Before the
Federal Communications Commission
Washington, D.C. 20554

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

REPLY COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

Nuala O'Connor
Joseph Lorenzo Hall
Rita Cant
G.S. Hans

Center for Democracy & Technology
1401 K St. NW, Suite 200
Washington, D.C. 20005
202.637.9800

July 6, 2016

Executive Summary

The Center for Democracy & Technology (CDT) respectfully submits these reply comments in response to the public comments filed as part of the Federal Communications Commission's Notice of Proposed Rulemaking (NPRM) regarding proposed rules to protect the privacy of customers of broadband and other telecommunications services. CDT is a nonprofit public interest organization dedicated to promoting openness, innovation, and freedom online — a mission that closely tracks with the Commission's goals for this proceeding.

CDT's reply focuses on four key legal and technical issues raised in the first-round of comments:

The Commission's proposed rules would satisfy First Amendment scrutiny. Commenters argued that the Commission's framework fails to sufficiently protect the First Amendment interests of Broadband Internet Access Service (BIAS) providers. We respectfully disagree. The Commission's careful consideration of privacy and speech concerns in the proposed rule would satisfy intermediate scrutiny by the courts.

The Commission should clarify several technical issues that may be ambiguous in the proposed rule. Commenters highlighted concerns and confusion concerning security research, aggregation and de-identification, and deep packet inspection. We propose ways to clarify these issues to avoid confusion or ambiguity in a final rule.

The Commission should act deliberately when proposing data breach notifications. Commenters raised concerns regarding the appropriateness of the proposed data breach notification standards. While CDT does not take a position on specific timing for notification following a breach as proposed in the NPRM, we note that data breach remains a highly regulated and hotly debated policy issue. Accordingly, we encourage the Commission to create a notification standard that considers existing laws and feasible reporting timelines.

The Commission has created appropriate definitions for CPNI, PII, and customer PI. Several commenters argued that the Commission's definitions for these categories are overbroad and not authorized by statute. As discussed in our initial comments, we disagree. The Commission's interpretation of the Communications Act is appropriate and narrowly scoped.

Table of Contents

I. Introduction

The Center for Democracy & Technology has advocated for privacy protections for consumers for more than two decades, and was pleased to submit comments[1] to the Commission in response to its NPRM concerning the privacy of broadband internet users.[2] Given their unique role as "gatekeepers" to the internet, and the privileged and comprehensive access to highly personal data such a relationship entails, BIAS providers are properly subject to regulation as common carriers — including nondiscrimination and confidentiality requirements. Consumers do not expect their internet activities to be monitored and sold as a condition of internet connectivity.

In these reply comments, we respond to key concerns raised by other commenters, focusing on three main areas.

First, in Part II, we analyze the First Amendment implications of the NPRM's approach to consent for the use of customer proprietary information (customer PI) for targeted advertising. We conclude that the Commission's proposal to approach free expression and privacy concerns according to a regulatory framework keyed to consumer expectations and choice would satisfy intermediate scrutiny under the First Amendment.

Second, in Parts III through VI, we urge the Commission to clarify multiple technical issues. The Commission should create a clear, narrow security research exemption; clarify the relationship between de-identification and aggregated data; explicitly delineate the differences between deep packet inspection and shallow packet inspection; and craft a data breach notification standard that considers the existing laws and regulations that govern data breaches.

Finally, in Part VII, we discuss the proposed definitions of customer PI; customer proprietary network information (CPNI); and personally identifiable information (PII). We support the Commission's proposed definitions as appropriately scoped and within the statutory provisions of the Communications Act.

II. The Proposed CPNI Rules Satisfy First Amendment Requirements

Commenters raised thoughtful arguments regarding the proposed rules' potential to limit BIAS providers' freedom of expression. Reconciling the speech and informational interests of broadband advertisers with the privacy and confidentiality concerns of American consumers is an appropriate regulatory goal for the Commission. It is uncontroversial that restrictions on commercial speech or advertising are subject to an intermediate level of judicial review.[3] The Commission's proposed regulation of the use or disclosure of BIAS customer PI properly accommodates both speech and privacy interests to satisfy constitutional imperatives.

---

[1] Center for Democracy & Technology, *Comment Letter on the FCC's Notice of Proposed Rulemaking on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* (May 27, 2016), https://cdt.org/files/2016/05/Broadband-Privacy-Comment-FINAL-word.pdf (hereinafter "*CDT Comments*").
[2] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* Notice of Proposed Rulemaking, 31 FCC Rcd. 2500, 2519 ¶ 57 (proposed Apr. 1, 2016) (hereinafter "*NPRM*").
[3] *See Central Hudson Gas & Elec. v. Public Svc. Comm'n*, 447 U.S. 557, 563 (1980).

a. Protecting the privacy of American consumers' internet connectivity is a substantial interest of the Federal Communications Commission.

A stable and secure internet connection is the basis for all online activity – including expression, access to information, and association. BIAS provider practices that subvert longstanding consumer expectations about the quality or privacy of their broadband connection can impose a severe toll on consumers' ability and willingness to enjoy the full benefits of internet access. These impacts are proper concerns of the Commission.[4]

As discussed in our previous comments and elaborated in section VII below, threats to consumers' privacy online are real and unsettling.[5] Further, growing public awareness of pervasive internet surveillance has coincided with a dramatic chilling effect on the expressive activities of internet users.[6] Indeed, large numbers of American consumers are withdrawing from important features of daily life online because of unexpected and unauthorized uses of their private browsing and communication habits.[7] Other commenters argued convincingly that protecting customer PI is essential to encouraging increased adoption and use of broadband.[8] In CDT's view, ensuring the confidentiality of BIAS customers' internet communications and access habits is a paramount interest — and one of the most consequential communications policy objectives the Commission can pursue in the digital age.

b. Requiring explicit approval for unexpected uses and disclosures of customer PI advances consumer privacy

The Commission's proposed rules governing use and disclosure of customer PI are designed to align with consumer expectations and promote choice — appropriate means of advancing privacy, and the optimal way of obtaining customer approval as required by section 222 of the Communications Act.

---

[4] *U.S. Telecom Ass'n v. FCC*, No. 15-1063, slip op. at 29 (D.C. Cir. June 14, 2016).
[5] *See CDT Comments*, at 19-20.
[6] *See id.* at 20 (citing Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, Nat'l Telecomm's & Info. Admin., NTIABlog (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities (finding online privacy or security concerns stopped 45% of U.S. households studied from conducting financial transactions, buying goods or services, posting on social media, or expressing controversial opinions on the internet)). *See also* ACLU, *Comment Letter on the FCC's Notice of Proposed Rulemaking on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* 2-3 (May 27, 2016), https://www.aclu.org/other/aclu-comments-federal-communications-commissions-rulemaking-protecting-privacy-customers ("*ACLU Comments*") (gathering research on surveillance-related chilling effects).
[7] *ACLU Comments,* at 2-3; *see also* OTI, *Comment Letter on the FCC's Notice of Proposed Rulemaking on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* 10 (May 27, 2016) ("*OTI Comments*") (describing results of a 2010 FCC survey on broadband adoption and use finding that 57% of internet non-adopters cited their concern about the risk of data theft).
[8] *See OTI Comments,* at 9-11 ("The evidence is clear that privacy and security concerns can chill consumers' willingness to get online and to use the network to its full potential."); *ACLU Comments,* at 2 ("If we as a society create a telecommunications infrastructure where privacy is not protected, then many people and businesses will seek out alternative, less efficient means of communicating, rendering that infrastructure *less valuable* to them and to society.").

