Other Types,[37] for how to encode in the hostname a set of mappings such as the IP address, network name, organization, and even geo-location to aid in troubleshooting network issues.

As result, to make the Internet operate, ISPs must disclose in their DNS servers for each end-point on their network the IPv4 address assigned and the assigned hostname that by convention has embedded in it a number of service attributes. In addition, as part of the contract that ISPs have with their regional Internet registry (RIR) (e.g. American Registry for Internet Numbers (ARIN) for U.S. ISPs) have contact information entered for IP address blocks into the shared Whois[38] project. For many ISPs, when they register an IP block, they will put in additional information (e.g. location, abuse contact information) to assist others who need more information about this block of IP addresses for purposes such as troubleshooting email, incident response, contacting network administrators, and obtaining the location of and contact information for businesses for common commercial purposes.

---

[36] S. Kitterman, *Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1 - RFC 7208*, DOI 10.17487/RFC7208 (Apr. 2014), *available at* http://www.rfc-editor.org/info/rfc7208.
[37] J. Reynolds and J. Postel, *Official Internet protocols - RFC 1011*, DOI 10.17487/RFC1011 (May 1987), *available at* http://www.rfc-editor.org/info/rfc1011.
[38] *Whois*, at http://whois.arin.net/ui/

Large content providers and content delivery networks (CDNs) are built with multiple servers working in clusters and often geographically dispersed. DNS is one of the methods used by large content providers and CDNs to distribute the load across their infrastructure. Large content providers and CDNs use DNS by using the IP source address of the DNS request and then trying to guess the location of the end-user to map the end-user to the closest server.[39] The method is prone to errors, especially when end-users use a DNS service other than the one provided by their ISP, that can cause the user to be mapped to a less than optimal server and that can lead to network delivery issues (e.g. choppy video). To address this, the IETF has been developing an update to DNS, EDNS-Client-Subnet DNS extension (ECS)[40] that will include the IP address information of the original query issuer in the query to the authoritative DNS server.[41] Supporting ECS requires DNS operators to update their DNS servers, including those operated by ISPs, to support appending the end-users IP or subnet in the DNS request to the authoritative DNS server. By doing so, the content provider or CDN can more accurately map the Internet end-point of the end user to its network resources.

As proposed, the rules in the *Privacy NPRM* could potentially require a ISP to solicit and obtain approval to share this CPI with third parties to make DNS work properly. In addition the new rules stifle Internet innovation from groups like A Faster Internet,[42] as their proposed

---

[39] P. Vixie. *What DNS is Not*, *available at* http://queue.acm.org/detail.cfm?id=1647302; Erik Nygren, Ramesh K. Sitaraman, and Jennifer Sun, *The Akamai Network: A Platform for High-Performance Internet Application, available at* https://www.akamai.com/us/en/multimedia/documents/technical-publication/the-akamai-network-a-platform-for-high-performance-internet-applications-technical-publication.pdf.

[40] IETF Datatracker, *Client Subnet in DNS Queries, available at* https://datatracker.ietf.org/doc/draft-ietf-dnsop-edns-client-subnet/.

[41] Florian Streibelt, Jan Bottger, Nikolaos Chatzis, Georgios Smaragdakis, and Anja Feldmann, *Exploring EDNS-Client-Subnet Adopters in your Free Time, available at* http://conferences.sigcomm.org/imc/2013/papers/imc163s-streibeltA.pdf.

[42] *A Faster Internet: The Global Internet Speedup*, at http://www.afasterinternet.com.

extensions to DNS might not be able to be adopted by ISPs without first getting the consent from their customers to append their IP address to the DNS request.

End-users today, while they have they have the option to use alternative DNS services, do not need to explicitly understand "what DNS is." An ISP provides Internet access as a service, and includes all the necessary DNS functions and other behind the scenes work to make it easy for the end-user to access the Internet. While advanced users have the understanding and necessary knowledge of DNS, certainly the general public has no knowledge of DNS. It would not be practical or realistic for the Commission to require end-users to have to make a decision if they "want their IP address of their Internet endpoint or equipment appended to their DNS requests" and understand the consequences of their actions or inactions.

