Before the
Federal Communications Commission
Washington, DC 20554

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

Comments of The Electronic Frontier Foundation

May 27, 2016

The Electronic Frontier Foundation (EFF) appreciates the Federal Communications Commission's (FCC) efforts to protect the privacy and security interests of users and customers of broadband Internet access service (BIAS) providers. EFF is a member-supported, nonprofit, public interest organization promoting individual rights and empowering innovation in the digital world. Founded in 1990, EFF represents tens of thousands of dues-paying members, including consumers, hobbyists, artists, computer programmers, entrepreneurs, students, teachers, and researchers. EFF has for years contributed its expertise in law, regulation, and technology to representing consumers on the issues of innovation, competition[1] and privacy.[2]

We submit these comments largely in support of the Commission's proposals, but we also have specific disagreements with some of the Commission's reasoning.

1. The Commission has the Statutory Authority Under Both Section 222 and Section 705 to Protect Consumer Privacy.

Telecommunications carriers are in the unique position of being the only means of access to critical online services in health, finances, housing, employment, communications, and other deeply intimate matters. No edge provider enjoys the ability to see everything a consumer does online. The technology now available for telecommunications providers allows for the possibility that every communication, activity, and movement can be tracked in real or near-real time.[3]

Congress enacted Section 222 following a tradition of sector-specific privacy regimes to address unique problems. Telecommunications as a telephone service posed all of the same privacy risks to consumers that modern day broadband communications does, as voice communications of sensitive information simply become digital transmissions. The Commission

[1] *See* Derek Slater, *Another Step Towards Cable Set-Top Competition*, EFF Deeplinks Blog (Jan. 11, 2007),
[2] *See* Lee Tien & Parker Higgins, *Initial Comments on Privacy and Security of Information Stored on Mobile Communications Devices*, FEDERAL COMMUNICATIONS COMMISSION (July 13, 2012), https://www.eff.org/files/eff_fcc_mobile_privacy_comments.pdf.
[3] Harold Feld et al., Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World at 48-49.

is now at a critical point to determine telecommunications providers' statutory obligations under Section 222 to protect consumer privacy.

The FCC has independent statutory authority from Section 222(a) to interpret what falls within the general duty of telecommunications carriers to protect customer data.

> *Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.*[4]

A plain reading of Section 222(a) states unambiguously "every telecommunications carrier has a duty to protect the confidentiality of, and relating to…customers."[5] Subsequent provisions in Section 222 do not limit the carrier's general duty to protect consumer privacy, but rather address specific obligations and exceptions in addition to that general duty to protect confidential customer information. In no other part of Section 222 is a carrier's "general duty" or "duty" referenced or limited by express statutory text. The statute expressly defines the limitations that do exist. Accordingly, the rules and regulations that enforce Section 222 can be robust so long as the rules are a reasonable interpretation of ambiguous terms in the statutory text.[6]

We further agree with the FCC that the general duty of a telecommunications carrier extends beyond just CPNI[7] and applies to all information that includes PII as well (collectively referred to as customer PI[8]).

The FCC has additional authority to enact rules that ensure that any divulgence or publication of private consumer information does not violate a telecommunications carriers' "general duty to protect" customer PI[9]; Section 705 of the Communications Act[10] provides the FCC with authority to address the practice of intercepting communications for purposes other than transmission to the intended recipient. Prior to the enactment of the Wiretap Act,[11] only Section 705 of the Communications Act regulated wiretapping at the federal level. The statute clearly prohibits communications personnel from divulging or publishing any information they received or transmitted (or assisted in receiving or transmitting) from "any interstate or foreign communication by wire or radio" to anyone except authorized persons.[12] Federal courts in the years that followed the enactment of Section 705 regularly barred the introduction of evidence acquired from a wiretap in criminal prosecutions.[13]

---

[4] 47 U.S.C. § 222(a).
[5] *Id*.
[6] Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc., 467 U.S. 837 (1984).
[7] FEDERAL COMMUNICATIONS COMMISSION, Notice of Proposed Rulemaking on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services at ¶ 57. [hereinafter NPRM]
[8] NPRM ¶ 57-59
[9] *Id*.
[10] 47 U.S.C. § 605.
[11] 18 U.S.C. §§ 2510-2522.
[12] 47 U.S.C. § 605(a).
[13] *See* Nardone v U.S., 302 U.S. 379 (1939); *See also* Benanti *v. U.S.*, 355 U.S. 96, 78 (1957); *See also* Weiss v. U.S., 308 U.S. 321 (1939).

Given its early historical interpretation, Section 705 serves as a broad prohibition against the divulgence or publication of a communication's "existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception."[14] Should the FCC adopt a strong Section 222 general duty framework for telecommunications providers that curtails data collection practices to only activities necessary to provide telecommunications service, Section 705's broad prohibition against divulgence or publication would serve as a clear statutory bar against carriers from selling consumer data for purposes outside the scope of providing telecommunications services. This would prevent telecommunications carriers from bypassing Section 705 by gaining authorization through customer consent and undermining the entire purpose of Section 222's privacy regime.

2. What Data Should be Protected and How it Should be Defined.

Any analysis of broadband privacy must begin with a clear understanding of what data is subject to privacy protections in the first place. EFF generally agrees with the Commission's definitions: the general duty of a telecommunications carrier extends beyond just CPNI[15] and applies to all information that includes PII as well (collectively referred to as customer PI[16]). More specific responses to the Commission's questions follow.

The statutory definition of CPNI in § 222(h)(1) is determinative, and EFF agrees with the broad approach adopted by the Commission in the *2013 CPNI Declaratory Ruling*.[17] That approach was consistent not only with the statutory language but also with its intent to protect consumer privacy. The raw power of BIAS providers to append CPNI to a customer's Internet traffic—something that is not easily detectable by the customer—has already proven to be detrimental to customer privacy in the case of Verizon's UIDH injection.[18] We therefore agree with the Commission's proposal to interpret such information as CPNI whenever it meets the statutory criteria of § 222(h)(1).

The Commission should provide illustrative examples of broadband CPNI, rather than a comprehensive list.[19] Such a list would likely need frequent updating given the rapid pace of technical change. Illustrative examples, however, will provide useful guidance for providers and reduce compliance costs without risking obsolescence.

