

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

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

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

Nuala O'Connor
Alex Bradshaw
Stan Adams
Rita Cant

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

May 27, 2016

Executive Summary

The Center for Democracy & Technology (CDT) respectfully submits these comments in response to the 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 the Commission’s goals for this proceeding.

CDT commends the Commission’s efforts to protect consumer privacy through adapting Title II’s consumer protection provisions to broadband internet access service (BIAS). In light of the vast amounts of personal information passing through BIAS providers’ networks, the Commission’s decision to update, rather than to forbear from, those provisions was correct. This gives BIAS customers a greater degree of control over information they have no choice but to disclose when they use the internet.

Although comprehensive baseline privacy protection is ideal, the Commission’s authority to regulate communications does not extend to providers at the edge of networks, nor does CDT believe that it should. Rather, CDT supports Congressional action to enact comprehensive baseline privacy law so that internet users gain more awareness and control over the information flowing from their actions online, regardless of where that information originates and who collects it. While the Commission’s enforcement of Title II cannot provide this comprehensive protection, its efforts to protect BIAS customers’ data provides a fundamental element of the U.S. privacy framework. The following proposals are essential to the Commission’s development of its fundamental role:

Customer Proprietary Information should include Personally Identifiable Information.

CDT agrees that “proprietary information of, and relating to . . . customers” described in Section 222(a) should be interpreted broadly. Specifically, it must include a broader set of information than that encompassed by 222’s definition of Customer Proprietary Network Information (CPNI). The statute generally requires carriers to protect the confidentiality of customers’ proprietary information (customer PI), but sets out the conditions under which a subset of that information, CPNI, may be used and shared. The remainder of customer PI, which should include personally identifiable information (PII), must generally be kept confidential absent customer approval to use or disclose it.

Customer Proprietary Network Information should include packet metadata.

In the broadband context, information that “relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service” can be found in the metadata of the layered headers enveloping internet protocol (IP) packets. Even a limited collection of this metadata can provide information about a customer’s whereabouts and their online activity. Over time, the analysis of these data points can reveal patterns of behavior and details about customers’ personal lives that, while commercially valuable, warrant a greater degree of customer control over its use.

Customer opt-in should be required for most secondary uses of customer PI.

CDT supports the Commission's proposal to generally require customer opt-in for use and sharing of customer data for marketing services unrelated to the service a customer has purchased. There are many legitimate uses for the customer information BIAS providers may collect. Some of these uses are necessary to maintain a functional, efficient network and require no consent. Others help carriers market relevant communications offerings. Customer opt-in should not be required in these cases since the privacy risks are lower and customers expect carriers to use their information for such purposes. However, customer opt-in should be required for all unaffiliated third-party use of customer PI for marketing and first-party or affiliate use of customer PI for marketing services that are not "communications-related."

The disclosure of customer PI to third parties often places that information outside the control of the carrier and in the hands of third parties that may not be subject to any privacy standards under the Communications Act. Therefore, the risk of data loss is greater and the Commission will have more difficulty addressing entities responsible for the loss. Requiring opt-in for most secondary uses of customer PI is also important because this gives customers more meaningful control over the use of their information. Even where opt-in is required, BIAS providers should still have flexibility under the rules to encourage customer opt-in, including offering monetary rewards in exchange for customer opt-in. However, because such inducements to consent raise serious public policy concerns, these programs must be transparent and must not be coercive.

Customer opt-out should be allowed for first-party and affiliate use of customer PI to market "communications-related services."

Customer opt-out would be sufficient for first-party and affiliate use and sharing of customer PI to market "communications-related services." "Communications-related services" should be limited to entities subject to privacy protection under the Communications Act; particularly voice, internet and cable services. Sharing customer PI with these entities would not significantly increase the risk of loss of customer data; the carrier would be likely to maintain control of the data once it is shared and the entity receiving the data would be subject to privacy protections under the Communications Act.

The following comment will address these proposals.

Table of Contents

I. Introduction	6
II. There are strong policy and legal bases for including personally identifiable information in the definition of customer proprietary information	7
A. Limiting covered information to CPNI would exclude much of the data consumers find most sensitive and would not meet customer expectations	8
B. The Commission’s definition of PII is appropriate	9
1. <i>PII should be interpreted broadly to include any information linked or linkable to an individual</i>	9
2. <i>It is critical that PII include location data</i>	10
C. The Commission has authority under 222(a) to create privacy rules for information beyond CPNI	11
1. <i>The statute and legislative history support this conclusion</i>	11
2. <i>Uses of “proprietary information” throughout the Communications Act as well as in other laws support this conclusion</i>	12
III. Customer Proprietary Information Must Include Packet Metadata	12
A. The information in packet headers fits the definition of CPNI and may also contain PII.....	13
1. <i>Frame headers contain device identifiers and information relating to the destination of telecommunications services</i>	13
2. <i>IP headers contain information relating to the destination and amount of use of a telecommunications service</i>	14
3. <i>Transport layer headers contain information relating to the destination and amount of use of a telecommunications service</i>	14
4. <i>Application headers contain information relating to the destination and location of a telecommunications service</i>	15
5. <i>Unique identifiers added to packet headers are PII and CPNI</i>	15
B. Long-term monitoring of network traffic raises privacy concerns.....	16
C. Encryption technologies do not adequately address privacy concerns.....	16
IV. Customer Opt-In Should Be Required for the Majority of Secondary Uses of Customer Proprietary Information; However, Opt-Out Approval May Be Appropriate in Some Circumstances.....	17
A. The Commission has a substantial interest in protecting the privacy of customer PI.....	17
1. <i>BIAS providers are uniquely positioned to have access to large amounts of very detailed customer PI</i>	17
2. <i>BIAS providers’ secondary use of customer PI has important privacy implications</i>	19
3. <i>Consumer privacy cannot be preserved unless there are reasonable conditions on BIAS providers’ secondary use of customer PI</i>	20
B. Requiring customer opt-in for the majority of secondary uses of customer PI advances consumer privacy and does not overburden BIAS providers	21
1. <i>Requiring opt-in for most secondary use of BIAS customer data advances consumer privacy</i>	21

2. <i>Requiring opt-in for the majority of secondary use of customer PI does not overburden BIAS providers</i>	24
C. Requiring customer opt-in for the majority of secondary uses of customer PI is appropriately scoped; opt-out would still be permissible for first party and affiliate marketing of “communications-related services”	26
1. <i>A sharply crafted definition of “communications-related services” would protect consumer privacy</i>	26
2. <i>A sharply crafted definition of “communications-related services” would still allow for reasonable secondary use of customer PI for marketing</i>	27
V. Conclusion	27
Appendix	29

I. Introduction

The internet's multitude of benefits would not be possible without its users. Individuals' activities while online — exchanging ideas, simplifying business and personal transactions, collaborating and socializing — are what make the internet the most significant communications network in history. People should be able to contribute to the online ecosystem without concern that their contributions will be intercepted, analyzed, or shared in unexpected ways.¹ Therefore, strong data use and sharing standards must be a component of any internet law framework. Broadband internet access service (BIAS) providers are uniquely positioned to not only enable widespread adoption of internet but also to steward responsible use of consumers' data. The present rulemaking to protect the privacy of broadband customers is a remarkable opportunity for the Commission to ensure BIAS providers fulfil this role.²

This is an exciting time for data driven innovation. Online data collection and use has revolutionized industries, public services, and the economy. In addition to actually building and maintaining the physical infrastructure through which we access the internet, BIAS providers are contributing to the digital revolution and data analysis in a number of meaningful ways. However, the transformative power of data should not overshadow increasingly prevalent concerns about unchecked use of consumers' personal information. These concerns are not restricted to BIAS, and BIAS providers certainly are not alone in their data monetization efforts. Edge providers have charted the path for data collection and sharing techniques and a large portion of edge services' profits come from data monetization. Device manufacturers are increasingly designing ways to monetize their customers' data as well—often through partnerships with edge services and advertisers.

Unfortunately, a strong consumer privacy framework does not accompany this robust data market. Despite how critical privacy protections are to the continued health of the internet, the United States lacks a comprehensive consumer privacy law.³ Instead, American consumers face a patchwork of privacy standards that leave some personal information unprotected in surprising ways, and a general purpose consumer protection law enforced by the Federal Trade Commission (FTC) that maps imperfectly onto privacy rights. For these reasons, CDT has long argued for simple, flexible baseline consumer privacy legislation that would protect consumers from inappropriate collection and misuse of their personal information. In principle, such legislation would codify the Fair Information Practice Principles⁴: requiring transparency and notice of data collection practices, providing consumers with meaningful choice regarding the use and disclosure of that information, allowing consumers reasonable access to the personal

¹ Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, Nat'l Telecomm's & Info. Admin., NTIA Blog (May 13, 2016), <https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities> (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).

² 47 U.S.C. § 222(h); *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 Center for Democracy & Technology, *Analysis of the Consumer Privacy Bill of Rights Act* (Mar. 2, 2015), <https://cdt.org/insight/analysis-of-the-consumer-privacy-bill-of-rights-act/> (the United States is one of only two developed nations without privacy protections for all personal data (Turkey is the other one); instead, there are a handful of sector-specific laws that apply to narrow categories of personal information).

⁴ Nat'l Inst. of Standards & Tech. (NIST), *National Strategy for Trusted Identities in Cyberspace*, app. A (April 2011), available at <http://www.nist.gov/nstic/NSTIC-FIPPs.pdf>.

information they have provided, providing remedies for misuse or unauthorized access, and setting standards to limit data collection and ensure data security.⁵

Title II and the larger patchwork of U.S. privacy laws cannot (and are not intended to) set standards for every industry. CDT therefore encourages Congress to swiftly pass baseline privacy legislation so that individuals gain more control over their data, regardless of where that information originates and who collects it. Nevertheless, absent Congressional action to pass such a law, the Commission has a statutory obligation and specialized expertise to protect the privacy of broadband customers now through its Title II authority.

This comment outlines how the Commission can embrace this opportunity in its rules. Part II calls for personally identifiable information (PII) to be included in the definition of customer proprietary information (customer PI). The Commission has the statutory authority to include PII in its definition of customer PI. Restricting what is covered under the rules to customer proprietary network information (CPNI) would be contrary to this grant of authority and, more importantly, public policy. Part III argues that CPNI should include packet metadata. The definition of CPNI in Section 222 maps well to metadata on internet transmissions. It is important that these data points are covered under the rules because they can reveal patterns of BIAS customers' behavior and personal lives that, while commercially valuable, warrant a greater degree of customer control over its use. Finally, Part IV calls for a majority opt-in customer consent framework for use of customer PI for marketing. Specifically, opt-in should be required for all non-affiliate third-party use of customer PI for marketing and for first-party and affiliate use of customer PI to market services that are not "communications-related." However, opt-out would be sufficient for first-party and affiliate use of customer PI to market "communications-related services." "Communications-related services" should be limited to entities subject to privacy protection under the Communications Act. This should include voice, internet and cable. This is because consumers are less likely to be aware of and exercise their choice in an entirely opt-out scheme. Opt-in is therefore more appropriate for unexpected uses and sharing of customer PI. Requiring opt-in for these unexpected uses is only marginally more intrusive than opt-out, but would significantly advance consumer privacy.

II. There Are Strong Policy and Legal Bases for Including Personally Identifiable Information in the Definition of Customer Proprietary Information

Internet users value their privacy online. More than half of Americans believe people should have the ability to use the internet completely anonymously in some cases.⁶ Further, although internet users realize their personal information is available online, they want to control who can access this information.⁷ To give BIAS customers the full privacy protection they expect, customer PI must be defined broadly to include PII, which should be defined as information "linked or linkable" to an individual. The Commission has the authority to protect customer

⁵ 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>; White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (February 2012), <https://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

⁶ Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Research Ctr. (May 20, 2015), <http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>.

⁷ *Id.* at 4.

information beyond CPNI and there are strong public policy reasons for broadening the scope of the customer PI rules in this manner.