5. MAC Addresses

The Commission is proposing in the *Privacy NPRM* to include MAC addresses in the definition of CPNI based on the argument that a MAC address can be used to uniquely identify a device and that ISPs use MAC addresses to route data packets to end users.[43] There are several concerns with this reasoning.

MAC Addresses as CPNI

In the NPRM, the Commission states that "We propose to consider any MAC address associated with a customer's device to be CPNI in the broadband context," and cite as a footnote a white paper from the Center for Democracy & Technology (CDT) to justify their conclusion.[44]

[43] Privacy NPRM ¶ 44.
[44] Privacy NPRM ¶ 44; Center for Democracy & Technology, *Applying Communications Act Consumer Privacy Protections to Broadband Providers* (2016), https://cdt.org/insight/applying-communications-act-consumer-privacy-protections-tobroadband-providers/ ("*CDT White Paper*").

What is omitted is that MAC addresses are only used at the link-layer for the point-to-point[45] transmission of datagrams and are removed at the first-hop router. This coupled with other important technological developments place substantial limits on ISPs' visibility into an end-user's online activity, and into end-user's overall Internet activity. This is described in detail in a paper by Peter Swire at Georgia Tech.[46]

Changing the MAC address

As a rule of thumb, a MAC address is both unique and can be used to identify a device as to which it is normally paired as blocks of MAC addresses are purchased from the IEEE by equipment manufacturers.[47] But MAC addresses can be overridden and changed. The changing of the MAC address is called "cloning." For instance, operating systems support allowing the users to change the MAC address associated with the network interface adapter[48] and not the device. Interface adapters (e.g. NIC cards) for many devices can be removed and replaced, and as a result break the binding or pair between the MAC address and the device.

MAC addresses, LANs and WiFi

Contrary to the Commission's assertions in the *Privacy NPRM*[49], MAC addresses are <u>not</u> used to route packets to end-users. IP Packets are routed at the network layer, one layer above the link-layer (also known as the media access control layer), where switching is used instead.[50]

---

[45] See, e.g. James. F. Kurose & Keith W. Ross, *Computer Networking* at 460-461 (6th ed. 2013) ("*Kurose & Ross*").
[46] Peter Swire, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* (Feb. 29, 2016), *available at* http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf.
[47] Manufacturers purchase from the IEEE an Organizationally Unique Identifier (OUI) that is a 24-bit number that uniquely identifies the vendor/manufacturer. The manufacturer then appends to that another 24-bit number they generate to form a unique 48-bit number that constitutes the MAC address.
[48] MAC addresses are assigned by the NIC card manufacturer and can be changed by the operating system.
[49] Privacy NPRM ¶ 44.
[50] See, e.g. Kurose & Ross at 308.

MAC addresses are used to address datagrams for transmission at the link-layer[51], while IP addresses are used to address datagrams at the network layer. Link-layer technologies such as Ethernet or 802.11 allow two hosts on the same local area network (LAN) segment to send their datagrams using their MAC addresses.[52] When two devices on the same LAN segment wish to communicate with each other, they learn each other's MAC address using the Address Resolution Protocol (ARP).[53] When there are more than two devices on the same network segment then some kind of network multiplexing device such as an Ethernet switch or 802.11 (WiFi) access point is used that multiplexes the communications between the various devices on the same network segment.[54] In 802.11 networks, each wireless device must first associate with an access point before it can send or receive network-layer data. To do this, *each WiFi access point must periodically broadcasts its name (i.e. SSID) and MAC address* to enable the devices to learn about the available access points. At the same time, *devices scanning for access points – which they do all the time – broadcast their MAC address* as part of the process to enable the access points to learn about the devices in the area. After learning about all the available access points, the device then selects an access point with which to associate itself to enable the access point to learn the device's MAC address.

Devices on the same network segment communicate directly with each other by addressing their link-layer frames with each other's MAC address. When a device needs to communicate to a device on a different network segment, then the datagrams get "routed" using their network layer address or IP address and the device addresses the link-layer frame with the MAC address of the network gateway or router that will "route" the datagram.

---

[51] *See id.* at 460-461.
[52] *See id.* at 476.
[53] *See* i*d.* at 465.
[54] *See id.* at 476.