For instance, the categories of geo-location information, device identifiers, IP addresses, IP headers, and domain name information are all rightly considered to be CPNI in the BIAS context.[20] These types of information are commonly used to identify individuals in criminal

---

[14] 47 U.S.C. § 605(a).
[15] NPRM ¶ 57
[16] NPRM ¶ 57-59
[17] Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Declaratory Ruling, 28 FCC Rcd 9609, 9618, ¶ 27 (2013).
[18] Jacob Hoffman-Andrews, *Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls*, EFF Deeplinks Blog (Nov. 3, 2014), https://www.eff.org/deeplinks/2014/11/verizon-x-uidh.
[19] NPRM, ¶ 40.
[20] NPRM, ¶ 43-46.

investigations or target users for advertising purposes, both offline and online.[21] As such, they clearly implicate customers' privacy interests, and should be protected.

Location information is most obviously CPNI because § 222 specifically protects location information, and it has been clear since the Supreme Court's decision in *United States v. Jones* that there is a reasonable expectation of privacy in one's location, even in a public space, when the government collects such information over a period of time.[22] Research has also shown that the amount of location information needed to identify a person in modern society is counter-intuitively small.[23] It thus makes perfect sense to treat location information as CPNI, whether based on signal triangulation or IP address.

The category of traffic statistics should be CPNI for similar reasons. The Commission correctly recognizes that traffic statistics are analogous to call detail records in that they contain enormous amounts of information about a customer's broadband activities as well as patterns that reveal customer location.[24] Obviously, the revelation that the government had been indiscriminately collecting call detail records in bulk under the NSA's so-called "Section 215" program has educated the world about the privacy risks of disclosing a person's calling history.[25] BIAS providers can glean at least as much information about a customer's beliefs and preferences—and likely future activities—from Web browsing history or Internet usage history,[26] especially if combined with port information, application headers, and related information about a customer's usage or devices (CPE).[27]

As already noted, we agree with the Commission's proposal to cover both CPNI and PII as customer proprietary information or "customer PI" under the reasoning of the *TerraCom NAL*.[28] We note that much information can be sensitive for both economic and privacy reasons; health or medical information is quintessentially considered private in our society, partly because it can affect employer hiring or retention decisions crucial to a person's livelihood, but it is now

---

[21] Simon Hill, *How Much do Online Advertisers Really Know About You? We Asked an Expert*, Digital Trends (Jun. 27, 2015), *available at* http://www.digitaltrends.com/computing/how-do-advertisers-track-you-online-we-found-out.

[22] *United States v. Jones*, 132 S.Ct. 945 (2012). Justice Sotomayor noted in her concurrence that even short term monitoring implicates the reasonable expectation of privacy when it generates a "precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." Id. At 955.

[23] In regards to wireless BIAS providers, a single smartphone transmission to a cell tower for purposes of providing a telecommunications service reveals the surrounding geography of the user and can be used to infer user activity. This happens even if location information and location tracking applications were deactivated. *See* OPEN TECHNOLOGY INSTITUTE, *The FCC's Role in Protecting Online Privacy,* (Jan. 2016) at 5, https://static.newamerica.org/attachments/12325-the-fccs-role-in-protecting-online-privacy/CPNI__web.d4fbdb12e83f4adc89f37ebffa3e6075.pdf.

[24] NPRM, ¶ 47 ("when the customer is at home, at work, or elsewhere.").

[25] A study demonstrated that phone metadata alone allowed for researchers to infer medical conditions, firearm ownership, and more. *See* Jonathan Mayer & Patrick Mutchler, MetaPhone: The Sensitivity of Telephone Metadata (Mar. 12, 2014), http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata.

[26] BIAS providers who also offer calling services, especially mobile telephony, would have both sets of data at their disposal.

[27] As the Supreme Court noted in its *Riley* decision, smartphones are both the repository of sensitive personal data as well as an access point to private records stored in other locations; *See Riley v. California*, 573 134 S. Ct. 2473, 2489-91 (2014).

[28] *See* NPRM, ¶ 57 and FN 88.

well established that individuals can be targeted for advertising purposes or even by those seeking to exploit the mentally ill.[29]

We generally also agree with the Commission's approach to the definition of "personally identifiable information,"[30] under which illustrative examples of PII would be provided for guidance purposes. In particular, we agree that the Commission must use the concept of "linked or linkable" given the omnipresent and increasingly sophisticated threat of re-identification. The Digital Advertising Alliance's self-regulatory multi-site principles for online behavioral advertising appear consistent with this approach in declaring that "[d]ata has been de-identified when an entity has taken reasonable steps to ensure that the data cannot reasonably be re-associated or connected to an individual or connected to or be associated with a particular computer or device."[31]

The Commission may and should protect the content of communications[32] even though other laws do so. The content of communications is clearly "proprietary" under the logic of *TerraCom NAL*—one need only think of the growth of electronic commerce (including the transmission of credit card numbers and other financial information) to realize that such communications implicate a customer's economic and privacy interests and belongs within the scope of § 222(a). And consistent with the Commission's belief that providers should never use or share such content without express, affirmative consent, consumer privacy interests will be better protected if the Commission establishes a rule requiring exactly that. The need for an explicit consent rule arises because both the Wiretap Act and the Stored Communications Act contain underspecified "consent" exceptions. Both statutes merely require "lawful consent" by a party to the communication without further elaboration;[33] the text does not specify whether consent must be affirmative, and consent provisions could be buried in privacy policies or terms of service. We therefore endorse a rule that would clearly cover communications content as customer proprietary information and impose a standard of affirmative or opt-in approval to the use or sharing of content, presented to the customer with sufficient notice for informed consent.

If the Commission protects communications content as we suggest and protects CPNI and PII as proposed, it would be unnecessary to treat certain types of information, such as health or medical information, as sensitive and entitled to special protection. Protecting this broad array of CPNI, PII and communications content (in combination) should adequately protect a customer's history of browsing websites about reproductive health concerns, of communicating with medical providers and health insurers, and so on. Conversely, defining categories of "sensitive" information may create a perverse incentive for BIAS providers to identify or inspect protected data in order to determine whether it falls into a "sensitive" category. Protecting the categories we have described without regard to content makes it unnecessary to know the content. Finally,

---

[29] Before the Subcommittee on Communications, Technology, and the Internet, and the Subcommittee on Commerce, Trade, and Consumer Protection of the House Committee on Energy and Commerce, 111th Cong. (2009)(statement of Pam Dixon, Executive Director of World Privacy Forum), *available at* http://www.worldprivacyforum.org/wp-content/uploads/2009/11/TestimonyofPamDixonfs.pdf.

[30] NPRM, ¶ 62.