Consumers consider unexpected acts to monitor their communications or link their identity to their confidential internet activities as serious invasions of privacy.[9] Internet users can reasonably expect BIAS providers to use and share their confidential and proprietary information as necessary for the provision of the service, because this is contextually appropriate.[10] BIAS customers may expect that their data will be also be used or shared in communications about the service to which they subscribe — including for the purposes of marketing related services.[11] But as the uses of customer PI become unmoored from the provision of internet access, consumer expectations shift so that using customer PI without express permission becomes inappropriate. The unauthorized use of customer PI for purposes that are unrelated to the provision of internet connectivity thus constitutes a harm to consumer privacy. This is true for both unauthorized disclosures of customer PI as well as its unauthorized use for internal purposes.[12]

The proposed rules establish the following process for ensuring customer consent for the use or disclosure of personally identifiable proprietary information, in which the presumption of consent turns on the service to which the customer is subscribed:

- The BIAS provider may use opt-out consent to use customer PI for targeted marketing of its communications-related services, but must seek opt-in consent for targeted marketing unrelated to communications services;
- The BIAS provider may use opt-out consent to release customer PI to its communications-related affiliates for communications services, but must seek opt-in consent to share or disclose customer PI to third-party agents and vendors who do not offer such services.[13]

These proposed rules accomplish two goals related to the statutory objectives of customer approval for the use of PI. First, the proposal sets a default rule for when BIAS providers may presume customer consent and when they may not, according to customer expectations arising from the service relationship. Thus, a BIAS provider may presume that its customers approve of relevant targeted marketing of related services, but must presume that its customers have not consented to targeted marketing of services that are not relevant to their BIAS subscription.

Second, the rules ensure that customers have appropriate channels for modifying those presumptions to align with their actual preferences. Thus, customers who experience an invasion of privacy in the disclosure of their customer PI to affiliated communications providers may opt out of such disclosures. Likewise, customers who do not experience the disclosure of their internet connectivity habits as a privacy harm can opt in to full third-party disclosure.

In sum, the proposed rules let BIAS providers secure customer approval through opt-out consent where the use or disclosure is reasonably expected in the context of the BIAS relationship, and

---

[9] *See CDT Comments*, at 21-25.
[10] *Id.*
[11] *Id.*
[12] *See id.* at 21 (noting that "[c]onsumer attitudes toward companies' privacy practices and what type of consent should be required for use of their data are highly contextual," and that "[i]ndividuals measure the appropriateness of an entity's use of their data, such as health, location, and political information, by the nature of their relationship with that entity and the reason for the data use.").
[13] *NPRM,* 2508 ¶ 18.

require opt-in consent where the use or disclosure is not reasonably expected. In CDT's view, the careful structure of this approval regime protects consumer expectations arising out of the BIAS customer-provider relationship and promotes customer choice.

c. The proposed approval process does not unnecessarily impair BIAS providers' commercial speech

BIAS providers, as well as their customers, have an interest in targeting speech to a particular audience. Targeted marketing is a protected form of commercial speech and may be more effective than broadcast marketing.[14] But the Commission's proposed rules do not unnecessarily suppress BIAS providers' commercial speech. Rather, they are proportional to Commission's goal of protecting privacy by promoting consumer expectations and choice.

i. The rules do not restrict most of the expressive activities of BIAS providers

In evaluating the impact of the rules on BIAS providers' expression, the Commission should also take stock of the expressive, research, and service-related activities of BIAS providers that fall entirely outside of the scope of the proposed rules. There are many such categories of BIAS activity.

The rules would not apply to BIAS providers' proprietary information, including network equipment data such as internal MAC or IP addresses or domain names used in provider communications to their customers.[15] Such information can be used for security research, as well as ensuring appropriate network operations. Because this data is not linked or linkable to an individual, it is not implicated in the proposed rules.

Nor would the CPNI approval rules apply to BIAS providers' use or disclosure of customer PI in aggregate and de-identified form. Thus, a provider could, for instance, still use composite data derived from customer PI to engage in analysis of network security, offer data discount programs based on broadband subscription rates and usage patterns, and develop new products and services. As long as the customer PI is not "linked or linkable" to an individual, its use or disclosure is not subject to the rules governing customer approval. Similarly, the rules do not address targeted communications that are based on information other than customer PI that has been acquired through the provision of internet access.[16]

The rules make a narrow exception for providers' use or disclosure of customer PI for reasonable network management, for example, to block certain ports for security reasons. While the network-management exception may be too narrow from the perspective of contract security researchers as discussed in Part III below, CDT believes that a carefully crafted security research exception combined with the provision for network management allows providers to perform the

---

[14] *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1232 (10th Cir. 1999); *Florida Bar v. Went for It*, 515 U.S. 618, 630 (1995) (noting that "an untargeted letter mailed to society at large is different in kind from a targeted solicitation").

[15] *See* discussion of de-identification, *infra* Part IV.

[16] *See* discussion of PII, CPNI, and customer PI definitions, *infra* Part VII. BIAS providers can, for example, purchase browser-specific behavioral advertising through Google AdSense or engage in direct marketing of new products and services to customers' email address of record without customer PI approval.

technical operations necessary to continue to provide secure, competitive, and innovative BIAS service for their customers.

Thus, the relevant inquiry under the First Amendment is not whether BIAS providers can engage in direct or targeted advertising, but whether and under what circumstances they may presume consent to use customer PI in targeted advertising.

ii. The approval process is narrowly tailored to consumer expectations and proportionate to the privacy concerns at play

The proposed rules do not alter the statutory status quo established by Section 222 in prohibiting regulated carriers from using individually identifiable customer PI for purposes other than the provision of service, "[e]xcept as required by law or with the approval of the customer."[17] As common carriers, BIAS providers are bound by the restrictions on customer PI use and the customer approval requirement.[18] The sole question for First Amendment purposes is whether the Commission's use of opt-in consent is a permissible means of ensuring customer approval, or whether the constitutional protection for speech requires opt-out consent in all circumstances.[19]

As discussed, the proposed rules allow opt-out consent for providers' use of customer PI to market communications-related services or to disclose it to communications-related affiliates for marketing purposes. Thus, a BIAS provider may presume a customer consents to receive targeted offers to expand her data-roaming coverage or offer her bundled deals on high speed internet and voice, for example, based on her data use, unless the customer explicitly opts out of that advertising. In these circumstances, opt-out rules are appropriate so long as their implementation is consistent with consumer privacy principles, including requiring transparency and notice of proposed data uses, providing consumers with meaningful non-coerced choice, allowing consumers reasonable access to their customer PI, providing remedies for misuse or unauthorized access, and setting standards to limit data collection and ensure data security.[20]

Opt-out consent is the least restrictive form of obtaining customer approval.[21] But the Commission need not use the least restrictive means of pursuing its goal. Under the *Central Hudson* test for regulations of advertising, opt-in consent is permissible if it is proportionate to the interest in consumer privacy, and if the differences between the alternative approaches support the Commission's considered decision to prefer opt-in consent.[22] We believe the proposed customer approval mechanism satisfies these requirements.