From this, there are several issues:

1) The MAC address of a device can be changed and does not need to be unique to that device. Thus, it is incorrect to assume that a MAC address can be used to uniquely identify a device.
2) It is incorrect to state categorically that ISPs use MAC addresses to route data packets; MAC addresses are used only for the transmission of datagrams at the link-layer communications
3) Devices disclose and share their MAC address as part of the link-layer communications with many other devices, and therefore information about MAC addresses is not unique to ISPs
4) MAC addresses are broadcast by all WiFi devices (such as iPhones, Android devices) and WiFi access points.

From this discussion, it should be clear that MAC addresses are not unique to ISPs.

6. Cybersecurity

The broadband privacy rules proposed in the *Privacy NPRM* are in conflict with how ISPs practice cybersecurity and will create unnecessary burdens in this area. The proposal directly affects the bundling of anti-malware software with Internet service and the second is cybersecurity information sharing.

IV. Malware

To mitigate malware ISPs, provide malware detection and remediation services that include anti-malware software on devices as a well as network-based passive DNS solutions.

A number of ISPs bundle anti-malware software with their Internet service.[55] Anti-malware software use two primary techniques[56] to examine files on a device and look for known viruses by means of a virus dictionary in order to identify suspicious behavior.

To do this, the anti-malware software collects and uses a great deal of data from the consumer equipment connected to the ISP's broadband service. This data may include: IP address, SIM card number, device ID numbers, geo-location, network information, file information (name, hash, size), device information (vendor, technical parameters), location information (time, zip code, area code, time zone), browsing and search history, service type, and applications used.[57]

ISPs often partner with vendors and their partner with whom IPS share the data collected by the anti-malware software is aggregated by the vendors and their partners to build data profiles, improve malware detection, and for other research purposes.[58] The proposal would hinder such work.

The network based solutions often leverage a technique known as passive DNS[59] that monitors DNS traffic for queries to well-known malware command & control (C&C) domains and then takes an action as recommended in the *U.S. Anti-Bot Code of Conduct (ABCs) for*

---

[55] AT&T, *AT&T Internet Security Suite powered by McAfee*, *at* http://www.att.net/iss; Comcast, *Constant Guard Internet Security by XFINITY*, *at* https://constantguard.xfinity.com; Cox Communications, *Cox Security Suite Plus by McAfee*, *at* http://welcome.cox.com/internet/features/security-software/.

[56] AntivirusWorld, *How does anti-virus software work?*, *at* http://www.antivirusworld.com/articles/antivirus.php.

[57] AVG, *Why do you collect my data?: AVG Privacy Policy*, *at* http://www.avg.com/us-en/privacy#why-do-you-collect-my-data; Symantec.com, *Symantec Advanced Threat Protection: Network Privacy Notice*, *at* https://www.symantec.com/content/en/us/about/media/privacypolicy/advanced-threat-protection-network-privacy-notice.pdf.

[58] *See* RFC 3316.

[59] Internet Systems Consortium, *Join the Global Passive DNS (pDNS) Network Today & Gain Effective Tools to Fight Against Cyber Crime*, *at* http://www.isc.org/blogs/join-the-global-passive-dns-pdns-network-today-gain-effective-tools-to-fight-against-cyber-crime/.

Internet Service Providers (ISPs)[60] that was the work of the Commission's CSRIC III Working Group 3, such as redirecting the user to a remediation webpage or sending the user an email notifying them they may be have malware. Passive DNS replicates the inter-DNS-server traffic to reconstruct a partial view of the data in the global Domain Name System to aid in identify malicious patterns. ISPs often have partner for passive DNS who are aggregating passive DNS information from multiple sources[61]. The proposed rules would hinder and even possibly prohibit ISPs with working with passive DNS partners.

V. Information Sharing

In 2015, the President signed Executive Order (EO) 13691, Promoting Private Sector Cybersecurity Information Sharing. EO 13691 directs the Department of Homeland Security (DHS) to strongly encourage the development and formation of Information Sharing and Analysis Organizations (ISAOs) for the voluntary sharing of information. On December 18, 2015 President Obama signed into law the Cybersecurity Information Sharing Act (CISA) to improve cybersecurity through enhanced information sharing about cybersecurity threats. The purpose of the two is to encourage more private-to-private and private-to-government voluntary sharing of cybersecurity threat information as means to improve the nation's cybersecurity posture.