[31] Digital Advertising Alliance, Self-Regulatory Principles for Multi-Site Data, *available at* https://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf

[32] NPRM, ¶ 67.

[33] E.g., 18 U.S.C. § 2511(3)(b)(ii); 18 U.S.C. § 2702(b)(3).

given the power of data analysis to make inferences about highly sensitive conditions (such as pregnancy[34]) from seemingly irrelevant data, it is difficult to imagine usable definitions of sensitive categories. For instance, if medical information were sensitive, location information that shows that a person visited a doctor's office or browsing data indicating that a person looked up the address of Planned Parenthood would be sensitive.

We agree with the definitions of opt-out and opt-in approval set forth at ¶ 68-69; we disagree with the proposal to eliminate the 30-day waiting period. Even if customers are able to "opt out at any time and with minimal effort," this does not address the reality that customers do not, or are often unable to, understand what the provider is doing in the first place or what it means for privacy and security. In today's world of complex privacy threats, it is unwise and unrealistic to assume that customer education about privacy only occurs "inside" the relationship between provider and customer. Watchdog agencies, popular media, technology publications and blogs frequently and usefully "translate" company announcements into terms that vulnerable citizens from various backgrounds can understand.

Relatedly, "communications-related services" should be narrowly defined to avoid expanding the range of opt-out approval. The definition should be limited to "telecommunications services and services related to the provision or maintenance of customer premises equipment,"[35] thus requiring opt-in approval for "information services typically provided by telecommunications carriers."

Finally, the rules for CMRS providers need to be revised. Current rules allow a wireless provider to "use, disclose, or permit access to CPNI derived from its provision of CMRS, without customer approval, for the provision of CPE and information service(s)."[36] But an ordinary BIAS provider would need to seek opt-out approval with respect to provision of CPE, and it makes no sense to have different rules. We also agree that the entire category of "information service" should be removed from the rule, consistent with our position on "communications-related services" described above.

3. Data Minimization and Retention

The Commission correctly recognizes that the more customer information that BIAS providers collect and retain, the more they must do to secure that information. Collection and retention of customer information also implicates customer privacy. As noted earlier, the providers' general duty under § 222 to protect customer PI can easily be understood as including duties to not take certain actions—such as not collecting or not retaining information that if exposed or shared would harm the privacy and security interests of the customer.

We also urge the Commission to require BIAS providers to set reasonable retention limits for customer PI. Rules for BIAS providers should be consistent with the framework of the Cable and Satellite Acts, under which entities must destroy personal data if the information is no longer

[34] Charles Duhigg, *How Companies Learn Your Secrets*, NY TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=1&hp=&pagewanted=all.
[35] We agree that "premises of a person" should include the person as well as a residence or place.
[36] NPRM, ¶ 81, FN 144.

necessary for the purpose for which it was initially collected.[37] It may be unnecessary to set specific time limits in all cases, but certain common situations, such as when a customer ends its relationship with the provider, or when a prospective customer does not become a customer, call for a specific short period. Such customers should not be required to deal with a former provider or an entity that never provided services in the first place.

We also recommend that if the Commission uses a flexible standard for time limits in most cases, that attention be paid to BIAS providers' actual retention practices. BIAS providers could be required to report to the Commission and publish their retention policies, while the Commission could audit providers to ensure that their practices meet the standard set forth in their retention policies.

Retention limits should not turn on the category of data, however, if the category is content-based, for the same reasons that we reject using content-based "sensitive" information categories. It may be appropriate to establish a different standard for de-identified data, because properly de-identified data poses less of a security and privacy risk. But differential treatment based on the de-identified status of data is a complex issue because the risks of re-identification are difficult to assess and are known to increase over time as more data about individuals becomes available or as new re-identification techniques are developed.

The Commission should not attempt to "ensure any retention periods are sufficiently flexible to accommodate requests from law enforcement or legitimate business purposes."[38] Quite frankly, it seems impossible to accommodate law enforcement requests while still protecting customers' interests in the privacy and security of their PI. It is our understanding that when the Commission sought to reduce compliance burdens on providers by eliminating the 18-month retention requirement, the FBI was the main reason that it remained. The Commission's 18-month toll billing record retention requirement probably contributed to the creation of programs aimed at exploiting the wealth of call detail records, such as the Hemisphere program[39] and the Section 215 program, and we see no reason to repeat that mistake. A flexible standard should be sufficient to meet legitimate business purposes with no further accommodation. We doubt that retention of customer PI can produce benefits that outweigh the risks of over-retention. Do any new consumer products or services exist today because of the Commission's 18-month toll billing record retention requirement?

Finally, the Commission should follow the data destruction model laid out by the Fair and Accurate Credit Transactions Act[40] and its implementing regulations, which include a non-exhaustive list of "reasonable measures" for destroying or erasing media such that the data cannot be practicably read or reconstructed.[41] The crucial point is that BIAS providers have a duty to secure customer PI, and must be held accountable if and when they fail.

---

[37] NPRM, ¶ 226-227; *See also* 47 U.S.C. § 551(e), 338(i)(6).
[38] NPRM, § 228.
[39] See, e.g., Mike Levine, *DEA Program Puts Phone Company Inside Government Offices*, ABC World News (Sep. 1, 2013), http://abcnews.go.com/blogs/headlines/2013/09/dea-program-puts-phone-company-inside-government-offices.
[40] 15 U.S.C. § 1681(w).
[41] NPRM, ¶ 231.

4. EFF Disagrees with the Commission's Proposed Consent Framework.

The Commission's proposed consent framework creates three tiers of consent for use and sharing of customer PI: no approval needed ("implied approval")[42]; opt-out consent; and opt-in consent.

First and most important, EFF questions the "implied approval" category. § 222 is intended to protect customers' proprietary information, which the Commission correctly interprets broadly. We are disturbed that the Commission proposes to eliminate all customer control over PII for a large range of activities, including marketing, and we fail to see how this is consistent with the statute, which imposes a general duty on providers to protect customer privacy and confidentiality. Section 222(c)(1) only refers to the authorization of use of CPNI by law or consent,[43] i.e., by requiring "the approval of the customer." But this concept of "implied approval" simply treats "no approval" as "approval." The "approval" language of § 222 cannot bear that much stress.