A blanket opt-out consent regime would not accomplish the Commission's goal of protecting consumer privacy by maximizing consumer expectations and choice. CDT has noted that large majorities of consumers do not have enough information or time to self-enforce their

[17] 47 U.S.C. § 222 (c)(1).
[18] *U.S. Telecom Ass'n v. FCC*, No. 15-1063, slip op. at 29 (D.C. Cir., June 14, 2016).
[19] *See, e.g.*, *Nat'l Cable & Telecommunications Ass'n v. FCC*, 555 F.3d 996 (D.C. Cir. 2009).
[20] *See* Center for Democracy & Technology, *Recommendations for a Comprehensive Privacy Protection Framework* (Feb. 4, 2011), https://cdt.org/insight/recommendations-for-a-comprehensive-privacy-protection-framework/#1.
[21] *See U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1240-48 (10th Cir. 1999) (Briscoe, J., dissenting) (describing three interpretations of section 222's customer approval requirement).
[22] *Nat'l Cable & Telecommunications Ass'n v. FCC*, 555 F.3d 996, 1002 (D.C. Cir. 2009).

expectations about the confidentiality of their data.[23] But large numbers of consumers approve of out-of-context data use and disclosure when they are provided with appropriate information and mechanisms to exercise their choice.[24] Rather than discouraging consumer choice, an opt-in/opt-out regime calibrated to the reasonable expectations of consumers advances the rights of the audience to receive useful information. In CDT's view, the proposed rules — based on consumer expectations and choice — best reconcile consumers' interests in privacy and in receiving marketing tailored to their particular needs and interests.

Further, the Commission's choice of opt-in over opt-out consent in the case of sharing with unaffiliated third parties or for marketing services that are not "communications-related" does not significantly impair BIAS providers' commercial speech. In *NCTA v. FCC*, the United States Court of Appeals for the District of Columbia Circuit recognized that a requirement to seek opt-out consent is not significantly less burdensome than a requirement to seek opt-in consent[25] — but it does offer fewer of the privacy benefits. Nor is there convincing evidence that segregating the PI of customers who have opted in is significantly more onerous than segregating the PI of customers who have opted out.[26] From CDT's perspective, pervasive and comprehensive monitoring of customer proprietary data likewise implies the ability to record and remember a customer's preferences about those tracking and monitoring activities, including activities such as identifying patterns in online activity, deducing interests and tendencies in behavior, developing customer profiles, and curating highly personalized advertising.

BIAS providers correctly argue that opt-in mechanisms may produce less customer approval than opt-out mechanisms.[27] However, research suggests that the failure of many consumers to opt out is attributable to framing, default, and lack of notice and understanding of means for withdrawing consent.[28] Many consumers can be persuaded to opt in when they are offered high-quality services and compelling information about the benefits of opting in to those services.[29]

Two final points must be addressed. First, "content-based" regulations of commercial advertising are properly subject to intermediate scrutiny under the First Amendment.[30] In contrast to other content-based regimes, the Commission's proposed definition of "communications-related services" does not impose a burden on advertising about particular services; rather, it *lowers* the consent standard for targeted marketing based on the service to which a customer is subscribed (regardless of what the service is).

---

[23] *CDT Comments*, at 21-22.
[24] *Id.*
[25] *See Nat'l Cable & Telecommunications Ass'n v. FCC*, 555 F.3d 996, 1002 (D.C. Cir. 2009) (holding that "opt-out is only 'marginally less intrusive' than opt-in for First Amendment purposes . . . for the sharing of customer creditor information.") (citing *Trans Union Corp. v. FTC (Trans Union II)*, 267 F.3d 1138, 1143 (D.C. Cir. 2001)).
[26] *Cf.* Lawrence H. Tribe & Nathan S. Massey, *The Federal Communications Commission's Proposed Broadband Privacy Rules Would Violate the First Amendment* 5 (May 27, 2016), https://ecfsapi.fcc.gov/file/60002079394.pdf.
[27] *See CDT Comments,* at 23 nn. 91-95.
[28] *Id.*
[29] *See id.* at 24-25 (discussing concerns with "pay-for-privacy" schemes).
[30] *See Metromedia, Inc. v. City of San Diego*, 453 U.S. 490, 506 (1981) (explaining source of government's flexibility to determine scope of regulations concerning commercial speech); *Sorrell v. IMS Health Inc*., 564 U.S. 552, 574 (2011) ("This is not to say that all privacy measures must avoid content-based rules.").

Second, protecting the confidentiality of the internet infrastructure by regulating BIAS providers and not edge providers is not equivalent to viewpoint discrimination. BIAS providers are not "disfavored speakers" in this context, because the customer approval rules do not unjustifiably single out BIAS providers or suppress a message or worldview particular to ISPs.[31]

BIAS providers are appropriately subject to consumer choice restrictions in the use of customer PI for targeted advertising. Broadband internet providers are not similarly situated to edge providers with respect to customer PI and CPNI generally.[32] First, to gain access to the internet, customers must connect through a BIAS provider. As a result, they cannot avoid sharing this information with BIAS providers if they wish to access the internet. Second, customers cannot simply opt out of disagreeable privacy practices by discontinuing their use of a particular internet service. Commenters have amply demonstrated that switching costs are a de facto barrier to competitive privacy shopping among BIAS services. The alternative, to drop internet access altogether, is wholly untenable as a solution in today's digital society. Third, BIAS providers have a unique view of their customers' activities, including privileged access to highly personal data and inferences about their customers. This privileged and comprehensive access to potentially sensitive information distinguishes BIAS providers from other service providers in the internet space.[33] And finally, the context in which broadband customers agree to share this sensitive view of their lives with BIAS providers is highly specific to their role as gatekeepers to the Internet. As part of the communications infrastructure, BIAS providers have a distinctive relationship to their customers, a relationship that implies all the responsibilities of common carriers — including nondiscrimination and confidentiality requirements. Consumers do not expect their internet activities to be monitored and sold as a condition of connectivity.

In conclusion, the proposed rules restrict speech in a context-sensitive manner designed to encourage broadband adoption, support consumer expectations about the privacy of their sensitive data, and promote user choice. At the same time, the proposed rules ensure that the most important channels of targeted advertising remain open to BIAS providers according to customer approval. The minimal limits on unexpected uses and sharing of customer PI are proportional to the interest in protecting consumer privacy online.