Cyber threat indicators can include IP addresses, domain names, and email addresses.[62] During large complex attacks networks may share raw packet captures as network operators work together to determine ways to mitigate an attack. The Commission's proposed broadband

[60] FCC, Communications Security, Reliability, and Interoperability Council, Working Group 7 – Botnet Remediation, *Final Report: U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs), at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf.
[61] Farsight and Damballa are two examples of passive DNS partners that work with ISPs. *See* Farsight Security, *at* https://www.farsightsecurity.com/; Damballa, *at* https://www.damballa.com/.
[62] Department of Homeland Security *Cyber Threat Indicator and Defensive Measure Submission System, at* https://www.us-cert.gov/forms/share-indicators.

privacy rules would appear to classify some of this type of information as CPNI. As can be seen with the anti-malware software, information about cyber threats is often collected, shared, and used long before it becomes an actual threat. The communications sector has an extensive cybersecurity information sharing ecosystem, where information is shared with an array of partners (e.g. vendors, researchers, other enterprises, government, etc.).[63] The underlying theory of cybersecurity information sharing is that by encouraging voluntary sharing cybersecurity information, it will result in a comprehensive picture of the cybersecurity threat landscape that in turn will accelerate responses to threats and improve the overall cybersecurity posture.

Several issues are noted with information sharing:

1) The *Privacy NPRM* includes a carve-out for cybersecurity,[64] but even with this carve-out the broad definition of CPNI is counter to the EO and CISA. The cybersecurity carve-out permits "BIAS providers to use or disclose CPNI whenever reasonably necessary to protect themselves or others from cybersecurity threats or vulnerabilities."[65] But as noted, to achieve the full potential of cybersecurity information sharing, it is important that an abundance of cybersecurity information as possible be shared early and often without fear of it being deemed a breach or deemed an improper disclosure. The proposed rules would make it harder to share cybersecurity information with researchers and technical and/or business partners.

[63] FCC, Communications Security, Reliability, and Interoperability Working Group 5: Cybersecurity Information Sharing, *Status Update* (Mar. 16, 2016) at 5, *at* https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG5_Presentation_031616.pptx.
[64] Privacy NPRM ¶ 117.
[65] Privacy NPRM ¶ 117.

2) In addition, the rules proposed in the *Privacy NPRM* would make it harder for ISPs to bundle anti-malware software and related malware detection and remediation services with their Internet service.

3) Finally, cybersecurity information sharing would effectively be discouraged due to concerns over the risk of enforcement action for even accidental disclosures.[66]

Finally, within the "cyber world" the proposed NPRM would make it harder to share cybersecurity information with partners and researchers. The issue here cannot be overstated. Fundamental to cybersecurity practices is the ability to share data, and this would cripple many effective defensive mechanisms preventing spam and bots. For example, at the simplest level, Spamhaus is a service used by most ISPs and effectively they work by blacklisting IP addresses for the transmission of email. Most ISPs, in support of best cybersecurity practices, give lists of *all* their residential IP addresses for Spamhaus to share and blacklist for the transmission of email. This is recommended as a best practice by M3AAWG, the leading ISP operational anti-abuse community.[67] The *Privacy NPRM* would create confusion if end users would have to consent to opt-in to share IPs with Spamhaus. Certainly the general public would not understand this point, and would likely have a detrimental effect on the ability of ISPs to fight malware and botnets.

7. Peer-to-Peer Networking

Peer-to-peer (P2P) networking is a distributed application architecture that divides the work across multiple peers, in contrast to client-server architecture, which divides the work by assigned function. P2P networks build virtual overlay networks across the Internet and are used

[66] Privacy NPRM ¶ 174.
[67] Messaging, Malware, and Mobile Anti-Abuse Working Group, *M3AAWG Senders Best Common Practices Version 3.0*, (Feb. 2015), https://www.m3aawg.org/sites/default/files/document/M3AAWG_Senders_BCP_Ver3-2015-02.pdf.

by a broad range of applications that include: file-sharing, distributed storage[68], content delivery networks, multi-player online games, and messaging systems. Each device or peer in the P2P network maintains a small routing table consisting of its neighboring peers IP addresses and is used to route information between devices in the P2P network.[69] As part of joining a P2P network, a device must know its publicly routable IP address so that it can share it with the network. Devices and applications behind home routers running network address translation (NAT) use techniques based upon Session Transversal Utilities for NAT (STUN).[70] The concepts in STUN are also used for the "matchmaking" service in multi-player online games.[71] Applications that do not rely on a technique like STUN often require the end-user to make a configuration change to the router to make the device bypass the NAT router and connect directly to the Internet.