A. Limiting covered information to CPNI would exclude much of the data consumers find most sensitive and would not meet customer expectations

The Commission has proposed calling all customer information covered under the rules “customer PI.” Customer PI would include both CPNI and PII. CPNI would have the same definition as that outlined in Section 222(h).⁸ PII would be defined as information “linked or linkable” to an individual.⁹ We agree with this approach and strongly support the Commission extending the scope of its proposed customer PI rules to PII. Including PII in the definition of customer PI meets consumer expectations and will ensure that the rules offer comprehensive privacy protection for BIAS customers. Some of the data types American consumers find sensitive include Social Security Numbers, passwords, payment card information, identification numbers, financial information, credit card information, account balances, government-issued identification numbers, biometric identifiers, and automated or electronic signatures.¹⁰ Of these, American consumers find Social Security Numbers, health information and the content of phone conversations most sensitive — 90% of Americans surveyed reported that their Social Security number is “very sensitive.”¹¹ National Institute of Standards and Technology (NIST) includes many of the aforementioned data in its examples of PII as well.¹²

Excluding PII from the proposed rules would be contrary to decades of U.S. privacy regulation and public policy.¹³ Some may argue that the proposed rules should protect only CPNI.¹⁴ We implore the Commission to reject similar arguments that may be raised in this proceeding. Not only is this position legally flawed,¹⁵ but it is crippling from a public policy standpoint. The

⁸ 47 U.S.C. § 222(h); *NPRM*, at 2519 ¶ 57. Our analysis of what should be considered CPNI in the broadband context is discussed in section III, below.

⁹ *NPRM*, at 2519, 2520-22 ¶¶ 56-57, 60-63.

¹⁰ Morrison & Foerster, *Consumer Outlooks on Privacy* 7 (2016), www.mofo.com/~media/Files/Resources/2016/MoFoInsightsConsumerOutlooksPrivacy.pdf; see also Aurélie Pols, *Customer Expectations of Privacy vs. Consumer Empowerment*, LinkedIn Pulse (Aug. 6, 2015), <https://www.linkedin.com/pulse/customer-expectations-privacy-vs-consumer-empowerment-aur%C3%A9lie-pols> (reporting results of 2013 survey finding that credit card data, financial data, information about children, health/genetic data, and information about a spouse were considered the top five most private types of data).

¹¹ Mary Madden, *Americans Consider Certain Types of Data to Be More Sensitive Than Others*, Pew Research Ctr. (Nov. 12, 2014), <http://www.pewinternet.org/2014/11/12/americans-consider-certain-kinds-of-data-to-be-more-sensitive-than-others/> (“A full 90% of adults feel as though their social security is a ‘very sensitive’ piece of information, and this view is broadly held across all demographic groups.”).

¹² Erika McCallister, Tim Grance & Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* §§ 21-2.2, NIST (2010), <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf> (“*NIST Guide to Protecting PII*”).

¹³ See, e.g., 45 C.F.R. pt. 160, pt. 162 & pt. 164 (Health Insurance Portability and Accountability Act (HIPAA)); 7 C.F.R. pt. 248 (SEC) (Gramm-Leach-Bliley Act (GLBA)); 16 C.F.R. pt. 682 (Fair Credit Reporting Act (FCRA)); 12 C.F.R. pt. 1022 (Fair and Accurate Credit Transactions Act (FACTA)); 45 C.F.R. pt. 5b (Privacy Act); 34 C.F.R. pt. 99 (Family Educational Rights and Privacy Act Regulations (FERPA)); 47 C.F.R. §§ 64-76 (Communications Act); 47 CFR 64.1200 (Telephone Consumer Protection Act (TCPA)); 16 C.F.R. pt. 312 (Children’s Online Privacy Protection Rule (COPPA)); 16 C.F.R. pt. 316 (Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)).

¹⁴ This argument was recently raised in the voice context; last year the Wireless Association (CTIA) filed a petition requesting partial reconsideration of the FCC’s *Order on Reconsideration* for its Lifeline program on the contention that Section 222 only allows for customer information that falls within the definition of CPNI to receive privacy protection. See *Petition for Partial Reconsideration* by CTIA, WC Docket No. 11-42 et seq. (filed Aug. 13, 2015).

¹⁵ This is further discussed *infra* section II.C

definition of CPNI is limited to 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.”¹⁶ For broadband, this arguably includes service plan information, geo-location, MAC address and device identifiers, internet protocol (IP) addresses and domain name information, traffic statistics, Uniform Resource Locators (URLs), and other packet metadata.¹⁷ However, it is unlikely to include much of the aforementioned data consumers find sensitive, such as Social Security Numbers, home addresses, birthdates and financial information. Restricting the rules’ application to only CPNI would deny BIAS customers privacy protection for the majority of the information they expect to remain private. While it is critical that CPNI is broadly defined and protected under the proposed rules, limiting information covered under the rules to CPNI would defeat the purpose of this rulemaking.

B. The Commission’s definition of PII is appropriate

1. PII should be interpreted broadly to include any information linked or linkable to an individual

PII should be defined as any information that is linked, or linkable, to an individual. This comports with the majority of U.S. privacy laws and regulations,¹⁸ and allows for regulatory flexibility as technology evolves to enable identification of individuals through new techniques. “Identifiable” information is increasingly contextual; while one or two data points alone may not identify an individual, these data could be linked to that person if combined with other data.¹⁹ We have seen numerous examples of this in recent years: a journalist was able to identify where celebrities had traveled in New York based on paparazzi photos and publicly released taxi records;²⁰ Netflix’s Internet Movie Database was used to identify its customers and their political preferences;²¹ and human geneticists discovered the identities of individuals who had contributed their DNA sequence to a research project through cross-referencing information available in public databases.²² Just last year, data scientists linked credit card transactions to 1.1 million people using publicly available information and a data set that was believed to have been

¹⁶ 47 U.S.C. § 222(h)(1).

¹⁷ This is further discussed *infra* section III.A; *see also NPRM*, at 2514 ¶ 41.

¹⁸ *See NPRM*, at 2520 ¶ 60.

¹⁹ Daniel Solove & Latanya Sweeney, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U.L. Rev. 1814, 1818 (2011) (“[T]he ability to distinguish PII from non-PII is frequently contextual. Many kinds of information are not inherently non-identifiable, or identifiable as an abstract matter.”); Joshua J. McIntyre, Comment, *Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should be Protected as Personally Identifiable Information*, 60 DePaul L. Rev. 895, 906 & n.126 (2011) (“There is an inherent conflict between enumerating bright-line examples of PII and protecting data only when it identifies an individual in practice . . . what is meant by ‘personally identifiable information’ is not a piece of data that always identifies an individual but a piece of data that could identify an individual given the totality of the circumstances.”); 1-2A Computer Law § 2A.02, at 16 (2009) (“A person can be identified . . . by a combination of significant criteria that permits narrowing down the group to which he or she belongs. . . . Whether an individual is identified depends on the circumstances.”).

²⁰ J.K. Trotter, *Public NYC Taxicab Database Lets You See How Celebrities Tip*, Gawker (Oct. 23, 2014), <http://gawker.com/the-public-nyc-taxicab-database-that-accidentally-track-1646724546>.

²¹ Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, in Proceedings of the 2008 IEEE Symposium on Security & Privacy (S&P) 112 (2008), available at https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf

²² Erika Check Hayden, *Privacy Loophole Found in Genetic Databases*, Nature.com: News (Jan. 17, 2013), <http://www.nature.com/news/privacy-loophole-found-in-genetic-databases-1.12237#/ref-link-1>.

anonymized.²³ Limiting the definition of PII to specific types of data or data that by itself can identify an individual is problematic; the customer PI rules would not cover much of the information that might be used to link online activity to a particular BIAS customer.

2. *It is critical that PII include location data*

It is particularly important that the Commission include location data as an example of PII. Location data can reveal intimate details about an individual²⁴ such as the types of doctors and clinics they visit, where they live, who lives with them, when they are away from their home for extended periods, and where their children go to school. Leaving this data unprotected or allowing it to land in unintended hands it could lead to a host of harms such as domestic abuse, stalking, theft and discrimination.²⁵ According to the U.S. Government Accountability Office (GAO), “when location data are amassed over time, they can create a detailed profile of individual behavior, including habits, preferences, and routes traveled—private information that could be exploited.”²⁶ The FTC agrees that location data deserves privacy protection and is “particularly useful for uniquely identifying (or re-identifying) individuals using disparate bits of data.”²⁷

Additionally, consumers are increasingly hesitant to share location data. Eighty-two percent of Americans feel the details of their physical location gathered over a period of time are sensitive.²⁸ In some cases consumers value location data as highly as health data.²⁹ One study reported that consumers would not trade their location data even for discounts on a product, such as car insurance.³⁰ Consumers were hesitant to share location data in this circumstance for a range of reasons, including lack of trust in the entity gathering the location data, worries about being surveilled by “big brother,” and concerns about the data being used discriminatorily.³¹ Smartphone technologies have raised consumer awareness of these privacy risks.³² This is

²³ Natasha Singer, *With a Few Bits of Data, Researchers Identify ‘Anonymous’ People*, N.Y. Times: Bits (Jan. 29, 2015, 2:01 PM), http://bits.blogs.nytimes.com/2015/01/29/with-a-few-bits-of-data-researchers-identify-anonymous-people/?_r=0; see also Gretchen McCord, *What You Should Know About “Anonymous” Aggregate Data About You*, Am. Libr. Ass’n: Choose Privacy Week 2015 (May 5, 2015), <https://chooseprivacyweek.org/choose-privacy-week-2015-what-you-should-know-about-anonymous-aggregate-data-about-you/>; Alessandro Acquisti & Ralph Gross, *Predicting Social Security Numbers from Public Data*, 106 Proceedings of the Nat’l Acad. of Sci. (no. 27) 10975-80 (July 7, 2009), available at <http://www.pnas.org/content/106/27/10975.full.pdf>.

²⁴ Trotter, *How Celebrities Tip*.

²⁵ Danielle Citron, *BEWARE: The Dangers of Location Data*, Forbes (Dec. 24, 2014), <http://www.forbes.com/sites/daniellecitron/2014/12/24/beware-the-dangers-of-location-data/#164afdb66968>.

²⁶ Consumers’ Location Data – Companies Take Steps to Protect Privacy, but Practices Are Inconsistent, and Risks May Not Be Clear to Consumers: Hearing Before the S. Subcomm. on Privacy, Technology and the Law of the S. Comm. on the Judiciary, 113th Cong. 2 (2014) (statement of Mark L. Goldstein, Dir., Physical Infrastructure Issues, Gov’t Accountability Off.), available at <http://gao.gov/assets/670/663787.pdf>.

²⁷ Fed. Trade Comm’n, *Protecting Consumer Privacy in an Era of Rapid Change, A Proposed Framework for Businesses and Policymakers* 33 (Mar. 2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

²⁸ Marry Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Ctr. 34 (Nov. 12, 2014), available at <http://www.pewinternet.org/2014/11/12/americans-consider-certain-kinds-of-data-to-be-more-sensitive-than-others/> (report concludes that 82% of Americans feel details of their physical location is sensitive).

²⁹ 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#>.

³⁰ *Id.* at 26.

³¹ *Id.* at 28-29 (one participant noted: “if they hike my rates due to location; for example, if they perceive an area to be unsafe, I wouldn’t think that is fair. Lots of people work/live in high crime areas, and I don’t think they should be penalized for that.”).

³² Lee Rainie & Maeve Duggan, *Privacy and Information Sharing*, Pew Research Ctr. 5 (Jan. 14, 2016), available at http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf (“Location data seems

unsurprising—sharing the location of a home computer is markedly different from sharing the location of a device carried on one’s person throughout the day. Despite these concerns, BIAS providers’ collection and monetization of location data is commonplace.³³ If the Commission’s rules provide no protection for customer location data, many of these practices would continue without limitation.