We also disagree with the Commission's proposal to interpret the statutory exception in §§ 222(c) and (d) to include "any customer PI, and not only CPNI."[44] The exceptions themselves refer to CPNI, and the Commission expressly states that CPNI is in a different category than PII.[45] Given the customer's interest in the sanctity of customer PI, and the broad range of data that the Commission proposes to treat as CPNI in the BIAS context, we see no reason to expand the exception beyond CPNI. Such a duty cannot be waived by customer consent in regards to PII, because the statute only authorizes consent waivers for CPNI.

Moreover, such expansion would have serious effects on customer privacy as well as undermine trust in the Commission's privacy rules. The Commission itself has noted that geo-location information is "particularly sensitive," and asks whether opt-in approval should be required.[46] Yet geo-location information would be CPNI under the Commission's proposal,[47] and available under the "implied approval" rubric.

Similarly, were the Commission to include "content" within the category of customer PI, the proposal would seem to permit content disclosure without customer approval. Content should not be disclosed without customer approval; laws like the Stored Communications Act make this clear. This specific proposal to expand disclosure of "any customer PI" appears to be utterly incoherent and inconsistent with Congress's intent to protect customers. We also believe that even when customer approval is "implied," customers should receive clear notice unless prohibited by statute.[48]

---

[42] NPRM, ¶ 112.
[43] 47 U.S.C. § 222(c)
[44] NPRM, ¶ 113; *See also* ¶ 114 (marketing of additional BIAS offerings in the same category of service that the customer already subscribes to); ¶ 115 (statutory exceptions under § 222(d)); ¶ 120.
[45] NPRM, ¶ 57.
[46] NPRM, ¶ 136.
[47] NPRM, ¶ 41.
[48] *E.g.*, § 222(d)(1) specifies disclosure shall not require customer notice.

The disclosure of call location information for public safety falls into a somewhat different category. We recognize that emergency situations may require somewhat laxer treatment of location data than we would otherwise deem necessary. But nothing in the record to date suggests that more than location is needed, and we see no basis for suddenly allowing "any" customer PI to be disclosed for emergency services.[49] Nor do we believe that the Commission can fairly interpret "call location information" in § 222(d)(4) to include "broadband usage location information" outside of the VoIP context. For instance, the pen register/trap and trace statute was amended in order to cover Internet activity. We also urge the Commission to require some after-the-fact accountability for emergency disclosures to ensure that location data not migrate out of the hands of statutorily specified recipients.

We agree with the proposal to permit disclosure of CPNI for cybersecurity purposes.[50] Such disclosure, however, should be limited to CPNI, and all such disclosures should be as de-identified as possible; also, such disclosures should only be permitted under § 222 when made to private entities, and not to any governmental entity.

We are more supportive of the Commission's proposal for disclosures that require customer approval.[51] In particular, we agree that opt-in approval should be required for the use and sharing of all customer PI[52] and that all affiliates should be treated as third parties.[53] As the Commission notes, companies can qualify as "affiliates" with virtually no obvious connection to a customer's known provider.[54] The Commission also recognizes that competition in the BIAS market is virtually non-existent and switching costs are high,[55] meaning that providers' incentives to cater to the customer relationship are weak in this market.[56]

We note that the Commission's discussion in this section is in extreme tension with its discussion of opt-out approval. Here, the Commission clearly recognizes that providers lack incentives to protect their consumers, yet its discussion of opt-out approval appears to assume that "a carrier's need to maintain a continuing relationship with its customer," along with the threat of liability, "would incentivize the carrier to prevent privacy harms."[57] Both cannot be true, and the truth is that providers lack sufficient incentives; this proceeding would be unnecessary if they did not.

[49] NPRM, ¶ 116.
[50] NPRM, ¶ 117.
[51] NPRM, ¶ 122-138.
[52] NPRM, ¶ 126.
[53] *Id*.
[54] NPRM, ¶ 128 and FN 222.
[55] NPRM, ¶ 128 and FN 223.
[56] NPRM, ¶ 128 and FN 224.
[57] NPRM, ¶ 125.

5. Deep Packet Inspection and Other Issues of Collection Limitation.

Deep packet inspection (DPI) represents a direct threat to consumers' legally protected privacy because it allows carriers to exploit their unique choke point position as gatekeepers to capture all consumer activity online.[58] Early uses of DPI raised several privacy concerns for EFF and other organizations as the conduct engaged by ISPs and third parties appeared to be in direct violation of multiple privacy laws.[59] Modern applications of DPI are even more sophisticated and despite arguments to the contrary that users are able to protect their privacy through encryption, virtual private networks, and multiple devices obfuscating user behavior,[60] a vast majority of user activity remains unencrypted and access to domain names alone reveals a treasure trove of information.[61] Furthermore, such arguments of user privacy self-defense are irrelevant as consumers have a statutory right to privacy under the Communications Act and telecommunications carriers have a legal obligation to protect that right. The FCC should ensure that telecommunications carriers do not act in ways that contradict their statutory obligations to protect confidential consumer information.

Therefore, as part of its general duty to protect customer PI, the FCC should find that carriers must refrain from utilizing deep packet inspection (DPI) of content that exceeds what is required of them to provide telecommunications service.[62]

More generally, the Commission should impose data minimization duties with respect to both the initial collection of customer PI as well as its retention.[63] Such limits will ensure that common carriers that enjoy liability protections[64] do not engage in activities unnecessary to their core purpose of providing telecommunications service. The level of market concentration in regards to high-speed broadband access of 25 Mbps and the inability of consumers to switch

---

[58] Upturn, What ISPs Can See – Clarifying the Technical Landscape of the Broadband Privacy Debate (March 2016), https://www.teamupturn.com/reports/2016/what-isps-can-see. [hereinafter Upturn Study]

[59] Letter to Congressman Edward Markey and Congressman Joe Barton, available at https://www.cdt.org/files/privacy/20080606markeybarton.pdf.

[60] Peter Swire et al., Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others, (Feb. 2016), http://peterswire.net/wp-content/uploads/Online-Privacy-and-ISPs.pdf.

[61] The Upturn Study noted that "many sites still don't encrypt: for example, in each of three key categories that we examined (health, news, and shopping), more than 85% of the top 50 sites still fail to encrypt browsing by default." In regards to volume versus sensitivity, the study noted that gigabytes of data consumers from watching a movie online does not reveal information as sensitive as megabytes of data from visiting the domain name www.webmd.com. *See generally* Upturn Study.

[62] As the Communications Act explains, "telecommunications" means the "*transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received*." *See* 47 U.S.C. § 153(50).