For any ISP provided application or service that relies on a P2P overlay network to communicate, the device must share its IP address so that others can communicate with it directly. As a result, the proposed rules potentially could require ISPs to solicit and obtain end-user's before they could utilize an ISP-provided P2P-enabled application or service the user wants to run. But, users generally do not know if their application is using P2P technology. This confusion would hinder the ability for end-users to use ISP P2P-enabled applications and hinder the ability of ISPs to offer such services (i.e. multiplayer on-line games, P2P cached content, messaging) that rely upon P2P technology.

---

[68] See Patent PCT/US2010/023075, Distributed Storage of Recoverable Data, awarded to Bittorrent, Inc.
[69] E. Lua, J. Crowcroft, M. Pias, R. Sharm, and S. Lim, *A Survey and Comparison of Peer-to-Peer Overlay Network Schemes*, IEEE Communications Surveys, Second Quarter 2005, Volume 7, No. 2.
[70] M. Petit-Huguenin and G. Salgueiro, *Datagram Transport Layer Security (DTLS) as Transport for Session Traversal Utilities for NAT (STUN) - RFC 7350*, DOI 10.17487/RFC7350 (Aug. 2014), *available at* http://www.rfc-editor.org/info/rfc7350.
[71] Unity Manual, *Internet Services, at* http://docs.unity3d.com/Manual/UNetInternetServicesOverview.html.

8. Network Routing

The Internet is a network of networks. Routing between these networks is fundamental to the operation of the Internet and is accomplished using the Border Gateway Protocol (BGP).[72] When networks interconnect, they announce their routes to each other using BGP. The announcing of the routes allows the routers on each network to build a routing table and learn the paths through the networks to get the end-points. Routing announcements contain blocks of IP addresses that are reachable via the network. The announced routes may either be pathways through the network if the network operator is providing transit or the announced route may be end-points within the operator's network.

BGP route announcements can be used to "steer" traffic for blocks of IP addresses or even a single host. Two examples of single IP addresses being announced are when an operator is sink-holing and black-holing traffic due to malicious behavior.[73] Network routing could clearly be affected by IP address included as CPNI.

[72] Y. Rekhter, T. Li, and S. Hares, *A Border Gateway Protocol 4 (BGP-4) - RFC 4271*, DOI 10.17487/RFC4271 (Jan. 2006), *available at* http://www.rfc-editor.org/info/rfc4271.

[73] Black hole routing and sink hole routing are when when routers are configured to silently drop packets for select address ranges.

9. Multi-Player Gaming

An extremely popular class of applications is multiplayer gaming. These applications can have different architectures, which could result in being affected by the proposed privacy rules. Technically, there are several basic architectures that exist for gaming: using a centralized server, variations on client-server, and peer-to-peer architectures. There are multiple ways that users connect, or are "discovered" in multi-player games which are implicated by the proposed privacy rules:[74]

- ***Direct IP Entry*** – Specifying the IP address directly with the user of whom you will be playing the game.
- ***DNS Entry*** – Uses a DNS or hostname entry point to the gaming server, where the end-user usually hosts the server. Used commonly in client-server games.
- ***LAN Broadcast*** – Used when all computers are on the same LAN. This approach is common with BYOC (Bring Your On Computer) parties, or with large events such as DreamHack.[75]
- ***Lobby Server*** – Has been common on such console games as XBOX 360 and services such as Steam. Users login to a common server, but will handoff the actual game to run on an end-user console directly with other users. Works similar to the match-maker service described earlier.

The architecture of the game itself could have an impact on a requirement to opt-in in order to be compliant with the proposed privacy rules. In the case of the Lobby Server, a centralized server is used to "organize" the game, but during the actual playing of the game an

[74] RakNet, *Multiplayer Game Components, at* http://www.jenkinssoftware.com/raknet/manual/multiplayergamecomponents.html.
[75] Dreamhack Austin, http://dreamhackaustin.com/.

end-user console is deemed the host and which connects directly to other end-user consoles, in a quasi-peer-to-peer architecture. This would require the end-user hosting the game to have the ability to disclose, and conceivably the other users connecting with the host console to disclose, since the host would be communicating back to the other end users.