C. The Commission has authority under 222(a) to create privacy rules for information beyond CPNI

1. The statute and legislative history support this conclusion

The Commission has the authority to protect customer information beyond CPNI. The plain language of 222(a) necessitates that carriers “protect the confidentiality of proprietary information of, and relating to... customers.”³⁴ It is the Commission’s responsibility to ensure that carriers comply with this mandate for all customer PI, not just CPNI. Legislative history supports this conclusion. The Conference Report for the 1996 version of the Communications Act says 222(a) “stipulates that it is the duty of every telecommunications carrier to protect the confidentiality of proprietary information of and relating to other carriers, equipment manufacturers and customers.”³⁵ The report does not suggest this is only required for CPNI, so one could reasonably conclude that this provision of the Act addresses a broader set of customer information.

especially precious in the age of the smartphone. Some of the most strongly negative reactions came in response to scenarios involving the sharing of personal location data. One respondent put it as follows: ‘I continually deny location services on my phone because I don’t want the chance of ads coming up.’”

³³ See Press Release, AT&T, *AT&T Data Patterns Gives Advertisers New Insights on Out-of-Home Media* (Dec. 12, 2015), http://about.att.com/story/data_patterns_gives_advertisers_new_insights.html (noting in December 2015, AT&T announced the launch of a third-party advertising feature that used anonymous and aggregated AT&T customer location data to determine if customers interacted with an advertisement after seeing it – such as by visiting the advertised store. AT&T marketed its “Data Patterns” feature as a way for companies to measure consumer “lift” – “the percentage of an audience that passed an outdoor advertisement and later watched TV programming that was promoted on the ad.” It continued: “In retail, when a store location also uses AT&T Wi-Fi, AT&T Data Patterns can measure the percentage of an OOH audience that converts into store visits. In each case, the numeric percentage is passed to clients as a statistic, giving them insight into campaign effectiveness.”); Comcast, *Comcast Spotlight Strengthens Audience Connection with Data Partnership*, <http://corporate.comcast.com/news-information/news-feed/comcast-spotlight-strengthens-audience-connection-with-data-partnership> (last visited May 24, 2016) (“Comcast Spotlight is able to show clients how local cable advertising can pinpoint the neighborhoods where their customers (and prospective customers) live, overlaying that with aggregated information about what those audiences are watching. Data can be analyzed and summarized at multiple geographic levels, from a market-wide perspective down to a zone level analysis.”); Cox, *About Location-Based Advertising*, Cox Residential Internet Support (Sept. 15, 2015), <http://www.cox.com/residential/support/internet/article.cox?articleId=%7B5074dfe0-12cc-11e0-cf95-000000000000%7D> (“Location-based advertising helps deliver offers and incentives from national brands and local businesses with content tailored to your area. Location-based advertising uses your zip code, including the last four digits, to identify your area and display relevant ads...For example, if a local pizza parlor wants to offer coupons to customers who live in a certain area, they can ensure online ads are only shown to high-speed Internet customers who actually live in that area.”). See also Ben Popper, *Verizon Reportedly Planning to Share Customer Location Data with AOL Advertisers*, The Verge (Mar. 30, 2016), <http://www.theverge.com/2016/3/30/11330812/verizon-share-customer-location-data-with-aol-advertising> (a small group of AOL advertisers were reported to have been granted access to Verizon data on cellphone users’ locations to reveal if Verizon customers visited a retail store after seeing an advertisement).

³⁴ 47 U.S.C. § 222(a).

³⁵ See Appalshop et al., Letter of Opposition to Petition for Partial Reconsideration In the Matter of Lifeline and Link Up Reform and Modernization, Telecommunications Carriers Eligible for Universal Service Support, Connect America Fund 13 (Oct. 9, 2014), available at <https://cdt.org/files/2015/10/Lifeline-Petition-Opposition.pdf>.

2. *Uses of “proprietary information” throughout the Communications Act as well as in other laws support this conclusion*

222(a)’s use of the term “proprietary information” as opposed to “personal information” or “personally identifiable information” does not foreclose an interpretation of proprietary information that includes customer information beyond CPNI. This is illustrated by the use of this term in separate sections of the Communications Act and other laws.

“Proprietary information” is used approximately 20 times in the Communications Act; at least half of these mentions are in completely separate sections from 222.³⁶ Use of “proprietary information” throughout the Communications Act suggests that proprietary information includes a range of material that would be reasonably expected to remain private, including data collected during audits and equipment procurement, and also data whose owner has indicated it should remain private. For example, Section 273 explicitly prohibits entities that set standards for or certify telecommunications-related equipment from releasing or otherwise using any proprietary information received during the standards-setting or certification process.³⁷ Section 273 gives owners of information obtained during standards-setting or certification processes broad discretion to determine what is proprietary.³⁸

Furthermore, the term “proprietary information” is used in a number of other statutes,³⁹ and interpreted broadly in some corresponding rules. For instance, the Housing and Community Development Act gives the Department of Housing and Urban Development (HUD) complete discretion to determine what information in a low-income housing termination plan is proprietary. According to the Act, any owner submitting a plan to terminate or adjust low-income housing shall submit all documentation supporting this plan to existing tenants upon request, but this documentation should not include “any information that the Secretary determines is proprietary information.”⁴⁰ HUD rules define “proprietary information” as “that information which cannot be released to the public because it consists of trade secrets, *confidential financial information, audits, personal financial information about partners in the ownership entity, or income data on project tenants.*”⁴¹ HUD’s definition of proprietary information is a strong indicator that Congress understood proprietary information would have a broad interpretation in 222(a).

III. **Customer Proprietary Information Must Include Packet Metadata**

Many, if not all, data points contained in the headers of IP packets should fall within the statutory definition of CPNI. Additionally, some of this metadata arguably fits the Commission’s proposed definition of PII. Metadata can be used, with or without its associated content, to create comprehensive customer profiles and to draw increasingly detailed inferences about

³⁶ See, e.g., 47 U.S.C. §§ 251, 272-74, 396, 605.

³⁷ 47 U.S.C. § 273.

³⁸ 47 U.S.C. § 273(d)(2) (prohibits release of PI “designated as such by its owner . . . for any purpose other than purposes authorized in writing by the owner of such information”).

³⁹ 12 U.S.C. § 4107(a)(2) (HUD); 10 U.S.C.S. § 129d(b) (U.S. Armed Services Law); 42 U.S.C.S. § 17112 (Public Health Service Act).

⁴⁰ 12 U.S.C.S. § 4107.

⁴¹ 24 C.F.R. § 248.101 (emphasis added).

individuals.⁴² Therefore, in the broadband context, CPNI must include packet metadata to ensure the rules provide privacy protection for BIAS customers.

A. The information in packet headers fits the definition of CPNI and may also contain PII

Every communication transmitted across the internet is sent as a packet or a series of packets.⁴³ The content, or payload, of these packets consists of data that is either created by or sent to applications running on the computers at the endpoints of the communication. Before it can be sent from one computer to another, however, the application data must be labeled with different kinds of routing and handling information to enable the programs responsible for sending, receiving, sorting, managing, and distributing network communications to efficiently and accurately perform those functions. This information is often described in terms of a “layered” model where each layer encapsulates information from the previous networking layer in an “envelope” adding metadata in the form of “headers” to the payload of packets, which contain information about themselves and the layers within. Much of the information in packet headers “relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service” and is “made available to the carrier by the customer solely by virtue of the carrier-customer relationship.”⁴⁴

1. Frame headers contain device identifiers and information relating to the destination of telecommunications services

The header fields for common protocols at each layer of an IP packet reveal several data points fitting the statutory definition of CPNI. The network layer contains a header referred to as the “frame” header where an Ethernet or WiFi connection is used,⁴⁵ contains the Media Access Control (MAC) address (a type of device identifier) of the individual device communicating with a network hub, which mediates communications outside of the local network. Each of the devices connected to a customer’s home network, whether by WiFi or Ethernet cable, sends its MAC address as part of the frame header in each transmission sent to the home network’s router. Likewise, the modem or server linking a home network to the BIAS provider’s network sends its MAC address along with each packet it sends out. This is one way in which more than one local area network (LAN) may be connected to a single subscriber account with only one IP address. Although in most cases⁴⁶ a modem connecting a customer’s home network to the BIAS

⁴² See Jonathan Mayer et al., *Evaluating the Privacy Properties of Telephone Metadata*, 113 Proceedings of the Nat’l Acad. of Sci. (no. 20) 5536 (Mar. 1, 2016), available at <http://www.pnas.org/content/113/20/5536> (finding that telephone metadata is highly interconnected, can trivially be re-identified, enables automated location and relationship inferences, and can be used to determine highly sensitive traits).

⁴³ See Center for Democracy & Technology, *Applying Communications Act Consumer Privacy Protections to Broadband Providers* (Jan. 20, 2016) (“CDT CPNI Chart”), <https://cdt.org/insight/applying-communications-act-consumer-privacy-protections-to-broadband-providers/>; see also Rus Shuler, *How Does the Internet Work?*, Pomeroy IT Solutions (2002), <https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm>.

⁴⁴ 47 U.S.C. § 222(h)(1)(A); Sandvine, *Internet Traffic Classification*, at 7 (one vendor describes these data points as “attributes” of network traffic that can be linked to individual subscribers).

⁴⁵ Ethernet and WiFi are part of what are referred to as “link layer” networking protocols that operate one layer beneath the internetworking layer (mediated by the Internet Protocol). See CDT CPNI Chart.

⁴⁶ Most BIAS modems rely on the IP to carry traffic outside of the home network, in which the frame envelope is removed, so MAC addresses in frame headers are not relevant to what a BIAS provider can see. There are nascent technologies such as Network Function Virtualization that would replace certain customer premises equipment like modems and routers with “virtualized” appliances (essentially software substitutes). In these cases, frame data may leave the home network and MAC

provider's network removes the MAC addresses of individual devices before sending packets out across the network, the MAC addresses of devices connected to the home network may also be included elsewhere in packets, such as in the payload or header at the application layer.⁴⁷ There are also network configurations in which individual device identifiers are sent directly to the BIAS provider, most commonly in the case of international mobile subscriber identity (IMSI) numbers for mobile devices.⁴⁸ The MAC address could therefore be visible to the BIAS provider in these cases.

MAC addresses and other device identifiers relate to the destination of a telecommunications service because they are used to route packets to individual devices connected to a network. As persistent, unique identifiers, MAC addresses may also be linked or linkable to individuals, particularly when associated with other information a BIAS provider may have, such as subscriber names or telephone numbers. Therefore, device identifiers fit the definitions of both CPNI and PII.

2. IP headers contain information relating to the destination and amount of use of a telecommunications service

The next layer up from the network layer, the IP layer, contains the routing information BIAS providers use to deliver packets across their networks. All packets sent by subscribers across a BIAS provider's network will contain an IP header, and may also contain header information for additional protocols operating at this layer.⁴⁹ The IP header will contain the IP addresses of both sender and receiver and will indicate the total size, in bytes, of the packet.⁵⁰ IP addresses are the destinations to which BIAS providers deliver packets and also may be associated with physical locations. Therefore, IP addresses should be considered CPNI. Likewise, the IP header field denoting packet size indicates the amount of use a customer makes of a telecommunications service. Therefore, packet length also fits the statutory definition of CPNI.

3. Transport layer headers contain information relating to the destination and amount of use of a telecommunications service

At the transport layer, the two most common protocols, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) include header fields specifying source and destination ports as well as packet size. Network ports are subaddresses within the internet protocol and are used by operating systems to sort and deliver packets to individual applications. Essentially, ports are a more granular form of destination information than IP and MAC addresses, indicating which

addresses would then be available to the BIAS provider directly from the frame header. See Margaret Chiosi et al., *Network Functions Virtualisation: An Introduction, Benefits, Enablers, Challenges & Call for Action* (Oct. 22-24, 2012) available at https://portal.etsi.org/NFV/NFV_White_Paper.pdf.