A "telecommunications carrier" is defined as "*any provider of telecommunications service, expect that such term does not include aggregators of telecommunications services (as defined in section 226 of this title). A telecommunications carrier shall be treated as a common carrier under this chapter only to the extent that it is engaged in providing telecommunications services, except that the Commission shall determine whether the provision of fixed and mobile satellite service shall be treated as common carriage.*" *See* 47 U.S.C. § 153(51).

[63] *See supra* Part 3.

[64] *See* 47 U.S.C. § 230 (The Communications Decency Act shields Internet access providers from liability arising from any "information provided by another information content provider," including customers and other users; *See also* 50 U.S.C. § 1885(a) (granting retroactive immunity to telecommunications providers for assisting the federal government in surveillance activities).

further bolsters the need for a robust general duty framework.[65] It will also provide the strongest assurance that common carriers can fulfill their mandate to protect sensitive private information by avoiding the possibility of becoming a repository of such valuable information and subject to malicious attacks from foreign governments and criminal actors.

A recent data breach provides a simple example of the importance of minimization. In October 2012, Comcast discovered that the names, addresses, and telephone numbers of approximately 75,000 California XFINITY Voice customers (and more across the country) who had requested and paid for a non-published directory listing and/or unlisted telephone number, had been posted on a publicly available Comcast-sponsored directory listing website, Ecolistings. The victims were Comcast subscribers who had paid $1.50 every month for an unlisted or non-published listing in order to help guard their privacy, and protect their personal information.[66]

The crucial point here is that Comcast failed basic minimization principles. Until October 2012, it was Comcast's practice to send both non-published listings and published listings to its "directory listing" agent, while placing a "privacy flag" on the non-published listings. Unfortunately, many California customers who elected non-published status prior to December 2009 were mistakenly not flagged as "non-published" and thus made available for publishing in July 2010.[67] This was a basic, yet spectacular, failure to minimize. The non-published listings should never have been sent or disclosed to Comcast's agent in the first place. A "privacy flag" is no substitute for not disclosing the information.

The most simple and straightforward solution is ensuring that a carrier simply cannot expose, leak, or disclose data that it literally does not possess. No legal or technical precaution can compare. Should the Commission follow our recommendations, the agency will provide robust protection of consumer privacy by ensuring that telecommunication carriers are unable to exploit their unique and powerful position as gateways to the internet[68] to engage in data collection and privacy monetization practices that consumers do not understand as necessary to their line of business.

---

[65] As the FCC Chairman noted, seventy five percent of Americans only have one choice in high-speed broadband of 25 mbps and higher. *See* Prepared Remarks of FCC Chairman Tom Wheeler, *The Facts and Future of Broadband Competition* (Sep. 4, 2014), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-329161A1.pdf.

[66] *Investigation into the Operations, Practices, and Conduct of Comcast Phone of California, LLC (U-5698-C) and its Unauthorized Disclosure and Publication of Comcast Subscribers' Unlisted Names, Telephone Numbers, and Addresses* (*Comcast Investigation*). Some of the documents in this proceeding are available at http://docs.cpuc.ca.gov/SearchRes.aspx?DocFormat=ALL&DocID=78432340. EFF Senior Staff Attorney and Adams Chair for Internet Rights Lee Tien was a witness in the California Public Utilities Commission enforcement action.

[67] A copy of the Settlement Agreement, Appendix B (Stipulated Facts), from which the facts in this paragraph are taken, is *available at* http://www.tellusventure.com/downloads/comcast/cpuc_comcast_settlement_17sep2015_appendix.pdf.

[68] Upturn Study; *See also* Princeton University letter from Nick Feamster, *available at* https://ftt-uploads.s3.amazonaws.com/fcc-cpni-nprm.pdf.

6. Customers should not have to pay for privacy.

The Commission should prohibit business practices that offer customers financial inducements for their consent to use and share customer PI, because such practices are prone to abuse. AT&T's Gigapower Premiere pricing program illustrates the problem: AT&T nevertheless uses the web browsing information of customers who are not part of the express use-and-sharing program.[69] Customers who pay more for privacy do not get the benefit of their bargain, and it is extremely difficult for such a customer to ever know one way or the other. More generally, as the Commission correctly observes, consumers generally do not understand the implications of such sharing, and many consumers are uncomfortable with exchanging their personal information for "free" services.[70]

7. Transparency

As we emphasized in our comments in the NPRM for the Open Internet Order, transparency is critically important.[71] Transparency is just as necessary in the area of BIAS provider use and sharing of customer PI as it is in the area of network management. To that end, the current transparency proposal in the NPRM is a good start, but we suggest several improvements.

First, the Commission asks if BIAS providers "should provide customers with information concerning their data security practices or their policies concerning the retention and deletion of customer PI."[72] While it is not necessary for BIAS providers to detail their data security practices, the disclosure of data retention and deletion policies is critically important. One of the key ways many customers will evaluate the privacy practices of BIAS providers is by looking at how long they retain different types of data: a privacy-focused customer would certainly prefer a BIAS provider that has a shorter retention period. Additionally, as discussed above in Section 3, the Commission should require BIAS providers to destroy customer PI once a customer no longer subscribes to the BIAS provider's services. However, if the Commission chooses not to enforce such a requirement, then it is vital that BIAS providers disclose how they handle customer PI after a customer terminates their relationship with the BIAS provider (at least in the case where the account is in good standing when it is terminated). If BIAS providers are allowed to retain customer PI for ex-customers, then those customers have a right to know whether or not a BIAS provider will retain their PI indefinitely, or will cease to use it once the customer ceases being a customer.

Second, the Commission asks if BIAS providers should be required to disclose "the specific entities with which they intend to share customer PI, rather than the categories of

---

[69] NPRM, ¶ 259, FN 402.
[70] For discussion of the problems with the "free" business model, see Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Internet's Most Popular Price*, 61 UCLA L. Rev. 606 (2014); Katherine J. Strandburg, Free Fall: The Online Market's Consumer Preference Disconnect, NYU School of Law, Public Law Research Paper No. 13 – 62 (2013).
[71] Electronic Frontier Foundation, *ISPs Mislead Public, FCC About Protecting the Open Internet* (Sep. 15, 2014), https://www.eff.org/press/releases/isps-mislead-public-fcc-about-protecting-open-internet.
[72] NPRM, ¶ 85.

entities."[73] The answer to this question is an unequivocal "Yes." The cost of compliance with this requirement is negligible: a BIAS provider simply needs to post the information on their privacy disclosure webpage—an act that costs almost nothing. Yet the benefits of such a requirement would be tremendous, particularly with respect to opt-in sharing of customer PI. After all, customers may not trust the privacy practices of entire categories of entities (say, online advertising networks), but may trust specific entities (say, online advertising networks which have particularly good privacy policies). By providing their customers with more specific information, BIAS providers will actually increase the chances that customers opt in to allowing their data to be shared, something that will presumably benefit both customers and BIAS providers. Moreover, this data is generated by customers themselves, and their interest in whom the data is shared with far outweighs any competitive benefit a BIAS provider might gain by keeping its data-sharing agreements a secret.