III. The NPRM Should Provide a Narrow Exemption for Security Research

The state of threats on the internet is continuously evolving, and researchers play a vital role in adequately defending internet users against these threats in a timely manner. The list of instances

[31] *Mainstream Mktg. Servs. v. FTC*, 358 F.3d 1228, 1238-39 (10th Cir. 2004) (observing that "[t]he under-inclusiveness of a commercial speech regulation is relevant only if it renders the regulatory framework so irrational that it fails materially to advance the aims that it was purportedly designed to further."); *cf. Sorrell*, 564 U.S. 564 (striking down law prohibiting pharmaceutical marketers from obtaining prescriber-identifying information but allowing same information to be purchased or acquired by other speakers with diverse purposes and viewpoints); *Minneapolis Star & Tribune Co. v. Minn. Comm'r of Revenue*, 460 U.S. 575, 591 (1983) (striking down ink-and-paper tax that singled out the press and targeted a small group of newspapers).

[32] *See CDT Comments*, at 17-20; *OTI Comments*, at 2-11.

[33] *See generally CDT Comments*; *In the Matter of Protecting and Promoting the Open Internet,* GN Docket No. 14-28*,* Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC 5601, 5631-32 ¶ 81 (2015) ("2015 Open Internet Order").

where researchers' access to CPNI or PII has been indispensable to protecting internet users is long, but includes the development of new internet protocols (which provide greater security to internet users), the usage of data to pinpoint the existence and location of compromised computers (e.g., machine-to-machine connections, such as are available through technical standards such as IPFIX or NetFlow), and the necessary and continuous improvement of spam filters. In fact, in their comment, professors William Lehr, Steve Bauer, and Erin Kenneally state "in most cases [data] sharing is likely to fit within the category of data that needs to be shared to sustain the safe operation of the end-to-end Internet."[34] In essence, security research often requires access to CPNI and PII, and is necessary for the safe and continuous improvement of the internet.

Security research — which sometimes falls outside the purview of network management — is not granted an exemption to opt-in consent by the proposed rule. This poses a problem to numerous security researchers who depend on access to CPNI and PII; without an adequate exemption for security research, the valuable work done by these researchers would at worst be eliminated completely and at best be severely compromised as seeking opt-in consent from the population of BIAS provider customers will be infeasible and unworkable.

Some initial commenters — companies like FarSight Security and ThreatSTOP,[35] research organizations like the Messaging, Malware, and Mobile Anti-Abuse Working Group (MAAWG),[36] and professors like Nick Feamster at Princeton University[37] — said that they would be significantly hindered from providing valuable input to BIAS providers in protecting their clients and the internet at large. In addition, companies like FarSight Security (which believes that CPNI is too broadly defined and would impede the security research that they partake in) would be protected through a narrow security research exemption, thereby averting the necessity of further altering the statutory definition of CPNI and PII.[38] We share the concerns of these commenters and urge the FCC to consider a narrow security research exception in the final rule that would allow using these kinds of data for security research to continue in order to best protect BIAS customers, thereby avoiding the need to narrow the definition of CPNI.

In order to ensure maximal privacy protection for consumers and to avoid the First Amendment rule against viewpoint-based restrictions, the notion of security research must be defined in a narrow manner. Having a broad definitional scope, or crafting an exemption for all researchers,

---

[34] William Lehr, Steve Bauer, & Erin Kenneally, *Comment Letter on the FCC's Notice of Proposed Rulemaking for Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* 8 (May 27, 2016), https://ecfsapi.fcc.gov/file/60002081123.pdf.

[35] Manos Antonakakis et al., *Comment Letter on the FCC's Notice of Proposed Rulemaking for Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* (May 27, 2016), https://ecfsapi.fcc.gov/file/60002079307.pdf (hereinafter "*Antonakakis et al. Comments"*).

[36] Messaging Malware Mobile Anti-Abuse Working Group, *Comment Letter on the FCC's Notice of Proposed Rulemaking for Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* (May 27, 2016), https://ecfsapi.fcc.gov/file/60002079047.pdf.

[37] Nick Feamster, *Comment Letter on the FCC's Notice of Proposed Rulemaking for Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* (May 27, 2016), https://ecfsapi.fcc.gov/file/60002079367.pdf.

[38] FarSight Security, *Comment Letter on the FCC's Notice of Proposed Rulemaking for Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* (May 27, 2016), https://ecfsapi.fcc.gov/file/60002057082.pdf.

could allow for research uses that are as not directly aligned with the interests of users as would be the case for network management and operational security uses. For example, marketing and social science research are very much attenuated from the direct interests of BIAS customers, and allowing those forms of research may lead to abuses of purported research data that subvert the intent of the NPRM to protect consumer privacy from such uses in the first place.

The NPRM implies that certain activities are intended to protect consumers: "Under Section 222(d) of the Act, providers may use, disclose, or permit access to CPNI, without customer notice or approval, to: … (2) protect the rights or property of the provider, or to protect users and other providers from fraudulent, abusive, or unlawful use of, or subscription to, broadband services…."[39] Thus, those researching such protections by using CPNI and PII from BIAS providers should be exempt from obtaining opt-in approval for such uses. An explicit and narrow exception would emphasize the beneficial uses of such data and that ISPs should not cease from participating in such crucial data sharing due to this rule.

There are some caveats to this proposal. Security researchers will have access to PII and CPNI, which is a minor breach of privacy for BIAS providers' customers. However, because some important research techniques use data that is likely not covered by the NPRM, the extent to which security researchers derive data from CPNI and PII is limited.[40] In essence, while PII and CPNI are being shared with researchers, any privacy infringement is offset by gains in security research over time. However, the FCC must develop generic protections that bind security researchers as a condition of receiving BIAS data, similar to the contractual binding of downstream recipients of shared aggregated, de-identified data elsewhere in the proposed rule.

IV. The Use and Requirements of Aggregation are Ambiguous

The proposed rules set out data aggregation as an important barrier against privacy leaks about individuals. The proposed rule defines aggregate data as "collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed."[41] However, the NPRM's definition of aggregate data confuses the concepts of aggregation and de-identification: de-identification is a process by which individual customer identities and characteristics are removed from data.[42] Data aggregation involves reducing the

[39] *NPRM*, at 2540 ¶ 115.
[40] *Antonakakis et al. Comments*, at 6 (explaining that "above-the-recursive" DNS data refers to data sent by the BIAS provider to the DNS system when the BIAS provider's own DNS data cache does not include a particular domain requested by a BIAS customer. This is a communication from the BIAS provider to the DNS system and contains no link to the individual customer originating the request (it is neither CPNI nor PII, and it is not "forwarded" communications from the BIAS customer). This data is exceedingly helpful in identifying new domains sending large quantities of "spam" email or domains being used for command and control of entire systems of computers infested with malware (botnets).
[41] *NPRM*, at 2554 ¶ 155.
[42] U.S. Department of Commerce, National Institutes of Standards and Technology, *De-Identification of Personal Information* 2 (Oct. 2015), http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf.

granularity of individual data points to a more general data point; binning, summing, averaging, and generalizing over intervals are all examples.[43]

Aggregation can sometimes result in de-identified data, though this is not necessarily true. For example, a data set aggregated to count the number of people in a single ZIP code with similar birthdates could potentially still allow the identification of individuals in that set if the population within that ZIP code is small enough. Thus, the first prong of the elements a BIAS provider must obey when sharing aggregated data, requiring the provider to ensure that "the aggregated customer PI is not reasonably linkable to a specific individual or device," is necessary and absolutely important to protecting the privacy of individual customer data.[44] Otherwise, naive aggregation processes may result in cases like the one previously described where an "aggregated" data element is linked or linkable to an individual.