⁴⁷ Any software program with network capability, for example, some Java-based programs or applications on certain platforms, can read a MAC address then transmit it in the application layer, as part of a URL, or other non-frame header locations.

⁴⁸ International mobile subscriber identity (IMSI) is the customer account's unique identification number across cell networks. See International Mobile Subscriber Identity (IMSI) Definition, Techopedia, <https://www.techopedia.com/definition/5067/international-mobile-subscriber-identity-imsi> (last visited May 20, 2016).

⁴⁹ For example, BGP is used to route traffic between different networks (called "autonomous systems"). See Internet Eng'g Task Force, A Border Gateway Protocol 4 (BGP-4), RFC 4271, IETF Tools (January 2006), available at <https://tools.ietf.org/html/rfc4271>.

⁵⁰ IP packets can be up to 65535 bytes long. DARPA Internet Program Protocol Specifications 12, RFC 791 (September 1981), available at <https://tools.ietf.org/html/rfc791>.

applications particular packets may be destined. For instance, ports 109 and 110 indicate the use of the Post Office Protocol (POP), marking the packet as an email transmission, while port 1214 indicates use of the Kazaa peer-to-peer file sharing protocol. An IP address combined with a port number is known as a socket and serves as the address for a specific connection between network endpoints. This combination is analogous to the combination of a telephone number and an extension, providing more specific routing information to facilitate more efficient communications management. This level of specificity also provides a more detailed picture of customers' uses of BIAS connections and provides clues as to which applications they may use. Network ports relate to the destination of a packet and as such should be considered CPNI.

4. Application headers contain information relating to the destination and location of a telecommunications service

Above the transport layer is the application layer, which contains both header information and the packet's payload. The majority of BIAS network traffic will carry application data using the Hypertext Transfer Protocol (HTTP).⁵¹ The structure of HTTP transmissions includes an initial request or response line, header lines, and the message body. When a user accesses a web site, her computer sends a request to the server asking for a specific file located within a host on the server using the host's name and path name associated with that file. In the address bar of a browser, the host's name is the domain name (cdt.org) and everything after the domain name describes the path to the file's location on the server (/insight/broadband-privacy-comments-fcc-nprm-2016/). This file path is called a Uniform Resource Locator (URL) because it specifies the exact location of the file or set of files that comprise an individual web page. Therefore, domain names and URLs should be considered CPNI because they relate to the destination or location of a customer's use of a telecommunications service.

5. Unique identifiers added to packet headers are PII and CPNI

In the practice known as "HTTP header injection," BIAS providers add a new HTTP header line after the message leaves the customer's browser.⁵² This header serves as a unique marker identifying all HTTP messages sent from a single subscriber account. In so doing, unique identifiers in application layer headers are "linked or linkable" to the BIAS customer. These identifiers also encompass each element of CPNI, relating the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service to an individual subscriber. Therefore, unique identifiers appended to packets could be considered both CPNI and PII. Although the uniquely identifying header is added by the BIAS provider in this case, it is "made available" by the customer's use of unencrypted HTTP. This is true regardless of whether the unique identifier is added by a BIAS provider or a third party, so long as the BIAS provider leverages its control over the customer's network traffic to collect this information.⁵³

⁵¹ Applying the definition of CPNI and PII to HTTP data will provide broad protections to most BIAS customers. However, any new rules or interpretations should not preclude the application of section 222 to the kinds of information carried by other application-layer protocols or future protocols that may become as popular as HTTP is now.

⁵² See Mark Bergen & Alex Kantrowitz, *Verizon Looks to Target Its Mobile Subscribers with Ads*, Advertising Age (May 21, 2014), <http://adage.com/article/digital/verizon-target-mobile-subscribers-ads/293356/>.

⁵³ See *Carrier IQ Declaratory Ruling*, 28 FCC Rcd. 9609, 9611 ¶ 7 ("When providers of mobile telecommunications service leverage their control of their customers' mobile devices to collect information that relates to the quantity, technical configuration, type, destination, location, and amount of use of the telecommunications service, that information is 'made available to the carrier by the customer solely by virtue of the carrier-customer relationship' and therefore is CPNI. A

B. Long-term monitoring of network traffic raises privacy concerns

The metadata from even a single packet may reveal much about a person, such as signs of the sites they have visited and location from which they use BIAS. Furthermore, the scope of personal information made available through network traffic adds weight to concerns raised by longer-term monitoring or logging of packet metadata and other metrics of network usage.⁵⁴ For instance, by monitoring the timing, frequency, and quantity of broadband transmissions, a network operator could infer whether subscribers are at home, when they sleep, whether they are browsing the internet or streaming music, or when multiple devices are sending messages.⁵⁵

Adding a record of IP addresses that a subscriber communicates to and from increases both the accuracy and the scope of these inferences. Sorting packet streams by the IP addresses with which a subscriber communicates would help determine how many devices or applications a subscriber is using at one time and could provide clues as to the geographic location and identity of the network endpoints with which the subscriber is communicating.⁵⁶ Adding details about packet size to the patterns observed in the timing, frequency, quantity, and IP address logs adds certainty to the inferences made about what kinds of activities a subscriber is conducting online. An hours-long stream of regularly-spaced groups of packets might indicate that the subscriber is streaming audio or video, while a shorter burst of large packets might indicate a download. When matched with a database of common edge providers' known IP addresses, one could infer that, for example, on weeknights a subscriber streams video from a popular service between 8 and 10 PM, then browses the internet until 11 PM, then stops actively accessing the internet until 6 AM when they check their email and stream audio from another popular service until 8 AM.

Since every header within a packet adds detail to its routing and handling information, the farther “up the stack” one looks when monitoring IP traffic, the more detail one receives about the communication itself. Such detailed information about a customer's communications may reveal more than just patterns of broadband usage; but also clues as to the content of those communications and the behaviors and interests of that customer.

C. Encryption technologies do not adequately address privacy concerns

BIAS transmissions may be encrypted in a variety of ways, and either the user or the edge provider may choose to use encryption. Some encryption methods can be initialized by the user to route incoming and outgoing traffic through remote servers, which encrypt both the payload and the headers of IP packets before wrapping them in new IP headers using the server's routing

telecommunications carrier that collects CPNI by virtue of its control over its customer's mobile device is obligated to protect that information by the [Communications] Act and by the Commission's rules.”)

⁵⁴ Aaron Rieke, David Robinson & Harlan Yu, *What ISPs Can See: Clarifying the Technical Landscape of the Broadband Privacy Debate* 7, Upturn (March 2016), <https://www.teamupturn.com/reports/2016/what-isps-can-see> (“What ISPs Can See”).

⁵⁵ See *What ISPs Can See*, at 7-9; Nick Feamster et al., *Peeking Behind the NAT: An Empirical Study of Home Networks*, in Proceedings of the ACM SIGCOMM Conference on Internet Measurement, IMC13 (2013) (“Peeking Behind the NAT”); see also Nick Feamster, *Who Will Secure the Internet of Things?*, Freedom to Tinker (Jan. 16, 2016), <https://freedom-to-tinker.com/blog/feamster/what-your-isp-probably-knows-about-you/>; Sarthak Grover & Nick Feamster, *The Internet of Unpatched Things*, PrivacyCon 2016 Slideshow, <https://www.dropbox.com/s/36nxibezelxrduk/FTC-PrivacyCon-2016.pdf>.

⁵⁶ For example, companies that sell IP address geolocation services claim that 46% of U.S. IP addresses can be resolved to an exact postal address. See MaxMind, *GeoIP2 City Accuracy*, <https://www.maxmind.com/en/geoip2-city-database-accuracy?country=&resolution=postal> (last visited May 20, 2016).

location.⁵⁷ Other methods simply encrypt the application data, leaving the packet routing information “in the clear” (unencrypted).⁵⁸ Although the use of encryption technologies by both subscribers and edge providers has risen significantly in the last few years, many transmissions remain unencrypted.⁵⁹ BIAS subscribers sending and receiving unencrypted transmissions are no less deserving of privacy protections than subscribers who only visit sites supporting HTTPS or who employ proxy or VPN services. As discussed above, even when application-layer encryption technologies like HTTPS obscure the payloads of packets, the routing information that remains visible may contain data that is CPNI, PII, or both.⁶⁰ Therefore, regardless of positive trends in the use of encryption technologies, packet metadata should be considered CPNI so that the Commission’s rules ensure privacy protection for all broadband subscribers.

IV. Customer Opt-In Should Be Required for the Majority of Secondary Uses of Customer Proprietary Information; However, Opt-Out Approval May Be Appropriate in Some Circumstances

CDT supports the Commission’s proposal generally requiring customer opt-in for use and sharing of customer data for marketing products and services unrelated to the service a customer has purchased. However, customer opt-out would be sufficient for first-party and affiliate use and sharing of data to market “communications-related services.” These proposed use and choice rules would advance the Commission’s interest in protecting the privacy of customer PI while giving BIAS providers considerable latitude to use customer PI for marketing.

A. The Commission has a substantial interest in protecting the privacy of customer PI

1. BIAS providers are uniquely positioned to have access to large amounts of very detailed customer PI

Consumers have an undeniably intimate relationship with their BIAS providers. Over seventy-four percent of U.S. households use the internet,⁶¹ sending emails, conducting search queries, streaming video, paying bills, posting on social media, and more through their broadband

⁵⁷ Microsoft, *How VPN Works*, TechNet (Mar. 28, 2003), <https://technet.microsoft.com/en-us/library/cc779919%28v=ws.10%29.aspx>.

⁵⁸ The HTTP over TLS protocol (commonly referred to as simply “HTTPS”) reveals which website a packet is destined for and the IP address of its source. For example, if a user loads the website for the National Domestic Violence Hotline, <http://www.thehotline.org/>, a network provider may not be able to see the content of what was loaded, but sensitive information (the fact the user seeks help with domestic violence) is revealed.

⁵⁹ See Peter Swire et al., *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* 3, Inst. for Info. Security & Privacy (Feb. 29, 2016), http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf (projecting 70% encryption rate for web traffic at close of 2016); but see *What ISPs Can See*, at 4 (reporting that more than 85% of top 50 sites fail to encrypt by default); Feamster, *Who Will Secure the Internet of Things?* (reporting high rates of cleartext traffic among Internet of Things devices).

⁶⁰ Some traffic classification techniques can even penetrate tunneling and encapsulation-style encryption. Sandvine, *Internet Traffic Classification* 5, Sandvine.com (2015), <https://www.sandvine.com/downloads/general/sandvine-technology-showcases/traffic-classification-identifying-and-measuring-internet-traffic.pdf> (last visited May 20, 2016).

⁶¹ Thom File & Camille Ryan, *Computer and Internet Use in the United States: 2013*, U.S. Census Bureau, American Community Survey Reports, ACS-28 (November 2014) (“In 2013, 74.4 percent of all households reported Internet use, with 73.4 percent reporting a high-speed connection . . .”).

service. Most adults stay connected when they leave home through smartphones.⁶² However, the prevalence of internet use is not complemented with a diversity of options for connecting to the internet. The BIAS market is dominated by a handful of companies: just five companies controlled nearly seventy percent of the market in 2013.⁶³ These industry leaders provide the conduits through which the majority of U.S. internet traffic travels. As such, they have access to information on that traffic and can paint increasingly detailed pictures of U.S. online activity – so much so that researchers have written entire papers on human behavior solely by analyzing internet transmission data.⁶⁴ This is the case even when considering what BIAS providers can glean from residential broadband services alone.⁶⁵

BIAS providers do not have to barter or purchase this intimate view into their customers' digital lives. Moreover, unlike most other participants in the internet ecosystem, BIAS providers almost always have access to personal information on subscribers such as home address, billing information, and Social Security numbers. This information, when combined with customers' online activity, presents a very detailed profile of that individual. BIAS providers' ability to monitor and track consumers' activity across the internet has been described as potentially "vast" and "completely invisible" by the FTC.⁶⁶ Of the players in the digital market, they arguably come closest to having a total view of U.S. internet users. Therefore, the privacy implications associated with BIAS data collection are especially significant.