Next, regarding material changes in BIAS provider privacy notices, the Commission's intuition that BIAS providers should be required to obtain express affirmative consent before making material retroactive changes to their privacy policies is correct.[74] In particular, simply continuing to subscribe to the BIAS provider's services must not be considered to constitute express affirmative consent. Further, where the customer has a long-term contract with the BIAS provider (e.g., has agreed to pay for a year of service in order to lock in a particular price), denying consent to retroactive privacy policy changes should not invalidate that customer's contract; to do otherwise would create a significant power imbalance when it comes to long-term BIAS provider contracts. (After all, customers usually have very little recourse when they want to get out of such a contract, but any BIAS provider that wanted to get out of a contract in order to raise a price could then simply introduce a change to its privacy practices so offensive that no customer would agree to it, thus invalidating the contract.)

In any case, notice of material changes to a BIAS provider's privacy policy should be made to the customer at least 30 days ahead of the scheduled changes (e.g., in the bill the customer receives the month before the changes take effect).

Fourth, regarding the format of BIAS provider privacy policies, it is clear that the development of a standardized template for disclosure that can serve as a safe harbor will help to ease the regulatory burden on BIAS providers, and could also help customers better understand BIAS provider privacy practices.[75] The Commission also asks whether BIAS providers should be required to provide a "privacy dashboard."[76] It is certainly vital that BIAS providers provide their customers with all of the capabilities such a privacy dashboard would provide, so that customers may easily exercise their privacy rights. However, creating such a dashboard might prove to be a particularly heavy burden for small BIAS providers. (For example, small providers may find it easier to manually process requests received via email or phone for the correction of inaccurate customer PI, than to develop a full-fledged web-based interface.) As such, BIAS providers should simply be required to provide customers all of the options such a dashboard would provide (particularly the ability to review any customer PI the BIAS provider maintains,

[73] NPRM, ¶ 85.
[74] NPRM, ¶ 100.
[75] NPRM, ¶ 90.
[76] NPRM, ¶ 95.

correct inaccurate customer PI, and request the deletion of data that is not necessary for providing the underlying broadband service), and an online privacy dashboard should not be dictated as the only way BIAS providers could satisfy such a requirement.

Finally, the Commission asks if privacy transparency requirements should be different for mobile BIAS providers.[77] Given some of the most egregious privacy practices to date have been at the hands of mobile BIAS providers[78], and that mobile BIAS providers are privy to even more sensitive information than fixed BIAS providers (e.g. mobile location)[79], it is vital that the privacy transparency requirements that apply to mobile BIAS providers be as strict as those applied to fixed BIAS providers, if not stricter.

8. Anonymization/Aggregation of CPNI

The issues surrounding aggregation, de-identification, and re-identification of the data BIAS providers collect about their customers are complex,[80] and the proposals regarding aggregate customer PI are a good start. However, several improvements could be made in order to increase the robustness of any aggregation methods BIAS providers use.

The Commission correctly suggests that the threshold to use for the definition of aggregate customer PI is that no part of any aggregate customer PI data be "reasonably linkable to a specific individual or device."[81] The Commission also asks if it "should develop a list of identifiers that must be removed from data in order" for it to be considered aggregated;[82] such a list should be offered only as guidance, and not as a minimal set of identifiers that guarantees BIAS providers any sort of safe harbor. This is because, as the Commission notes, the field of re-identification is constantly advancing, and any such list would quickly become obsolete when it comes to ensuring that data cannot be re-identified to specific customers or devices.

Further, given continued advances in the field of re-identification, there is good reason to be concerned about the effectiveness and reliability of whatever methods BIAS providers choose to use in order to ensure that aggregate customer PI is not linkable to a specific individual or device. In order to ensure that the data BIAS providers share truly is unlinkable, the Commission must add a transparency requirement that would force BIAS providers, whenever they use a new method for generating aggregate customer PI, to disclose the details of that method to their customers (or preferably, directly to the public). This would expose the methods BIAS providers use for aggregation and de-identification to independent analysis by the academic community and other researchers, thereby ensuring that whatever methods BIAS providers use are truly impervious to any attempts to re-link the data to a specific individual or device.

---

[77] NPRM, ¶ 102.
[78] Hoffman, *supra* note 18.
[79] Yves-Alexandra de Montjoye et. al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, Nature.com Scientific Reports (Mar. 25, 2013), http://www.nature.com/articles/srep01376.
[80] NPRM, ¶ 154.
[81] NPRM, ¶ 154.
[82] NPRM, ¶ 163.

The alternative is essentially "security through obscurity." If BIAS providers are *not* required to disclose the methods they use to generate aggregate CPI (as in the current proposal), then there will be no other active pressure on BIAS providers to use more robust aggregation methods, and the lack of public scrutiny will inevitably lead to the use of weak aggregation methods instead. Then, when aggregate CPI is inevitably targeted and leaked in a data breach, that CPI will end up being much easier to re-link to individuals than if the aggregation algorithms that generated it had been subject to scrutiny from the beginning.

A transparency requirement of the sort we propose should require a BIAS provider to disclose enough information that an objective independent analyst with knowledge of de-identification and aggregation techniques would be able to evaluate the method's efficacy. At the very least, this should include:

1. The minimum number of customers whose data are used as an input to the de-identification/aggregation algorithm,
2. All of the specific types of data that are an input to the de-identification/aggregation algorithm,
3. How the algorithm processes those data types into aggregate information, and finally
4. The form of the resulting data that the BIAS provider then shares.

As an example, suppose a BIAS provider wanted to share the top 100 IP addresses its customers sent traffic to (as ranked by traffic volume per customer), broken down by zip code. A corresponding aggregation transparency disclosure might then look something like:

> "We may share the top 100 IP addresses our customers send traffic to, broken down by zip code. In order to aggregate this information, we first rank the IP addresses each customer sends traffic to by the amount of traffic sent. Then, for each IP address that appears in the top 100 for at least 30 customers, we compute its average rank. We then share those average ranks and their corresponding IP addresses."