For Direct IP Entry and the DNS Entry architectures, opt-in would also be required. Some games are privately hosted on servers provided by a third parties or even with end users such as with the game "Minecraft." In this case, the end user may need to disclose their location in order to pick the closest server to achieve the best performance. Opt-in would be required for this scenario.

Since games programs are applications running end-to-end, their network design varies, and end users are not aware of the architecture. However, running a game involves communications of various parameters (IP address, MAC address, geographical location and others), and often requires the disclosure of this information. Where the game application starts on a centralized server such as one hosted by an ISP on its cloud infrastructure, but hands off control to an end user server, could require the soliciting and obtaining approval to share this information.

Further, as games evolve, the host server may be dynamic during a game. The host could be handed off to another end user or site, creating further uncertainty about how CPNI would be applied. The assumptions of what CPNI would be needed at the start of a game may change during the game. ISP gaming offerings available to broadband customers could be inhibited by the proposed rules.

10. Bundled Services

ISPs often provide additional products and services that complement the Internet service they are offering. These products and services include – in addition to such services as email, DNS and network security functions – home security, home energy management, home automation, customized online news, music streaming, over-the-top subscription video, cloud storage, parental controls, content filtering[76], computer security software, and customer care. The products and services may be offered through a partnership with a third party and/or white-labeled by the ISPs. They are all accessed by, and delivered to, the end user via a broadband service transmission. Further, these services may be tied to the location where the Internet service is being delivered and rely upon the MAC address or IP address that is assigned to the modem terminating the Internet service, which needs to be shared with the third party delivering the service. In their current form, the proposed privacy rules potentially could require soliciting and obtaining approval to share this information.

ISPs are also integrating their modems into other premise equipment such as home gateways and set top boxes. These devices may leverage cloud based services (storage, voice recognition, etc.) as part of delivering the service to the end-user. The line partitioning the service between the CPE and cloud is blurry is will get even blurrier as ISPs begin to deploy virtual CPEs. How the proposed rules in the *Privacy NPRM* apply is unclear and potentially will hinder innovation and slow time-to-market for new services.

[76] Note: Parental controls and content filtering are examples of services where deep packet inspection (DPI) could be used as part of delivering the service

11. Future Services and Applications

How networks are architected, designed, and deployed are on the cusp of going through some revolutionary changes. Historically networks have been built using specialized dedicated hardware (e.g. routers, switches, soft switches, web servers, email servers, etc.). It is now possible with network function virtualization (NFV) to move these functions to commercial-off-the-shelf (COTS) servers as NFV leverages advancements in computing power and hardware virtualization to replace the dedicated network hardware with virtualized versions. In tandem, software-defined networks (SDNs) are re-architecting these functions to better leverage the underlying hardware by de-coupling the control plane and data planes of the network elements. The decoupling allows the control plane logic to be moved to the network cloud, and only use specialized hardware for the data forwarding plane. SDN and NFV together allow networks to be built on-demand and updated on-demand (e.g. add/remove bandwidth, adjust latency, add links or paths)[77]. The virtualization of the network isn't just happening at the core, but also at the edge with virtualized consumer devices as operators look to replace their customer's existing premise equipment. A virtual piece of consumer-premise equipment is a combination of a device that provides network bridging function and a remotely-hosted virtual device in the Cloud.[78] The virtual device provides a path for extending cloud-based services that include managed firewalls, video on demand, and NAT to an operator's subscriber base.

The growing deployment of Internet-of-Things puts increasing demands on networks for a highly scalable content distribution. Information-centric networking (ICN)[79] is a potential

[77] Telecomlead, *AT&T sets new SDN NFV goals, other telecoms to follow* (Dec. 17, 2014), *at* http://www.telecomlead.com/telecom-services/att-sets-new-sdn-nfv-goals-telecoms-follow-55024.
[78] Ericsson, *Virtual CPE and Software Defined Networking*, *at* http://www.ericsson.com/res/docs/2014/virtual-cpe-and-software-defined-networking.pdf.
[79] Ghodsi, A., Koponen, T., Raghavan, B., Shenker, S., Singla, A., Wilcox, J., "Information-Centric Networking: Seeing the Forest for the Trees", Hotnets '11, November 14-15, 2011.

solution. SDNs help to pave the way for ICNs. The fundamental concept of ICN is to use named data as a principal network service and evolve the Internet from today's host-based packet delivery towards directly retrieving information from in-network caches in a secure, reliable, scalable fashion.