This inherent lack of clarity in the NPRM's definition of aggregation, which does not reflect the generic definition of aggregation, has led to confusion regarding what kinds of information *should* be shared without opt-in consent. The Internet Commerce Coalition, in its comment, states "we urge the Commission to revise its definition of de-identified data to make it fully consistent with the Federal Trade Commission's (FTC's) definition, as applied, and remove the proposed requirement that data be both de-identified and aggregated."[45] Similar confusion can be seen in comments submitted by CenturyLink,[46] Competitive Carriers Association,[47] and T-Mobile,[48] amongst others.

CDT agrees that it would be useful for the Commission to clarify that its definition of aggregation essentially includes de-identification as a prerequisite for the sharing of aggregate data without opt-in consent.

Additionally, there are important differences between the FTC and FCC's requirements for sharing aggregate data ("de-identified data" in the FTC framework). The NPRM states that the BIAS provider can share aggregate customer PI if, among other requirements, the provider "exercises reasonable monitoring to ensure that those contracts are not violated" and "that the burden of proving that individual customer identities and characteristics have been removed from aggregate customer PI rests with the BIAS provider."[49] We believe this clause is necessary, but

---

[43] European Union, Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques* 16 (Apr. 10, 2014), http://www.cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf.
[44] *NPRM*, 2553 ¶ 154.
[45] Internet Commerce Coalition, *Comment Letter on the FCC's Notice of Proposed Rulemaking for Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* at i (May 27, 2016), https://ecfsapi.fcc.gov/file/60002081118.pdf.
[46] CenturyLink, *Comment Letter on the FCC's Notice of Proposed Rulemaking for Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* (May 27 2016) (hereinafter "*CenturyLink Comments*"), https://ecfsapi.fcc.gov/file/60002081093.pdf.
[47] Competitive Carriers Association, *Comment Letter on the FCC's Notice of Proposed Rulemaking for Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* (May 27 2016), https://ecfsapi.fcc.gov/file/60002079353.pdf.
[48] T-Mobile, *Comment Letter on the FCC's Notice of Proposed Rulemaking for Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* (May 27 2016), https://ecfsapi.fcc.gov/file/60002080297.pdf (hereinafter "*T-Mobile Comments"*).
[49] *NPRM*, 2554 ¶ 154.

that it is currently overly vague, limiting its effectiveness. Without increased specificity, the legal and technical specifications of how to exercise reasonable monitoring are unclear and sufficiently vague that First Amendment concerns could arise regarding data sharing. We suggest the FCC consider releasing guidelines about what technologies and methods could be used to enforce real-time monitoring of the re-identification of de-identified data. Nonetheless, this clause is necessary for holding downstream recipients of this data to account in the enforcement context. Without this clause, the FCC has to rely on the BIAS provider to bring suit for breach of contract against the downstream recipient, who very well may be a customer of the BIAS provider; with this clause, the FCC can move against the BIAS provider for failing to properly monitor attempts to re-identify.

V. The Use and Requirements of Deep Packet Inspection are Ambiguous

Deep Packet Inspection (DPI) is defined by the NPRM as a technique that "involves analyzing traffic beyond the basic header information necessary to route a data packet over the internet."[50] What this definition implies is that those using DPI would be looking directly at application-layer data and content, rather than the packet metadata (e.g. destination, location, port usage, etc.). In the Internet Protocol suite, there exist three essential components for internet access: the internet/network data (layer 3), the transport data (layer 4), and the application data (layer 7).[51] Applying the FCC's definition quoted above, a BIAS provider can examine packet headers of each layer here as long as they do not dip down into the actual content of the application layer (like video, email, or chat messages). This definition of DPI is congruous with generally accepted definitions of DPI. We suggest that A) DPI be used exclusively to mean content-layer examination; and; B) a term like "shallow packet inspection" be used for non-content inspection.[52]

There is no doubt that DPI can be used for objectionable purposes that impinge on user privacy. For example, DPI can reveal application content, such as information regarding the content of users' audio and video communications, textual content (chat, web pages), and personal information. DPI has been used by countries like Iran[53] and China[54] to monitor user content. Nonetheless, there are also benign uses — uses generally aligned with user interests — for network inspection. These include searching for protocol non-compliance (in essence, users who are using the network for malicious purposes), viruses and spam, interference, and for collecting network statistics. These benign purposes fall under the purview of network management and

[50] *NPRM* 2584 ¶ 264.
[51] Center for Democracy & Technology, *Applying Communications Act Consumer Privacy Protections to Broadband Providers* (Jan. 20, 2016), https://cdt.org/insight/applying-communications-act-consumer-privacy-protections-to-broadband-providers/.
[52] Thomas Porter, *The Perils of Deep Packet Inspection* (Oct. 19, 2010), http://www.symantec.com/connect/articles/perils-deep-packet-inspection.
[53] Simurgh Aryan et al., *Internet Censorship in Iran: A First Look*, PROCEEDINGS OF THE 3RD USENIX WORKSHOP ON FREE AND OPEN COMMUNICATIONS ON THE INTERNET (2013) https://jhalderm.com/pub/papers/iran-foci13.pdf.
[54] Roya Ensafi et al., *Examining How the Great Firewall Discovers Hidden Circumvention Servers*, PROCEEDINGS OF THE 2015 ACM CONFERENCE ON INTERNET MEASUREMENT CONFERENCE 445-458, https://censorbib.nymity.ch/pdf/Ensafi2015b.pdf.

security research, and those operators using DPI for these purposes should, for all intents and purposes, be protected.

Sandvine has suggested that DPI is necessary for some of their operations, like understanding traffic down to the application level.[55] However, in such use-cases, Sandvine's understanding of DPI is different from that implied in the NPRM, as it defines DPI as being any inspection past the IP layer (layer 3). We believe that such a use case, in general, requires *shallow packet inspection* that looks at headers, rather than application content. In the context of the NPRM's definition of DPI, any uses of DPI other than those for network management and security research would severely impact user privacy, though the same cannot be said for shallow packet inspection. The more general practice of network inspection – encompassing both deep and shallow packet inspection – should not be singled out as a problematic method. Instead, forms of inspection that dip deeply into the content layer for uses outside of network management (which DPI can *sometimes* be used for) should be characterized as privacy infringing.