Given that these sorts of disclosures are likely to be of interest to academic researchers and watchdog groups, providing them to each customer individually may be unnecessary. Instead, aggregation transparency disclosures could be included along with the other information regarding transparency that the Open Internet Order requires BIAS providers to post on their websites. In particular, BIAS providers should not have to share this part of their privacy disclosure with customers at the point of sale.

Regarding the sharing of aggregate customer data, the Commission suggests that BIAS providers should be required "to contractually prohibit any entity to which the BIAS provider discloses…aggregate customer data from attempting to re-identify that data."[83] In order to test the effectiveness of the BIAS provider's aggregation methods, an exception should be added to this requirement so that BIAS providers may share aggregate data with some entities explicitly for the purposes of re-identification. This exception should be designed to allow BIAS providers to take advantage of the expertise of academics, privacy researchers, and other interested parties who offer to test the efficacy of BIAS providers' aggregation methods using the actual aggregate

[83] NPRM, ¶ 161.

data. Such an exception should require that these third parties not further share any re-identified data (except with the BIAS provider itself) or use the data for any other purpose.

Finally, the Commission's conclusion that de-identified but non-collective data does not fall under the exception for use and disclosure of aggregate customer data enumerated in §222(c)(3) is correct, precisely because such data is not collective.[84] As such, de-identified non-collective data falls under the general use and disclosure prohibitions of §222(c)(1), and should be subject to the proposed opt-out and opt-in customer consent requirements described in the rest of the NPRM.

9. BIAS Providers Should be Accountable for Third-party Misuse of CPNI.

We agree with the Commission's proposal to require that BIAS providers take responsibility for the use of customer PI by third parties with whom they share such information,[85] precisely because the privacy purposes of § 222 can easily be "vitiated by the actions of agents."[86] Such responsibility should persist for as long as the data is in the third party's hands. Such an approach has long been part of the HIPAA Privacy Rule regarding "business associates." Prior to the Omnibus Rule promulgated after enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act, HIPAA covered entities were required to use standardized contracts (business associate agreements (BAA)) to create contractual liability for such third parties, but monitoring and enforcement were left to the covered entity. Unfortunately, HIPAA covered entities were less than diligent about overseeing BAAs. Under the current HIPAA rules, the government can now directly proceed against business associates for violating BAAs. Given this experience in the health arena, the Commission should require the specific contractual commitments laid out in ¶ 212, and should require publication of any such contracts to facilitate monitoring for compliance.

10. Any "Unlawful Use" Exceptions Must Be Carefully Circumscribed.

If the customer privacy rules for BIAS providers are to contain any express or implied exception for "unlawful use" of broadband services, the Commission should take care to limit the scope of that exception, especially with respect to accusations of copyright or trademark infringement.

BIAS providers, along with other Internet intermediaries, are protected against most forms of liability for unlawful acts by Internet users.[87] In particular, businesses including BIAS providers who merely transmit data are not liable for copyright infringement by third parties,[88]

---

[84] NPRM, ¶ 165.
[85] NPRM, ¶ 174.
[86] NPRM, ¶ 210 and FN 337.
[87] Section 230 of the Communications Decency Act, 47 U.S.C. § 230, shields "interactive computer service[s]," including Internet access providers, from liability arising from any "information provided by another information content provider," including customers and other users. Intellectual property laws and Federal criminal laws are exempted. *Id.*, § 230(e).
[88] *See, e.g.*, *Religious Tech. Ctr. v. Netcom On-Line Communications Servs., Inc.*, 907 F. Supp. 1361, 1370 (N.D. Cal. 1995) ("Although copyright is a strict liability statute, there should still be some element of volition or causation which is lacking where a defendant's system is merely used to use a copy by a third party."; *CoStar*

can obtain protection against most copyright remedies for such infringement,[89] and have no duty to prevent trademark infringement by users.[90] These protections have been vital to the development of the Internet economy, both because they create predictability and lower compliance costs for service providers, and because they remove incentives for Internet intermediaries to proactively block communications, a phenomenon that can chill free speech.

Recently, despite these strong statutory policies against Internet intermediaries acting as intellectual property enforcers, those intermediaries, including BIAS providers, are facing increasing pressure to do just that. Major U.S. Internet service providers today participate in private, voluntary copyright and trademark enforcement regimes despite having no legal duty to do so. For example, five major BIAS providers implemented the voluntary "Copyright Alert System" in 2013, which involves monitoring of Internet communications that use various peer-to-peer protocols, leading to interruptions of service for Internet subscribers as "mitigation measures."[91] Future private enforcement could include deep packet inspection (DPI) by BIAS providers, or other privacy-intrusive means, to detect infringement. These arrangements are driven by vertical integration[92] and close commercial ties between BIAS providers and major content producers, and by threats of new legislation to erode providers' protections against liability.

There are two reasons why the Commission should take caution in this area. First, broadband providers are poorly placed to determine whether or not content passing through their services is infringing or otherwise unlawful, which is why the law generally does not require them to make such determinations.[93] Deciding when use of the Internet is "unlawful" is a task generally reserved to attorneys, law enforcement, and courts. A loophole broadly permitting DPI, or the disclosure of customer information to third parties, based on voluntary copyright and trademark enforcement activities, would give BIAS providers incentive to be cavalier about making these difficult determinations.

Second, such an exception could easily swallow the rule; BIAS providers could excuse any number of privacy-intrusive practices by asserting that they were intended to target infringement. For example, the NPRM refers to Comcast's controversial use of DPI, discovered in 2007, to surreptitiously identify and block peer-to-peer traffic.[94] That roundly criticized practice led to Commission enforcement action and ultimately helped to shape the 2015 Open Internet Order.[95] However, had Comcast justified that invasion of privacy as a voluntary attempt

---

Group, Inc. v. LoopNet, Inc., 373 F.3d 544, 555 (4th Cir. 2004) ("Agreeing with the analysis in *Netcom*, we hold that the automatic copying, storage, and transmission of copyrighted materials, when instigated by others, does not render an ISP strictly liable for copyright infringement under §§ 501 and 106 of the Copyright Act.").

[89] 17 U.S.C. § 512(a).

[90] *See, e,g, Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93 (2d Cir. 2010).

[91] Center for Copyright Information, Memorandum of Understanding (July 6, 2011), http://www.copyrightinformation.org/wp-content/uploads/2013/02/Memorandum-of-Understanding.pdf.