⁶² The majority of U.S. adults had a smartphone at the close of 2015. Monica Anderson, *Technology Device Ownership: 2015* Pew Research Ctr. (Oct. 29, 2015), <http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/>. During the period November 2015 to January 2016, 98.5 million people in the U.S. owned smartphones, and smartphones control 79.1% of the mobile market. ComScore, *ComScore Reports January 2016 U.S. Smartphone Subscriber Market Share* (Mar. 3, 2016), <https://www.comscore.com/Insights/Rankings/comScore-Reports-January-2016-US-Smartphone-Subscriber-Market-Share> (last visited May 5, 2016).

⁶³ Comcast, AT&T, Verizon, Time Warner Cable and CenturyLink – all of which offer cable or satellite services – controlled nearly 70% of the BIAS market in 2013. Emil Protalinski, *Over 70% of U.S. Households Now Have Broadband Internet Access, With Cable Powering Over 50% of the Market*, NextWeb (Dec. 9, 2013), <http://thenextweb.com/insider/2013/12/09/70-us-households-now-broadband-internet-access-cable-powering-50-market/#gref>; see also Webpage FX, *Who Controls the Internet: A State-by-State Look*, <http://www.webpagefx.com/blog/internet/who-controls-the-internet-a-state-by-state-look/> (last visited May 5, 2016). This is not only the case for residential broadband; many mobile hotspot networks are operated by the same five providers. Comcast's Xfinity WiFi roaming service increased 500% in 2015, deploying 10 million WiFi hotspots which users accessed 3.6 billion times during the year. Jeff Baumgartner, *Comcast Wifi Net Surpasses 10m Hotspots*, Multichannel News (July 27, 2015), <http://www.multichannel.com/news/technology/comcast-wifi-net-surpasses-10m-hotspots/392510>. Time Warner Cable was similarly successful in this area: last year Time Warner Cable Internet subs engaged in more than 180 million WiFi sessions on its network, up 327% from the previous year. Jeff Baumgartner, *Time Warner Cable's WiFi Net Hits 100K+ Hotspots*, Multichannel News (June 4, 2015), <http://www.multichannel.com/news/technology/time-warner-cable-s-wifi-net-hits-100k-hotspots/391106>.

⁶⁴ Letter from Princeton Professor Nick Feamster to FCC Chairman Tom Wheeler (Mar. 3, 2016), available at <http://ftt-uploads.s3.amazonaws.com/fcc-cpni-nprm.pdf>.

⁶⁵ *Id.* (“[M]ost users rely exclusively on one Internet Service Provider (ISP) for home broadband internet access, which places a substantial fraction of user activity within the purview of a single ISP; the shared access points that these ISPs now [have] exacerbate this consolidation.”). Note that individual device identifiers are stripped by the home network router and all its transmissions to the BIAS provider, which would have only the routing information necessary to identify the router as the sender/receiver. *Peeking Behind the NAT* at 1.

⁶⁶ Fed. Trade Comm’n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* 56, FTC.gov (2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> (“2012 FTC Privacy Report”).

2. *BIAS providers' secondary use of customer PI has important privacy implications*

BIAS providers have the incentive to use or share their customers' data because it is highly valuable to third parties wishing to market products and services to subscribers. However, consumers have repeatedly expressed dissatisfaction with companies' unauthorized uses of their personal information and their lack of control over these uses.⁶⁷ Studies show that over half of Americans do not want to lose control of their data online, but believe such loss is an inevitable consequence of internet use.⁶⁸ Ninety-three percent of recently surveyed consumers described the ability to control who can access information about them as "important" and seventy-four percent felt this was "very important."⁶⁹ These sentiments are understandable. Irrelevant or unexpected marketing may lead to embarrassment or exposure of information a person prefers to keep private.⁷⁰ Additionally, data breach impacts the entire online community, including BIAS providers.⁷¹ A 2014 study found that sixty percent of U.S. companies have experienced more than one data breach in the past two years, and that breaches were increasing in frequency.⁷² Large accumulations of personal information are a valuable target for bad actors who exploit breached databases for a range of reasons. Some hold accounts hostage until ransom is paid, or sell the stolen information in underground markets, where buyers may bid on individuals' identities to open or exhaust lines of credit.⁷³ Others engage in political or moral campaigns, threatening to use or expose data for the purpose of extortion or public humiliation.⁷⁴ These

⁶⁷ Rainie & Duggan, *Privacy and Information Sharing*, Pew Research Ctr. ("People are not happy when data are collected for one purpose but are used for other, often more invasive purposes. Many Americans express suspicion that data collectors (from employers to advertisers) have ulterior motives in their pursuit of personal data. One respondent put it this way: 'I do not trust insurance companies, and I feel they could use this data to increase my rates under whatever pretend excuse. Insurance companies are in the risk management business, and they cannot reduce that risk at the cost of their customers. The more they know, the less risk for them and the higher cost for customers.'").

⁶⁸ Joseph Turow, Michael Hennessy & Nora Draper, *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation*, Univ. of Penn. Annenberg School of Comm'n 3 (June 2015), available at https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

⁶⁹ See Madden & Rainie, *Americans' Attitudes*, Pew Research Ctr.

⁷⁰ Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before her Father Did*, Forbes (Feb. 2, 2012), <http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#2b1e880634c6>; see also Ithaca College, *Online Creep: Targeted Ads May Have Opposite Effect of Marketers' Intent*, Science Daily (April 2015) <https://www.sciencedaily.com/releases/2015/04/150408171201.htm> (suggesting that consumers may find certain targeted advertising based on web browsing habits "creepy" and reduce interactions with a service as a result).

⁷¹ In March 2016, Verizon suffered a breach of an estimated 1.5 million customers' data. The database was advertised for sale on an online forum for \$100,000. *Verizon Enterprise Data Breach*, Fortune (March 24, 2016),

<http://fortune.com/2016/03/24/verizon-enterprise-data-breach/>. Last year, 280,000 AT&T customer names and partial social security numbers were released and then used by unauthorized parties to attempt to unlock stolen cell phones. *AT&T Data Breaches Revealed 280k U.S. Customers Exposed*, CNBC.com (April 8, 2015), <http://www.cnbc.com/2015/04/08/att-data-breaches-revealed-280k-us-customers-exposed.html>. Over 156,000 customers of UK telecommunications company TalkTalk experienced data breaches (including debit and credit card numbers) this past November. Sean Farrell, *Nearly 157,000 Had Data Breached in TalkTalk Cyber Attack*, Guardian (Nov. 6, 2015), <https://www.theguardian.com/business/2015/nov/06/nearly-157000-had-data-breached-in-talktalk-cyber-attack>.

⁷² Morgan Kennedy, *Ponemon Institute Releases Second Annual Study on Data Breach Preparedness*, Inside Privacy Blog (Oct. 1, 2014), <https://www.insideprivacy.com/data-security/ponemon-institute-releases-second-annual-study-on-data-breach-preparedness/>.

⁷³ Joseph Cox, *Ransomware Complaints Double in a Year, Total Over \$1.5 Million*, Motherboard (May 25, 2016), <http://motherboard.vice.com/read/ransomware-complaints-double-in-a-year-total-over-15-million>; Candid Wueest, *Underground Black Market: Thriving Trade in Stolen Data, Malware, and Attack Services*, Symantec (Nov. 20, 2015), <http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services>.

⁷⁴ See Kim Zetter, *Hackers Finally Post Stolen Ashley Madison Data*, Wired (Aug. 18, 2015), <http://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/>; Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harv. Univ. Press 2014); Jon Ronson, *So You've Been Publicly Shamed* (Riverhead Books 2015); see also NIST *Guide to Protecting PII*, at 2-1 ("Unauthorized access, use, or disclosure of PII can seriously harm both individuals, by

reports, in addition to news of hacks into major retail chain, entertainment studio, bank, voter registration system, healthcare provider and even federal government databases,⁷⁵ underscore the need for BIAS customer PI rules that set reasonable standards for not only data security, but also data sharing.

Failing to protect customer information against unauthorized intrusion and to give consumers control over how their data is shared can have profound repercussions for a person's life and willingness to participate in social, political, and economic activities online.⁷⁶ BIAS customers should therefore have a say in whether certain secondary uses of their data are appropriate. This builds consumer trust.

3. Consumer privacy cannot be preserved unless there are reasonable conditions on BIAS providers' secondary use of customer PI

Section 222 and its legislative history indicate Congress agreed that customer information gathered by carriers in the provision of telecommunications services deserves privacy protection and that the privacy of customer information cannot be preserved without placing conditions on secondary uses of this information.⁷⁷ Congress chose prior customer approval as one such condition. The Commission implemented this condition in its 2007 rules delineating customer opt-in and opt-out requirements. The Commission should similarly "rel[y] on Congress's reasonable, common sense determination that express customer consent [is] required"⁷⁸ in the present proceeding.

contributing to identity theft, blackmail, or embarrassment, and the organization, by reducing public trust in the organization or creating legal liability").

⁷⁵ See Ahiza Garcia, *Target Settles for \$39 Million Over Data Breach*, CNN.com (Dec. 2, 2015),

<http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/>; Kim Zetter, *The Year's Worst Hacks, From Sony to Celebrity Nude Pics*, Wired (Dec. 23, 2014), <http://www.wired.com/2014/12/top-hacks-2014/>; Matthew Goldstein, Nicole Perlroth & David E. Sanger, *Hackers' Attack Cracked 10 Financial Firms in Major Assault*, N.Y. Times (Oct. 3, 2014), http://dealbook.nytimes.com/2014/10/03/hackers-attack-cracked-10-banks-in-major-assault/?_r=0; Katie Bo Williams, *Report: 191M Voter Records Exposed Online*, Hill (Dec. 28, 2015), <http://thehill.com/policy/cybersecurity/264297-report-191m-voter-records-exposed-publicly-online>; Jeff Stone, *10 Million Records Exposed in BlueCross BlueShield Hack: Why That May Be Just the Beginning*, Int'l Business Times (Sept. 10, 2015), <http://www.ibtimes.com/10-million-records-exposed-bluecross-blueshield-hack-why-may-be-just-beginning-2091324>; Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, Wash. Post (July 9, 2015), <https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/>; Nicole Perlroth, *State Department Targeted by Hackers in 4th Agency Computer Breach*, N.Y. Times (Nov. 16, 2014), http://www.nytimes.com/2014/11/17/us/politics/state-department-targeted-by-hackers-in-4th-agency-computer-breach.html?_r=0; Ellen Nakashima, *Hackers Breach Some White House Computers*, Wash. Post (Oct. 28, 2014), https://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html.

⁷⁶ In May 2016, the NTIA released a report showing that large numbers of Americans were limiting their online activity in the face of growing concerns over privacy, security breaches, and data theft. See Goldberg, *Lack of Trust in Internet Privacy*, NTIA Blog. The business community also believes that consumer confidence in companies' data security practices is good for business and the economy. See *Data Privacy Is Good for Business*, Better Business Bureau, <https://www.bbb.org/council/for-businesses/toolkits/data-privacy-for-small-businesses/data-privacy-day-message-for-business/data-privacy-is-good-for-business/>; Nat'l Cyber Sec. Alliance, *National Cyber Security Alliance Reminds Organizations of All Sizes that "Privacy Is Good for Business,"* PR Newswire (Jan. 20, 2016), <http://www.prnewswire.com/news-releases/national-cyber-security-alliance-reminds-organizations-of-all-sizes-that-privacy-is-good-for-business-300206696.html>; David A Hoffman, *Privacy Is a Business Opportunity*, Harv. Business Rev. (Apr. 18, 2014), <https://hbr.org/2014/04/privacy-is-a-business-opportunity/>; see also NIST *Guide to Protecting PII*, at 2-1.