The Privacy NPRM is silent on the evolution of any new technologies. It is not clear how rigid CPNI rules would impact the deployment of such new features. The concern is that such rules would lock ISPs into today's network architectures, preventing them from innovating and evolving to meet demands.

12. Lack of Clarity Regarding Proposed Exceptions

While the Privacy NPRM contains some exceptions to the consent requirement for uses of CPNI and PII, it is not at all clear how or whether these exceptions would apply to any or all of the use cases discussed. All examples above involve ISP uses of data elements proposed as CPNI in connection with services and capabilities that, from both a technical and customer perspective, are tightly integrated with – and provided at the same time as – broadband service transmissions. From a network engineering and operations perspective, it is difficult to understand when, how, and why application of the privacy restrictions (or any exceptions to those restrictions) are triggered in these examples. And the "future proofing" of any applicable privacy rules will always be challenged to be kept current with the underlying technology being used to provision Internet services. As shown in this paper, there are many examples of where the proposed rules in the *Privacy NPRM* are ambiguous and could potentially intrude upon how the Internet operates today and going forward.

In addition, the statement in the Privacy NPRM at paragraph 13 and footnote 35 that the proposed privacy rules do not apply to "the provision of other services by broadband providers"

that are "not part of the broadband Internet access service" may or may not exempt some of these use cases. But the NPRM does not offer any guidance as to whether a broadband provider simultaneously providing an integrated bundle of broadband and non-broadband services and capabilities to its customers should be considered a provider of broadband service subject to the rules or a provider of "other services" not subject to the rules.

Further, as the underlying technology evolves and with the introduction of new technology the proposed rules will be obsoleted. A good example is the introduction of virtual CPEs by ISPs that rely upon NFV and SDN technology. Functionality that was previously delivered by hardware in the CPE will now be delivered by the ISP's cloud infrastructure. This virtual CPE will enable the introduction an array of new services. Trying to sort out which ones are communications-related and/or in the provision of broadband services will further complicated the technology evolves.

Other examples of the proposed rules in the *Privacy NPRM* that are not future-proof and that reflect a rear facing paradigm are:

- Specifically exempting voice call location information for emergency situations[80] as there are alternatives to voice such as text and messaging for emergency calling. Some of these were discussed and examined in the FCC CSRIC IV WG1 - NG911.[81]

[80] Privacy NPRM ¶ 115.
[81] See FCC, Communications Security, Reliability, and Interoperability Council, *CSRIC IV Working Group Descriptions and Leadership* (Oct. 23, 2014), *at* https://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC%20IV%20Working%20Group%20Descriptions%2010%2023%2014.pdf.

- Numbers other than phone numbers can be spoofed[82] such as IP addresses, MAC addresses, and email addresses.
- Disclosure of CPNI for cybersecurity threats or vulnerabilities does not take into account the information sharing framework authorized with the passage of CISA and EO 13691 that encourage the sharing of information for cybersecurity "purposes".

CONCLUSION

From a technical perspective, the expansive set of data elements in the *Privacy NPRM* defined as CPNI significantly impacts a greater amount of broadband network functionalities and capabilities. As a result, the NPRM potentially subjects overly broad, out-of-scope base-level network functions and operations to the restrictions on CPNI use, which could be severely disruptive and frustrating for consumers because they would be potentially subject to repeated queries as to whether their data can be used to perform basic network functions and service operations related to ISPs. Multiple use cases are presented which illustrate the potential implications, including the possibility of needless complexity and confusion to end-users who would be required to make decisions on low-level technical functionality of which they would not understand the consequences. The existing privacy rules enforced by the FTC have served the Internet eco-system well. The new, more restrictive privacy rules proposed by the Commission could hinder the performance of existing services and the innovation of new emerging services.

[82] Privacy NPRM ¶ 118 (discussing spoofed phone numbers).