[92] *See, e.g.*, "Comcast completes NBC Universal merger," Reuters (Jan. 29, 2011), http://www.reuters.com/article/us-comcast-nbc-idUSTRE70S2WZ20110129; Kevin Fitchard, "The Real Reason Verizon bought AOL," Fortune (June 24, 2015), http://fortune.com/2015/06/24/verizon-gains-aol/.

[93] *See supra* notes 87-90.

[94] NPRM ¶ 264 & n.414.

[95] In the Matter of Protecting and Promoting the Open Internet, Report and Order, GN Docket No. 14-28 (rel. Mar. 12, 2015) ¶¶ 65, 111.

to reduce copyright infringement conducted over peer-to-peer protocols, a broad or vague "unlawful use" exception could have excused Comcast's conduct.

Mere accusations of "unlawful" Internet use cannot justify disclosures of customer information. Under the law of many states, a subpoena for personally identifying information of an Internet user in a civil case alleging unlawful communications cannot issue unless the complaining party can show, using available facts, that a violation of law has occurred.[96] Intellectual property claims, as with other claims of unlawful communications, require a factual showing and an opportunity for the alleged wrongdoer to respond before a disclosure of PII can be compelled.[97] These decisions provide guideposts for the Commission regarding BIAS customer privacy.

To avoid undermining important legal protections for speech and privacy, the Commission should make clear that any exception relating to "unlawful use" of broadband services does not apply to copyright or trademark infringement unless 1) specific, concrete instances of infringement are identified, 2) the customer is given notice and an opportunity to challenge any otherwise prohibited use or disclosure of CPI; and 3) any otherwise prohibited use or disclosure of CPI be limited to what is necessary to initiate legal action or otherwise remedy the infringement. Collection or retention of CPI for the purpose of preventing "unlawful" use of the Internet should not be allowed except where it is explicitly permitted by FCC rules, or required by court order. Voluntary preemptive monitoring or prevention of intellectual property infringement should not, by itself, qualify for any "unlawful use" exception.

Conclusion

We support the FCC updating its privacy regulations. The obligations of telecommunications carriers have evolved in the broadband marketplace. Every telecommunications carrier holds a general duty to protect customer PI.[98] The FCC has clear legal authority to establish regulations to detail the contours of that general duty and related legal responsibilities.[99] Congress enacted the privacy provisions within the Communications Act in order to make clear that telecommunications carriers' customers and competitors would have their private information protected. By not acting, the FCC will place the burden on the user community to protect their own privacy interests and in many instances it is impossible for them to completely shield their online activity from their BIAS provider.

The Commission should establish that a telecommunications carrier's general duty comes in direct conflict with many uses of DPI and only allow its use when directly related to the provisioning of BIAS.[100] By doing so, the rules will ensure privacy protections for broadband

[96] *See, e.g.*, *Dendrite Int'l v. Doe No. 3*, 342 N.J. Super. 134, 775 A.2d 756 (N.J. App. 2001); *Doe v Cahill*, 884 A.2d 451 (Del. 2005).
[97] *See, e.g.*, *In re BitTorrent Adult Film Copyright Infringement Cases*, 296 F.R.D. 80, 83 (E.D.N.Y.), *report and recommendation adopted sub nom. Patrick Collins, Inc. v. Doe 1*, 288 F.R.D. 233 (E.D.N.Y. 2012) (noting that accused infringer was given "an opportunity to move to quash" a subpoena to his or her Internet service provider for PII).
[98] See *supra* Part 1.
[99] *Id*.
[100] *See supra* Part 5.

consumers by avoiding the dangers of excessive information collection. We strongly urge caution when contemplating exceptions to the rule and how DPI should be allowed to search for "unlawful uses" of broadband service, particularly in the areas of copyright and trademark infringement.[101] Vertical integration or close commercial ties between content producers and broadband providers raises concerns that a broad exception to inspect for "unlawful uses" would defeat the goals of protecting consumer privacy by making all content subject to inspection. In order to avoid this outcome, the Commission's exceptions must be narrowly defined and require a provider to give notice to the customer.[102]

EFF agrees with the broad approach the FCC adopted in its 2013 CPNI Declaratory Ruling and the interpretations of what falls within CPNI under § 222(h)(1) as well as the agency's definition of PII and of "customer PI." We recommend that the FCC provide an illustrative but not exhaustive list of examples to the industry and update it frequently as technology changes to reduce compliance costs and avoid obsolescence.[103] In regards to other definitions, the FCC should define "communications-related services" narrowly in order to avoid an expansion of opt-out approval that would defeat the underlying customer protections.[104]

The FCC should avoid establishing retention rules that attempt to accommodate requests from law enforcement and legitimate business purposes, as that would make it impossible to protect consumers' interests in privacy. Rather, the FCC should solely be focused on meeting the legitimate business purposes as well as follow the data destruction model under the Fair and Accurate Credit Transactions Act.[105] We further urge the agency to establish clear transparency rules of retention and deletion practices in order for the public to ensure compliance and robustness.[106]

We disagree with the proposal to remove the 30-day waiting period as customers do not or often are unable to ascertain what the provider intends to do with their information. We further disagree with the Commission's consent framework in regards to a three tiers approach.[107] An implied approval category that allows for a telecommunications carrier to treat "no approval" as essentially approval contradicts the language of § 222. Lastly, decisions on an opt-out approval process by the Commission must be firmly rooted in protecting consumers and not rely on non-existent provider incentives of maintaining a relationship with their customers. Telecommunications providers have resisted the FCC from establishing clear robust privacy protections for consumers as it directly impacts their interests in monetizing their customers' online activity.

[101] *See supra* Part 10.
[102] *Id*.
[103] *See supra* Part 2.
[104] *Id*.
[105] *See supra* Part 3.
[106] *See supra* Part 7.
[107] *See supra* Part 4.

BIAS providers are uniquely positioned to gather a wide variety of data on their customers—data that they most certainly can (and in many cases, already do) monetize. This issue is exacerbated by the fact that many consumers have only one choice for high-speed access in most parts of the country, and so cannot "shop around" for more privacy-friendly broadband service.[108] Arguments to the contrary ignore the underlying reality that access to the internet is wholly dependent the BIAS provider, and absent strong privacy rules, providers have every reason to take advantage of the opportunity to monitor, collect, and monetize user data.

Respectfully submitted,

Ernesto Falcon
Lee Tien
Jeremy Gillula
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

[108] Prepared Remarks of FCC Chairman Tom Wheeler, *supra* note 65.