VI. The Commission Should Act Deliberately When Contemplating Data Breach Notification Rules

The proposal within the NPRM regarding data breach notifications bears special consideration by the Commission. Data breaches have long been an extremely vexing issue for companies, policymakers, and the public.[56] CDT has frequently worked on data breach issues, commenting on both federal and state proposals, and has a wealth of experience in this area.[57]

Data breach remains a politically active policy debate, with frequent data breaches highlighting the need for strong protections of consumer data. With a complex framework of state statutes governing breach notifications,[58] and sector-specific coverage under some federal laws,[59] policymakers in multiple venues continue to debate how to effectively protect consumer data while providing thoughtful and constructive notice of breach and avoiding potential "notice fatigue."[60]

---

[55] Sandvine, *Comment Letter on the FCC's Notice of Proposed Rulemaking for Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* 2 (May 27, 2016), https://ecfsapi.fcc.gov/file/60002077715.pdf.

[56] *See, e.g.*, David E. Sanger & Julie Hirschfeld Davis, *Hacking Linked to China Exposes Millions of U.S. Workers*, N.Y. TIMES (June 4, 2015), http://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html.

[57] Alex Bradshaw, *Consumer Privacy Protection Act is Data Breach Legislation We Can Support*, CENTER FOR DEMOCRACY & TECHNOLOGY (Apr. 30, 2015), https://cdt.org/blog/consumer-privacy-protection-act-is-data-breach-legislation-we-can-support/; Center for Democracy & Technology, *CDT Issue Brief on Federal Data Breach Notification Legislation* (Jan. 27, 2015), https://d1ovv0c9tw0h0c.cloudfront.net/files/2015/01/2015-01-27-Issue-Brief_DataBreach_TEH2.pdf.

[58] BakerHostetler, *Data Breach Charts* (2015), https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf.

[59] Office for Civil Rights, *Breach Notification Rule*, U.S. DEPT. OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited July 5, 2016).

[60] "Notice fatigue" itself remains a contested topic. *See* Jeff Kosseff, *Notified About a Data Breach? Too Late*, WALL STREET JOURNAL (Oct. 8 2015), http://www.wsj.com/articles/notified-about-a-data-breach-too-late-1444345445; Michael Bruemmer, *The misconceptions of data breach fatigue*, THE INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (Feb. 22, 2016), https://iapp.org/news/a/the-misconceptions-of-data-breach-fatigue/.

It is within this context that we encourage the Commission to act deliberately when contemplating notification requirements in this rulemaking. Several commenters, including those filed by the Federal Trade Commission, objected to the notice period in the NPRM, arguing that it was potentially too short to effectively promote the goals of protecting consumer data.[61] While we do not take a position on what precise terms of notification should be required, we agree with those commenters that any precise timeframe enacted must provide meaningful notice, be realistic, and be enforced. We thus encourage the Commission to keep in mind the many state laws and FTC enforcement decrees that have provided useful guidance on how data breaches should be addressed in order to best protect consumers.[62] The breach notification provisions in the final rule should complement existing law in order to create a consistent regime of consumer protection.

VII. The Proposed Rules Provide Well-Scoped Definitions for Customer PI, PII, and CPNI

a. Customer PI should be defined to include PII and CPNI

Customer PI and CPNI are currently protected under Section 222. However, CPNI, as defined in Section 222(h)(1), does not adequately encompass all data that needs protection, and customer PI is left undefined. PII does not presently have a uniform definition in the United States,[63] which has resulted in an absence of concrete protection for consumers.[64] Although some commenters to the NPRM dispute the Commission's authority,[65] the Commission *does* have authority under Section 222 to safeguard consumers by extending customer PI to include PII as well as CPNI, and to make rules protecting it.[66]

---

[61] FTC, *Comment Letter on the FCC's Notice of Proposed Rulemaking for Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* (May 27, 2016), https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf.

[62] *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[63] Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L.Q. REV. 1814, 1816 (2011), http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2638&context=facpubs.

[64] *Id.*

[65] *See e.g.,* Sprint, *Comment Letter on the FCC's Notice of Proposed Rulemaking on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* 5 (May 27, 2016), https://ecfsapi.fcc.gov/file/60002078174.pdf (hereinafter "*Sprint Comments*"); *T-Mobile Comments*, at 16; United States Telecom Association, *Comment Letter on the FCC's Notice of Proposed Rulemaking on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* 8 (May 27, 2016) (hereinafter "*U.S.T.A. Comments*"); Wireless Internet Service Providers Association, *Comment Letter on the FCC's Notice of Proposed Rulemaking on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* 6 (May 27, 2016), https://ecfsapi.fcc.gov/file/60002080933.pdf (hereinafter "*WISPA Comments"*); American Cable Association, *Comment Letter on the FCC's Notice of Proposed Rulemaking on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* at iii (May 27, 2016) (hereinafter "*ACA Comments*"), https://ecfsapi.fcc.gov/file/60002081117.pdf.

[66] *See infra* Part VII.b.

It is important that the Commission exercise its Section 222(a) authority to define customer PI as both CPNI and PII, and to define PII as "any information that is linked or linkable to an individual."[67] Commenters to the NPRM have argued that this definition of PII is far too broad and therefore it will not benefit consumer privacy.[68] This is incorrect. It will benefit consumer privacy precisely because of the definitional link between information and individual, which is a precondition for informational privacy harms.

American consumers consider data such as Social Security Number,[69] birth date, physical location over time, search engine history, and financial information[70] to be highly sensitive, private information. Many of these data types are not included in the current definition of CPNI. CPNI is defined in Section 222(h)(1) as "quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service" and billing information.[71] Sensitive data poses serious privacy threats to consumers, such as identity theft, reputational damage, and blackmail,[72] and should be included under the protection of customer PI.