⁷⁷ See *supra* notes 38-39 and accompanying text; H.R. Rep. No. 104-458, at 205 (1996) ("[I]t is the duty of every telecommunications carrier to protect the confidentiality of proprietary information of and relating to other carriers, equipment manufacturers and customers.").

⁷⁸ *Nat'l Cable & Telecomm's Ass'n v. FCC*, 555 F.3d 996, 1002 (D.C. Cir. 2009).

B. Requiring customer opt-in for the majority of secondary uses of customer PI advances consumer privacy and does not overburden BIAS providers

1. Requiring opt-in for most secondary use of BIAS customer data advances consumer privacy

The Commission should require customer “opt-in” for most secondary uses of customer PI. This approach will mitigate the aforementioned privacy risks associated with BIAS data collection, and is the most appropriate consumer consent mechanism given BIAS providers’ highly detailed view of customers’ online activity. Consumer attitudes toward companies’ privacy practices and what type of consent should be required for use of their data are highly contextual.⁷⁹ Individuals 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.⁸⁰ In one study, respondents considered a doctor’s request for an individual’s Social Security number or health information to be appropriate to the doctor-patient relationship and the doctor’s business needs, but considered a search engine or library’s use of the same information to be out-of-context and inappropriate.⁸¹ By contrast, individuals expected some search engines and libraries to use political information when providing information services, but did not expect their doctor to consider this information.⁸² Consumers also expect entities may share their data with affiliated parties in order to provide certain services, but do not expect providers to share the same data with unaffiliated parties or use the data for purposes unrelated to the provision of services.⁸³ Consumers respond negatively to companies selling information to data brokers and

⁷⁹ For a discussion of the meaning of “context,” see generally Helen Nissenbaum, *Respecting Context to Respect Privacy: Why Meaning Matters*, *Sci. & Eng’g Ethics* (2015), <http://link.springer.com/article/10.1007/s11948-015-9674-9>. See also Pols, *Customer Expectations of Privacy vs. Consumer Empowerment*, LinkedIn Pulse.

⁸⁰ Kirsten E. Martin & Helen Nissenbaum, *Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables* 6 (forthcoming 2016), available at SSRN, <http://ssrn.com/abstract=2709584>; Katie Shilton & Kirsten E. Martin, *Mobile Privacy Expectations in Context*, in 41 Proceedings of the Research Conf. on Comm’n, Info. & Internet Policy 4 (Mar. 24, 2013), available at SSRN, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2238707 (testing hypothesis that “tactics such as behavioral advertising, data collection and retention, or tracking, may be appropriate and within the contextually-defined privacy norms in one context while inappropriate in another.”).

⁸¹ Martin & Nissenbaum, *Measuring Privacy* at 6 (concluding that “[t]he context of an information exchange – how the information is used and transmitted, the sender and receiver of the information – all impact the privacy expectations of individuals.”).

⁸² *Id.*

⁸³ See, e.g., Joseph Phelps, Glenn Nowak & Elizabeth Ferrell, *Privacy Concerns and Consumer Willingness to Provide Personal Information*, 19 *J. Pub. Pol’y & Marketing* 27, 28 (2000). Consumers support limits on third-party selling or sharing of personal or sensitive data when asked about specific industry practices. Chris Jay Hoofnagle & Jennifer King, *Consumer Information Sharing: Where the Sun Still Don’t Shine*, Berkeley Research Paper 6-7, (Dec. 17, 2007), available at <https://www.law.berkeley.edu/files/sb27report.pdf>. See, e.g., Elizabeth A. Bell, Lucila Ohno-Machado & M. Adela Grando, *Sharing My Health Data: A Survey of Data Sharing Preferences of Healthy Individuals*, AMIA Proceedings 2014, 1699-08 (2014) (finding majority of respondents felt comfortable participating in research if they were given choices about which portions of their medical data would be shared, and with whom those data would be shared); D.J. Willison et al., *Consent for Use of Personal Information for Health Research: Do People With Potentially Stigmatizing Health Conditions and the General Public Differ in Their Opinions?*, 10 *BMC Med. Ethics* 1 (July 2009) (finding individuals felt health information should not be used for marketing purposes, and that re-consent should be needed for sharing with for-profit research institutions); Consumer Fed. of California, *Poll: 91% Voter Support for Financial Privacy Initiative*, Privacy Rights Clearinghouse (Feb. 10, 2003), available at <http://www.privacyrights.org/ar/CFCsurvey.htm> (poll finding that a majority of Californians would support restrictions on financial companies’ sharing of financial information with third-party companies without their consent); Tena Friery, *North Dakota Votes for “Opt-In” Financial Privacy*, Privacy Rights Clearinghouse (June 21, 2002), https://www.privacyrights.org/ar/nd_optin.htm (reporting referendum results reversing statewide transition from opt-in to opt-out regime for banks selling their customers’ financial information to third parties).

other third parties⁸⁴ and express a strong preference for opt-in consent in such circumstances.⁸⁵ This is because these secondary uses are generally out of context and therefore do not meet customers' expectations when performed without their approval.

Likewise, the Commission should consider the contexts in which customer PI might be used when determining BIAS customer consent rules: customer opt-in should be required where secondary use or sharing is for an unrelated service (or not a "communications-related service") and/or with an unrelated entity (such as a joint venture partner or independent contractor). Data collection and tracking across unrelated services, and the business relationships underlying these programs, are much harder to identify and understand. BIAS customers who exceed their data caps likely would not expect to have to give permission to their providers to use customer PI to offer a larger data package because the BIAS provider is offering an upgrade to a service to which the customer already subscribes. The customer might expect to be offered an internet and cable "bundle" without opting in for these promotions since their BIAS provider likely offers cable services and it is typical to purchase these services in package deals.⁸⁶ However, it is much more difficult to argue that a BIAS customer would expect their provider to use their customer PI to offer them a smart refrigerator or share their PI with a third party to create targeted advertising profiles. While some practices, such as use of browsing data to market related services, have not garnered considerable press attention or public concern, other practices such as BIAS providers' use of uniquely identifying HTTP headers to track subscribers' movements online have instigated public outcry⁸⁷ and regulatory interventions.⁸⁸ Relatedly, BIAS providers' efforts to sell access to customer profiles based on customer PI have provoked strong criticism from privacy advocates.⁸⁹ Opt-in should be required in these cases because they are unrelated to the BIAS provider and its communications service, and therefore out of context.

Consumer behavior also calls for an opt-in approach for most secondary uses of customer PI. Research indicates that many consumers do not have the technical and legal literacy to understand privacy policies and disclaimers,⁹⁰ but without an understanding of these policies, an

⁸⁴ Shilton & Martin, *Mobile Privacy Expectations in Context*, at 9 (finding that "the secondary use of information was the most important factor in meeting privacy expectations. Selling to a data exchange . . . and using tracked information for social advertising to contacts and friends . . . both negatively impacted meeting privacy expectations.").

⁸⁵ In 2000, the Pew Internet & American Life Project found that 86% of Americans support opt-in consent before companies sell personal information. See Susannah Fox, *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*, Pew Research Ctr. (Aug. 20, 2000), available at <http://www.pewinternet.org/2000/08/20/trust-and-privacy-online/>.

⁸⁶ Such bundles make up large percentages of BIAS providers and their cable and voice affiliates' revenues. A Time Warner Cable executive recently noted that triple play customers generate half of the company's monthly residential revenues. Martha C. White, *No "Bundle" of Joy: Cost TV, Internet and Phone Service Rising*, NBCNews.com (Oct. 13, 2015), <http://www.nbcnews.com/business/consumer/no-bundle-joy-cost-tv-internet-phone-service-rising-n443646>.

⁸⁷ See, e.g., Dann Albright, *What Are Supercookies, and Why Are They Dangerous?*, Security Matters (Mar. 25, 2016), <http://www.makeuseof.com/tag/what-are-supercookies-and-why-are-they-dangerous/>; Alex Wawro, *How To Protect Yourself From Supercookies*, PC World (Aug. 26, 2011), http://www.pcworld.com/article/238895/how_to_protect_yourself_from_supercookies.html; Jose Pagliery, "Super Cookies" Track You, Even in Privacy Mode, CNN.com (Jan. 9, 2015), <http://money.cnn.com/2015/01/09/technology/security/super-cookies/>.

⁸⁸ Jon Brodtkin, *Verizon's "Supercookies" Violated Net Neutrality Transparency Rule*, Ars Technica (Mar. 7, 2016), <http://arstechnica.com/business/2016/03/verizons-supercookies-violated-net-neutrality-transparency-rule/>.

⁸⁹ Jack Marshall, *How Verizon Plans to Fix Mobile Advertising*, Wall St. J. (May 23, 2014), <http://blogs.wsj.com/cmo/2014/05/23/how-verizon-plans-to-fix-mobile-advertising/>.

⁹⁰ See Pedro G. Leon, Justin Cranshaw, Lorrie Faith Cranor, Jim Graves et al., *What Do Online Behavioral Advertising Disclosures Communicate to Users?*, CMU-CyLab-12-008 (2012), available at http://works.bepress.com/lorrie_cranor/26/; see

opt-out framework does not give consumers meaningful opportunity to assert their choice. Furthermore, reviewing ever-lengthening privacy policies can be a daunting task. The average consumer would need to spend between 181 and 304 hours each year reading web site privacy policies to be able to understand how their information is being used.⁹¹ Not only ordinary users have trouble controlling the distribution of their personal data;⁹² even informed consumers have difficulty exercising choice because they lack the same level of knowledge as the provider about exactly how their information may be used.⁹³ Opt-in is more likely than opt-out to put the consumer on notice that their data is being shared if a consumer does not read or understand a privacy policy. Studies also indicate that consumers expect privacy but tend to accept default settings, even in cases where the default setting conflicts with their privacy expectations.⁹⁴ In some cases, customers are unlikely to opt out, even if they would not have opted in in the first place.⁹⁵ These studies demonstrate that default privacy settings do not always correspond with consumer privacy expectations and therefore an opt-out setting is insufficient to give consumers meaningful control in all circumstances

Taken together, these findings illustrate the highly contextual nature of consumer choice as well as consumers' tendency to accept default settings and not read privacy policies. BIAS providers should therefore seek their customers' affirmative opt-in when sharing customer PI with unaffiliated third parties for marketing or when using customer PI to market non-communications-related services.⁹⁶ Below are examples of scenarios when BIAS customer opt-in should be required:

A BIAS provider inserts uniquely identifying HTTP headers into its customers' internet transmissions. The BIAS provider shares these uniquely identifying HTTP headers with third parties to target advertisements to the customer.

As discussed above, unique identifiers are both CPNI and PII and therefore fall within the scope of the BIAS rules. Customer opt-in should always be required when customer PI is shared with an unaffiliated third party — regardless of whether the marketed service is “communications-related.” In this case, an unaffiliated third party is using the BIAS providers' uniquely identifying

also Wendy Davis, *Study: Web Users Don't See AdChoices Icon*, MediaPost (Nov. 13, 2012),

<http://www.mediapost.com/publications/article/187164/study-web-users-dont-see-adchoices-icon.html>.

⁹¹ Aleecia McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 J. of L. & Pol'y for the Info. Society (I/S) 540, 560 (2008), authors' draft available at <http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>.

⁹² Pedro G. Leon et al., *Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising*, CMU-CyLab-11-017 (Oct. 31, 2011), https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11017.pdf.

⁹³ See generally Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 19 Wake Forest L. Rev. 261 (2014).

⁹⁴ See Eric J. Johnson, Steven Bellman & Gerald Lohse, *Defaults, Framing and Privacy: Why Opting In-Opting Out* 13 Marketing Lett. 5, 9 (2002), available at SSRN, <http://ssrn.com/abstract=1324778>.