Commenters to the NPRM are correct to observe that a lack "of real guidance as to what does and does not constitute PII" will be costly to BIAS providers and of little help to consumers.[73] Therefore, we support the Commission's proposed definition for PII, "any information that is linked or linkable to an individual," because it is clear, well-scoped, and would effectively capture sensitive non-CPNI data.

b. The Commission has Section 222(a) authority to define and protect customer PI, and PII and CPNI are distinct subsets of customer PI

Commenters argue, among other things, that the Commission cannot apply Section 222 outside of the telephony context,[74] that Section 222(a) is not a standalone grant of authority,[75] and that the Commission cannot use Section 222(a) to protect information beyond CPNI.[76] Other commenters make variations on these arguments.[77] This is not the case. The Commission's plain

---

[67] *NPRM*, at 2520 ¶ 60.
[68] *See e.g., T-Mobile Comments*, at 20; *WISPA Comments*, at 22; CTIA, *Comment Letter on the FCC's Notice of Proposed Rulemaking on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* 35 (May 27, 2016) (hereinafter "*CTIA Comments*") https://ecfsapi.fcc.gov/file/60002064853.pdf.
[69] Mary Madden, *Americans Consider Certain Kinds of Data to be More Sensitive than Others,* PEW RESEARCH CENTER (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/americans-consider-certain-kinds-of-data-to-be-more-sensitive-than-others/.
[70] *Id.*
[71] 47 U.S.C. § 222(h)(1).
[72] Erika McCallister et al., *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE 2-1 (Apr. 2010), http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.
[73] *T-Mobile Comments*, at 20.
[74] *U.S.T.A. Comments*, at 6.
[75] *T-Mobile Comments,* at 16.
[76] AT&T, *Comment Letter on the FCC's Notice of Proposed Rulemaking on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* 103 (May 27, 2016) (hereinafter "*AT&T Comments"*), https://ecfsapi.fcc.gov/file/60002080023.pdf.
[77] *See e.g., CenturyLink Comments*, at 14; *Sprint Comments,* at 5; *CTIA Comments*, at 11.

language reading of Section 222 supports its proposed adoption of rules protecting customer PI.[78] Section 222(a), which states that "every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to . . . customers," is a general grant of authority to protect customer PI.[79]

In Section 222, customer PI is not defined and appears as a term distinct from CPNI twice: once in Section 222(a) and once in Section 222(b).[80] CPNI appears eight times total in Section 222 and is defined at Section 222(h)(1).[81] The Commission is correct to view CPNI as a subset of customer PI because of the way Section 222 uses these terms. That Congress chose to protect customer PI in Section 222(a) and Section 222(b), but specified CPNI in other provisions of the statute demonstrates that Congress considered customer PI and CPNI to encompass different ranges of information. Furthermore, the guiding grant of authority for Section 222 imposes a duty to protect customer PI. CPNI does not appear in Section 222 until Section 222(c), where the statute enacts a specific protection for it. This shows that Congress considered CPNI to be a category of information subordinate to customer PI.

c. The Commission's interpretation of CPNI is within the statutory definition of CPNI

CPNI is defined by statute at Section 222(h)(1) and the Commission's reading of this statutory definition is correct because it effectively protects information pertaining to consumers. While some commenters argue that CPNI is not applicable to broadband,[82] they are incorrect. Not only is the statutory definition of CPNI applicable to broadband, but the Commission's interpretation of CPNI is within that statutory definition and is appropriate to the purpose of protecting consumer privacy.

The types of information that the Commission includes in its non-exhaustive list of CPNI fit squarely within Congress's definition of the same. The list includes information such as Media Access Control (MAC) address, IP address, domain names, and geographic location. These are all examples of "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service," as well as examples of sensitive information with major privacy implications.

For instance, a MAC address is a persistent identifier. It identifies a single, specific device, such as a mobile phone or a personal laptop. Every device on a network has one. The purpose of a MAC address is to allow routing to a specific device on a network, meaning it relates to the destination of a telecommunications service. A MAC address is factory-assigned and it will not change unless a consumer goes through a technical and laborious process of reconfiguring the operating system to manually change it. While a customer's home modem will normally remove a MAC address associated with an individual device on the home network before communicating

[78] *NPRM*, at 2594, ¶ 296.
[79] 47 U.S.C. § 222(a).
[80] 47 U.S.C. § 222(a), (b).
[81] 47 U.S.C. § 222.
[82] *See e.g. U.S.T.A. Comments*, at 6.

with the provider's network, a MAC address embedded in the packet payload or header at the application layer could remain and be visible to the BIAS provider.[83]

It is important to craft regulations that will adapt with technology. It is believed that some future forms of BIAS network architectures may remove the need for a network modem, making available a MAC address farther up into the BIAS provider's network outside of the home network.[84] As MAC addresses function to uniquely specify a device, a MAC address accompanying any transmission can be used to link anything related to that transmission to an individual device and an altered MAC address could even be used to impersonate another device and its owner.

Industry has recognized the privacy threat of MAC addresses, as shown by the implementation of randomized and automatically changing MAC addresses on all major computer operating systems.[85] However, this is an imperfect security measure and researchers have shown they can reveal a device's true MAC address, despite the randomization, and then track the device.[86] In light of the major privacy issues surrounding them, MAC addresses and other types of information that fit the statutory definition of CPNI need to be included as protected customer PI in a plain language interpretation of Section 222.

As to the second part of the statutory definition of CPNI, the Commission's examples of CPNI qualify as CPNI because they are "made available to the carrier by the customer solely by virtue of the carrier-customer relationship." This is the case because, if the customer were not transmitting data over the BIAS provider's network, or, put another way, if the customer were not a customer of the BIAS provider, then the BIAS provider would not have access to any of that transmitted data. That third-parties might gain access to the same data when a consumer uses their services does not negate the fact that the BIAS provider has gained access to the data only because the customer elected to use the BIAS provider's telecommunications service. Furthermore, as there are privacy implications, it does not follow that BIAS providers should be able to freely share sensitive information simply because some other actors are already privy to it. That the data exists in the hands of certain other entities does not mean that further dissemination by the BIAS provider no longer implicates consumer privacy.

d. PII is sensitive data and is a privacy threat if left unprotected

Commenters to the NPRM argued that the proposed definition for PII "is essentially boundless"[87] and "has no limiting principle."[88] Those arguments are incorrect because they fail

---

[83] *CDT Comments*, at 13.
[84] Margaret Chiosi et al., *Network Functions Virtualization: an Introduction, Benefits, Enablers, Challenges & Call for Action,* SDN AND OPENFLOW WORLD CONGRESS (Oct. 22, 2012), https://portal.etsi.org/NFV/NFV_White_Paper.pdf.
[85] Ionut Ilascu, *MAC Address Randomization Gets Closer to Becoming a Standard,* SOFTPEDIA (June 26, 2015), http://news.softpedia.com/news/mac-address-randomization-gets-closer-to-becoming-a-standard-485372.shtml.
[86] Mathy Vanhoef, *Why MAC Address Randomization is not Enough: an Analysis of Wi-Fi Network Discovery Mechanisms,* PROCEEDINGS OF THE 11TH ACM ON ASIAN CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY (2016), http://dl.acm.org/citation.cfm?doid=2897845.2897883.
[87] *T-Mobile Comments*, at 20.
[88] *CTIA Comments,* at 35.

to understand the division the definition draws, as well as the origin of potential harms to consumers. All data is either "linked or linkable to an individual" or "unlinked and un-linkable to an individual." Information linked or linkable to an individual is a privacy threat because the link identifies an individual. The threat is magnified when this linkable data combines with other pieces of linkable data. Unlinked and un-linkable data by definition cannot be a privacy threat because there cannot be an individual privacy threat if there is no underlying link to an individual. By selecting the definition "any information that is linked or is linkable to an individual" as its definition of PII, the Commission creates a very simple binary distinction entirely based on whether or not the information can harm a consumer. As this definition is straightforward and effective, the Commission should adopt it.