⁹⁵ *Id.* Default selections have a major role in determining consumer preferences. Researchers have found that almost twice as many participants agreed to be contacted for future research when they were already opted into the research rather than when they had to affirmatively opt themselves in. See Eric J. Johnson & Daniel Goldstein, *Do Defaults Save Lives?*, 302 Science 1338 (2003); Eric J. Johnson & Daniel Goldstein, *Defaults and Donation Decisions*, 78 Transplantation 1713-16 (2004), http://www.dangoldstein.com/papers/JohnsonGoldstein_Defaults_Transplantation2004.pdf (finding that people tend to accept the default option chosen for them, regardless of their prior preferences, even in cases such as organ donation where the implications of each option are clear).

⁹⁶ See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6947 ¶ 39 (2007) (“2007 CPNI Order”); *Nat'l Cable & Telecomm's Ass'n*, 555 F.3d at 999.

HTTP headers to target advertisements to the customer. Therefore, customer opt-in must be obtained.

A BIAS provider offers internet service as well as a home security service. The security service comes in three packages: “Standard,” “Plus,” and “Premium.” The Premium package includes an additional feature that allows customers to adjust their home’s thermostat remotely. A customer has BIAS service as well as the Standard home security service. The BIAS provider uses its customer PI to determine that the customer has a smart thermostat in their home purchased through another company. The BIAS provider offers the customer the Premium security package at a discounted rate.

The BIAS provider has used customer PI to market an additional feature within its home security service to the customer. Although customer opt-out is acceptable for first-party and affiliate use of customer PI to market “communications-related services,”⁹⁷ the home security and thermostat service is not a communications-related service. Therefore, even though the customer already has the home security service, the BIAS provider arguably should have to obtain customer approval in the form of opt-in.⁹⁸

2. Requiring opt-in for the majority of secondary use of customer PI does not overburden BIAS providers

Requiring an opt-in approach would not significantly restrict BIAS providers’ use and sharing of customer PI. The Commission’s proposed framework would still allow BIAS providers to use customer PI for a range of marketing efforts — including those unrelated to the original service that the customer purchased — provided that the customer opts in to this use. BIAS providers could arguably still offer a monetary incentive to customers in exchange for their data as well.⁹⁹ 222 does not prohibit such marketing practices; on the contrary 222(c)(2) suggests carriers *must* share customer information if directed to do so by the customer.¹⁰⁰ However, “pay for privacy” schemes must not undermine the larger opt-in framework. Pay-for privacy raises public policy concerns that deserve the Commission’s special attention.¹⁰¹ The consumer consent rules would certainly be undermined if a customer is unaware that he or she is opting into a pay-for-privacy scheme or if service prices are inflated so that the customer is essentially forced to accept a

⁹⁷ We address the appropriate definition of “communications-related service” in section IV.C.

⁹⁸ Section 222 allows certain use of customer PI to market upgrades within services to which the customer has already subscribed. *See* 47 U.S.C § 222(c)(2). We will not address this aspect of the rules in the present comments. However, it should be noted in this example that the customer only subscribes to the *Standard* security service (not the *Premium* service) and therefore does not already receive the smart thermostat service from the BIAS provider. Thus, even if the rule were to apply, opt-in would still be appropriate.

⁹⁹ These are commonly known as “pay for privacy” schemes. *See Pay for Privacy Definition*, WhatIs.com, <http://whatis.techtarget.com/definition/pay-for-privacy> (last visited May 15, 2016).

¹⁰⁰ *See* 47 U.S.C § 222(c)(2) (“Disclosure on request by customers. A telecommunications carrier shall disclose customer proprietary network information, upon affirmative written request by the customer, to any person designated by the customer.”). The statutory language supports the conclusion that section (c)(2) was likely included to facilitate *customer-initiated* sharing of CPNI with third parties, as opposed to *carrier-initiated* efforts to encourage customers to share CPNI with third parties. *Id.* (requiring disclosure to any party requested by the customer). Section 222(c)(2) is limited to CPNI, moreover; § 222(a) does not have a similar requirement.

¹⁰¹ Sandra Fulton, *Pay-for-Privacy Schemes Put the Most Vulnerable Americans at Risk*, Free Press (May 10, 2016), <http://www.freepress.net/blog/2016/05/10/pay-privacy-schemes-put-most-vulnerable-americans-risk>; *see also* Open Tech. Inst., *The FCC’s Role in Protecting Online Privacy*, New Am. Found. 8 (Mar. 10, 2016), available at <https://www.newamerica.org/oti/press-releases/oti-applauds-fcc-action-on-broadband-privacy-rules/>.

discount in exchange for use of their customer PI.¹⁰² Consumers are not always willing to exchange their data, even for monetary rewards.¹⁰³ Moreover, lack of transparency around company data collection strategies is a recurring concern.¹⁰⁴ If the Commission's rules allow for pay-for-privacy programs, additional regulations must be put in place to ensure these programs do not diminish the general prohibition on secondary use of customer PI without opt-in.

According to Section 201, it is the duty of the Commission to ensure all carrier practices are "just and reasonable."¹⁰⁵ The Commission should draw upon this authority to put rules in place that will restrict pay-for-privacy programs if a BIAS provider is not transparent about the program or inflates service prices to essentially coerce the customer into accepting a discount in exchange for opting in to data sharing. Inducements to consent, such as service discounts, should *only* be allowed if a BIAS provider:

- (1) Makes it easy for the customer to decide whether or not they opt in to the program;
- (2) Makes it easy for the customer to opt out of the program;
- (3) Commits to disclosing to the Commission the ZIP +4 for all customers who have opted in to the program;
- (4) Complies with all notice requirements outlined in Section 64.7001 of the proposed rules¹⁰⁶; and
- (5) Commits to not designing programs that are unconscionable or coercive.

These requirements would reduce public policy concerns associated with pay-for-privacy programs, while also giving BIAS providers flexibility to offer incentives for individuals to share their customer PI for marketing.

¹⁰² See Harold Feld et al., *Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World* 64, Public Knowledge (February 2016), available at <https://www.publicknowledge.org/assets/uploads/blog/article-cpni-whitepaper.pdf> ("Protecting Privacy, Promoting Competition").

¹⁰³ This is especially so when they consider the data to be sensitive data such as IoT devices. See Rainie & Duggan, *Privacy and Information Sharing*, Pew Research Ctr. (reporting that, for example, 55% of U.S. adult respondents felt it would be unacceptable for a "smart thermostat" to monitor their movements around the home in exchange for a discount on their energy bill, and that 45% found it unacceptable for car insurance companies to monitor their driving location and speed in exchange for discounts on their premiums).

¹⁰⁴ 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, 1854 (2011) (noting that "the lack of transparency regarding practices of data collection and tracking creates an asymmetry of knowledge about existing information collection practices between consumers and the organizations that collect information about them," an information asymmetry that "places consumers at a profound disadvantage in negotiations, such as they may exist, with those who collect their information.").

¹⁰⁵ 47 U.S.C. § 201(b).

¹⁰⁶ *NPRM*, app. A.

C. Requiring customer opt-in for the majority of secondary uses of customer PI is appropriately scoped; opt-out would still be permissible for first-party and affiliate marketing of “communications-related services”

1. A sharply-crafted definition of “communications-related services” would protect consumer privacy

CDT supports allowing customer opt-out for first-party and affiliate use of customer PI to market “communications-related services.”¹⁰⁷ This would allow BIAS providers to employ creative marketing techniques for services which the customer already purchased and related services. More importantly, this approach would maintain consumers’ privacy.¹⁰⁸ An appropriately scoped definition of “communications-related services” will help ensure this outcome.

“Communications-related services” must be narrowly defined and limited to services already subject to privacy protection under the Communications Act. CDT supports the Commission limiting what is considered “communications-related” to voice, internet and cable services. This support is based on two justifications offered by the Commission in its 2007 rulemaking for requiring customer opt-in for sharing CPNI with joint venture partners and independent contractors: (1) the carrier no longer has control over the customer’s protected information once it is shared with a joint venture partner or independent contractor; and (2) the privacy protections outlined in section 222 may not extend to joint venture partners or independent contractors themselves in all cases.¹⁰⁹ We agree that these factors heighten the risk of loss of customer data and therefore urge the Commission to adopt a similar position in the present proceeding. This standard should still allow for cable to be included in the definition of “communications-related,” even though it is not a Title II service. This is because the risks outlined above are arguably low: a BIAS provider is likely to maintain control over customer PI once shared for cable service marketing, and cable providers are subject to privacy standards outlined in the Communications Act.

The majority of leading BIAS providers are also key providers in the cable service industry.¹¹⁰ This means consumers are most likely to receive their internet and cable service from the same provider and, in turn, share their PI with the same provider. Thus, if a BIAS provider shares customer PI to market cable services, this information would almost certainly remain in the BIAS provider’s control and the risk of data loss would not be significantly heightened. Even if the cable entity were not controlled by the BIAS provider, the risk of loss would not be similar to that of the joint venture partners and independent contractors addressed in the Commission’s 2007 order. Cable services, while not Title II services, are regulated under the Communications Act and therefore under the Commission’s enforcement jurisdiction.¹¹¹ Cable services are subject to highly restrictive privacy protections under section 631 of the Act.¹¹² These entities will therefore remain subject to certain privacy requirements when accessing BIAS customer PI.

¹⁰⁷ *NPRM*, at 2538 ¶ 107.

¹⁰⁸ See section IV.A, above.

¹⁰⁹ 2007 CPNI Order, at 6947 ¶ 39.

¹¹⁰ See Protalinski, *Over 70% of US Households Now Have Broadband Internet Access, with Cable Powering Over 50% of the Market*; Feld et al., *Protecting Privacy, Promoting Competition*, at 22.

¹¹¹ Cable Comm’s Policy Act of 1984 § 631, 47 U.S.C. § 551.

¹¹² Feld et al., *Protecting Privacy, Promoting Competition*, at 21.

Considering cable a “communications-related service” would not detract from the Commission’s efforts to protect consumer privacy.

2. A sharply-crafted definition of “communications-related services” would still allow for reasonable secondary use of customer PI for marketing

In addition to maintaining consumer privacy, this approach would still afford BIAS providers and their affiliates considerable latitude to use customer PI to market their other commonly-offered services to customers. BIAS providers would be able to use customer information to market cable and/or voice services on a customer opt-out basis. Given that these services are often owned and operated by the same entities, the rules would not significantly disrupt existing advertising structures. The regulations would certainly still allow for double- and triple-play bundles to be marketed on a customer opt-out basis.¹¹³ For example, the rules would allow for customer opt-out in the following scenarios:

A BIAS provider offers both broadband internet and home phone services. An existing customer only purchases internet service. The BIAS provider notices that the customer has been visiting voice providers’ websites. The BIAS provider uses this information to offer the customer a double-play internet and home phone package for two years at a discounted rate.

This appears to be a fairly standard secondary use of customer PI that would comply with both existing CPNI rules and the Commission’s proposed customer PI rules for broadband. In this case the BIAS provider is marketing a service to which the existing customer is not already subscribed. Therefore, the BIAS provider must obtain customer approval. However, since the marketed service (voice services) is a “communications-related service” customer opt-out is sufficient.

A customer subscribes to internet and cable from a BIAS provider. The provider notices that although the customer frequently visits ESPN.go.com they have not purchased a cable package with ESPN. The BIAS provider offers the customer an upgrade on their existing cable package to include free ESPN for a year.

In this case, the BIAS provider has used customer PI to determine that a customer may be interested in a particular cable service. Although the cable service is not a category of service that falls within Title II, cable is subject to privacy protections under Title VI of the Communications Act. Therefore, it should be considered a “communications-related service” and opt-out is appropriate.

V. Conclusion

For the foregoing reasons we respectfully request the following proposals be implemented in the Commission’s rules: (1) include PII in the definition of customer PI and

¹¹³ Such bundles make up large percentages of BIAS providers and their cable and phone affiliates’ revenues. A Time Warner Cable executive recently noted that triple play customers generate half of the company’s monthly residential revenues. White, *No “Bundle” of Joy*, NBCNews.com.

broadly define “PII”; (2) consider packet metadata CPNI; (3) require customer opt-in for all non-affiliate third-party use of customer PI for marketing and for first-party and affiliate use of customer PI to market services that are not “communications-related;” (4) allow opt-out for first party and affiliate use of customer PI to market “communications-related services;” and (5) limit what is considered “communications-related services” to services subject to privacy protection under the Communications Act—particularly voice, internet and cable. These proposals, if adopted, would significantly advance consumer privacy online.

Appendix

Applying Communications Act Consumer Privacy Protections to Broadband Providers

Applying Communications Act Consumer Privacy Protections to Broadband Providers

What is this diagram all about?

With the reclassification of broadband internet access service (BIAS) as a telecommunications service, BIAS providers became subject to the privacy protections of Title II's Section 222. Section 222(c) limits use of customer proprietary network information (CPNI), defined as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship." The FCC will need to interpret how this definition applies to BIAS. One approach would be anchoring the application of CPNI to broadband in the individual components of Internet traffic, known as "packets." Since all Internet traffic is made of packets, a definition of CPNI based on the technical aspects of packets can apply to all transmissions across the Internet.

The accompanying diagram discusses privacy implications of different components of IP packets. Before turning to it, we must answer a few questions:

What is a packet, anyway?

All Internet traffic is divided into packets. Some transmissions fit into a single packet, while longer transmissions are sent in a series of packets. These packets may take different routes through the networks, and may not arrive in the correct order, but the receiving computer can reassemble them if it understands how they are labeled. That's why networked computers rely on protocols.

What are protocols?

When computers sort, send, receive and reassemble packets, they do so according to standardized protocols. These protocols consistently organize the content and routing information so that computers on each end of the communication can understand the meaning of the bytes within the packets' headers (explained below).

What are layers?

Layers are a feature of "network models" of the Internet. The TCP/IP network model is an abstract construct that represents each aspect of an Internet data exchange as a layer. The bottom layer is the actual physical media over which the message will travel, such as copper wire or optical fiber. Above that is the link layer, which describes how the message will be sent across the physical layer. Ethernet and WiFi are protocols that operate at this layer. Above the link layer is the internet layer, which consists of protocols describing how packets will be exchanged across networks. The most common protocol operating here is the Internet Protocol (IP). Above the internet layer is the transport layer, consisting primarily of two protocols: TCP and UDP. This layer determines whether the receiver of a packet needs to send receipt confirmation to the sender and to which part of your operating system the message should be routed. At the top of the stack is the application layer, which contains the actual content of the message such as the file to be read or instructions to perform a task. There are

many application protocols, but one of the most common is the Hypertext Transfer Protocol (HTTP) used to connect users to websites.

What are headers?

Headers are sort of like the shipping information on your snail mail. As your computer sorts information into packets, it wraps the original information with headers. Like information written on a letter's envelope, each of these headers contains data about the data you are sending (metadata) like the size and number of packets in a transmission, where the packet came from and should go, and in what order to open the packets. Just like a mail carrier needs to know your letter's destination, routers within networks across which packets may travel must inspect parts of the packet metadata to correctly forward the packets to their destination. However, neither mail couriers nor ISPs need to know the contents of the letters or packets they transport. When network operators look beyond the packet metadata and into the application data, it is often referred to as "deep packet inspection."

So, what does packet metadata have to do with privacy?

Long-term monitoring of packet headers traveling to and from IP and MAC addresses can reveal patterns and associations that paint a picture of what kinds of information customers are sending and receiving over the Internet, and when, where, and how they do so. For instance, by looking at packet size, packet streams, and IP addresses, a network operator could infer that you are streaming a movie from a particular content provider. A network operator could begin to develop a comprehensive profile of your broadband usage patterns, or even your personal habits, like when you sleep, work, watch movies and send email.

But, what about encryption?

Encryption can enhance privacy, but it is not a panacea. Most encryption occurs at the application layer, meaning the content of a transmission may not be visible to a network operator, but the packet headers are not obscured. If these headers reveal private information, most encryption will not cover it.

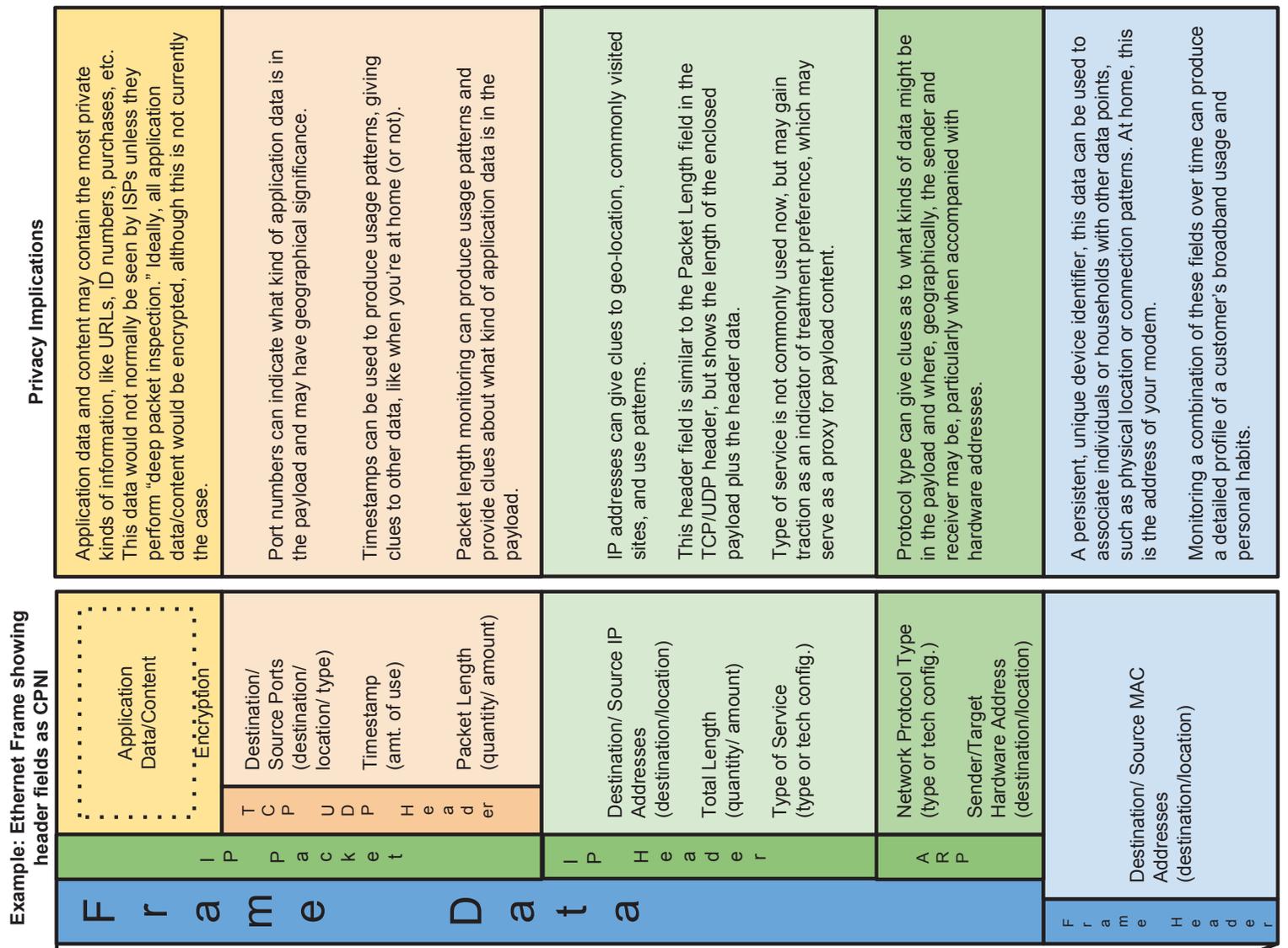
Where does that leave us?

Interpreting the definition of CPNI to include packet metadata would not prevent broadband providers from monitoring or collecting header information, but it could limit their ability to market or disclose that information to third parties without customer consent. Some application data may also be considered CPNI, such as the parts of a URL that follow the domain name in your browser's address bar, because this provides even more detailed network location information than the IP header.

The accompanying diagram shows a simplified version of the TCP/IP model on the left, with examples of protocols used at each layer. As a packet of application data moves down through the stack, various components of the application or content provider's computers and network connection hardware add headers to the packet, which then leaves the application provider's server and travels across the

Internet to arrive at your modem. The packet then travels back up the stack, where your network connection hardware remove the headers and deliver the packet payload to your application software.

The right side of the diagram shows an expanded abstract of an Ethernet frame, made up of the application payload and the protocol headers attached to it. The relevant header fields that might be considered CPNI are listed within the packet headers, accompanied by the relevant term from the definition in parentheses. To the right of the expanded packet diagram are descriptions of the potential privacy implications associated with the monitoring and collection of header information.



Privacy Implications

Application data and content may contain the most private kinds of information, like URLs, ID numbers, purchases, etc. This data would not normally be seen by ISPs unless they perform "deep packet inspection." Ideally, all application data/content would be encrypted, although this is not currently the case.

Port numbers can indicate what kind of application data is in the payload and may have geographical significance.

Timestamps can be used to produce usage patterns, giving clues to other data, like when you're at home (or not).

Packet length monitoring can produce usage patterns and provide clues about what kind of application data is in the payload.

IP addresses can give clues to geo-location, commonly visited sites, and use patterns.

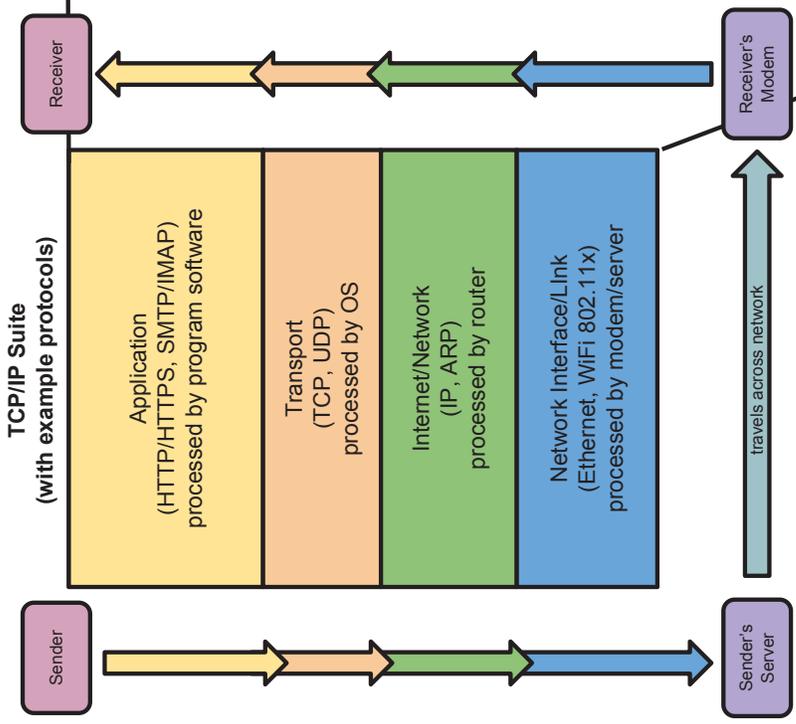
This header field is similar to the Packet Length field in the TCP/UDP header, but shows the length of the enclosed payload plus the header data.

Type of service is not commonly used now, but may gain traction as an indicator of treatment preference, which may serve as a proxy for payload content.

Protocol type can give clues as to what kinds of data might be in the payload and where, geographically, the sender and receiver may be, particularly when accompanied with hardware addresses.

A persistent, unique device identifier, this data can be used to associate individuals or households with other data points, such as physical location or connection patterns. At home, this is the address of your modem.

Monitoring a combination of these fields over time can produce a detailed profile of a customer's broadband usage and personal habits.



Customer Proprietary Network Information means 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