Beyond CPNI, individual pieces of PII, as well as multiple pieces of PII in combination, pose risks to consumers. Location data is one especially troubling example of PII creating a major privacy risks and which should be encompassed by any definition of PII that the Commission adopts. Researchers have found that when a consumer makes a cell phone call, the researchers can uniquely identify 95% of individuals with only four location data points, taken hourly. The researchers are able to make this determination using location data no more specific than the location of the carrier's nearest routing antennae.[89]

With a single transmission of timestamped location data and a map, identified consumers will reveal whether or not they are home or at work. They might also reveal where they are eating lunch, or that they at a sensitive location such as an abortion clinic or a drug treatment facility. Thus, location data can be used to make inferences about an individual's personal life when they would not normally share that information. Furthermore, location data collected over time can reveal details about an individual's schedule and daily routine. Entities with access to location data could then act on any inferences made using that data. California Attorney General Kamala Harris issued a consumer alert advising California residents to turn off location data sharing on mobile phone applications, warning that such location broadcasting could, "expose you and your family to risk of theft or physical harm."[90] Harris also observed that geo-tagged selfies "can be dangerous, especially for victims of stalking or domestic abuse."[91]

Expanding from single data point PII risks, multiple pieces of PII in combination also pose profound threats to consumers.[92] Identity theft is the greatest privacy concern of American consumers. Social Security Number, name, mother's maiden name, address information, and birth date are all linked or linkable to an individual, meaning that they fall under the Commission's proposed definition of PII. These pieces of PII are also transmitted over the internet and, taken together, are the ingredients for identity theft.

Relatedly, sometimes data is not individually linked to an individual, but is linkable to an

---

[89] Yves-Alexandre de Montoye et al., *Unique in the Crowd: the Privacy Bounds of Human Mobility,* 3 SCIENTIFIC REPORTS (MAR. 25, 2013), http://www.nature.com/articles/srep01376.
[90] William M. Welch, *Calif. A.G.: Shut off smartphone location services,* USA TODAY (Dec. 22, 2014), http://www.usatoday.com/story/news/nation/2014/12/22/california-attorney-general-smartphone-wawrning/20778295/.
[91] *Id.*
[92] Morrison Foerster, *Consumer Outlooks on Privacy* 5 (2016), http://www.mofo.com/~/media/Files/Resources/2016/MoFoInsightsConsumerOutlooksPrivacy.pdf.

individual when combined with other bits of data. A study using the 2000 census showed that while a 5-digit ZIP code alone could not be linked to an individual, 5-digit ZIP code combined with gender and date of birth could identify 63% of individuals.[93] Adding more pieces of PII together in combination increases ability to accurate identify a unique individual and also increases the privacy threat to that individual. This combination problem means that, while it is helpful to list types of PII such as Social Security Number and birth date, it is impossible to create a comprehensive list of all possible instances of PII. In short, PII is contextual.

e. BIAS providers have unique access to large amounts of PII

While the internet ecosystem is comprised of many entities exchanging many types of data, a BIAS provider's access to a consumer's data is unique because the BIAS provider serves as the gatekeeper between the consumer and the internet and the shepherd of the consumer's data across the internet.

Returning to the example of location data, many mobile phone applications allow consumers to turn location sharing on and off. A consumer can keep all of their application location sharing turned off and turn it on only when they need to use a particular feature. Thus, a consumer who normally keeps all location sharing off might briefly turn on location sharing to check directions on Google Maps, then turn location sharing off, then briefly turn location sharing back on to check for restaurants on Yelp later that same day, then turn location sharing off again. In this example, Google Maps handles one piece of the user's location data, Yelp handles another piece of the user's location data, and the user's BIAS provider handles both pieces of data. Expanding on this example, the BIAS provider in this case will also always have some form of location data for the consumer with the phone, even if that data is not as specific as GPS data, simply because the BIAS provider cannot serve a phone that it cannot find.

Even in the wired context, a BIAS provider will always have some kind of location data for a device and, while laptops are not as immediately connected to an individual as mobile phones with SIM chips, they do have MAC addresses that can be combined with PII such as usernames for online accounts to pin down that an individual is in a particular place. If a BIAS provider is using network address translation (NAT), then the BIAS provider might even have better location data than any location data an edge provider would normally obtain through a user's IP address.

f. Consumers want to protect their data, but are unable to do so

Consumers are well aware of the risks the availability of their data exposes them to. Among Americans, "there is a widespread worry that people's information is vulnerable, even when companies that collect it do their best to keep it safe."[94] A survey published in the *Harvard Business Review* showed that "72% of Americans are reluctant to share information with

---

[93] Philippe Golle, *Revisiting the Uniqueness of Simple Demographics in the US Population,* PROCEEDINGS OF THE 2006 ACM WORKSHOP ON PRIVACY IN THE ELECTRONIC SOCIETY (Oct. 30, 2006), https://crypto.stanford.edu/~pgolle/papers/census.pdf.

[94] Lee Rainie & Maeve Duggan, *Privacy and Information Sharing,* PEW RESEARCH CENTER (Jan. 14, 2016), http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf.

businesses" because of privacy concerns.[95] Indeed, when it comes to protecting personal information, 61% of American adults "would like to do more."[96]

Consumers lack effective means of protecting their PII. Even when consumers appear to have the tools to do so, they do not actually have the capability. Federal Trade Commission Consumer Protection Bureau Director Jessica Rich testified before the Senate Privacy, Technology, and Law subcommittee that the FTC has brought action against companies found collecting and transmitting geo-location data and other data despite privacy policies saying that they do not engage in such activities.[97] The FTC has also found companies offering data collection opt-out options to consumers, but collecting the data despite consumers opting out.[98]

VIII. Conclusion

For the foregoing reasons, we respectfully assert that 1) the Commission's proposed definitions of customer PI, PII, CPNI, and communications-related services are appropriate, well-scoped, and promote the goals of protecting consumer privacy; 2) the proposed rules satisfy First Amendment scrutiny; 3) the Commission should provide a narrow security research exemption; 4) the Commission should clarify its definitions of aggregation, de-identification, and deep packet inspection in the manner described; and 5) that the Commission should act deliberately when contemplating data breach notification requirements, given other regulatory requirements. We applaud and support the Commission's work in protecting consumers through this rulemaking.

---

[95] Timothy Morey et al., *Customer Data: Designing for Transparency and Trust*, HARVARD BUSINESS REVIEW (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust#.

[96] Mary Madden, *Most Would Like to do More to Protect Their Personal Information Online,* PEW RESEARCH CENTER (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/most-would-like-to-do-more-to-protect-their-personal-information-online/.

[97] *Location Privacy Protection Act of 2014: Hearing on S.2171 Before the Senate Judiciary Subcommittee on Privacy, Technology and the Law*, 113th Cong. (2014) (statement of Jessica Rich, Director, FTC Consumer Protection Bureau).

[98] *Id.*