Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	WC Docket No. 16-106
Petition of Public Knowledge et al. for Declaratory Ruling that Section 222 of the Communications Act Prohibits Telecommunications Providers from Selling Non-Aggregate Call Records Without Customers' Consent	WB Docket No. 13-306

COMMENTS OF NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE

Filed May 27, 2016

TABLE OF CONTENTS

INTRODUCTION AND SUMMARY

New America's Open Technology Institute ("OTI") strongly supports the proposed privacy rules for BIAS providers, as laid out in the FCC's Notice of Proposed Rulemaking ("NPRM").[1] The Federal Communications Commission ("FCC" or "Commission") has a long history of protecting the privacy of Americans on vital communications networks. Today, OTI urges the Commission to ensure these vital consumer protection measures apply to customers of broadband Internet access service ("BIAS"), the most important network of our time.[2]

The FCC has clear authority to address customer privacy and CPNI in the broadband context. This authority flows from the 2015 Open Internet Order, which in reclassifying BIAS service as a Title II service gave the FCC a statutory mandate to enact the privacy protections outlined in Section 222.

This Commission's approach to consumer privacy, grounded in principles of transparency, choice, and security, brings much-needed consumer control over data practices of BIAS providers. The proposed rule contains key checks and balances to ensure that BIAS providers are responsive to customer privacy preferences while still giving them opportunities to improve their services.

It is time to grant online communications the same privacy protections available to services like landline phones. Although Internet use is an essential part of everyday life, much like access to phone service, consumers have well-

---

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Notice of Proposed Rulemaking, 31 FCC Rcd 2500 (Apr. 1, 2016) ("NPRM" or "Notice").

[2] Many thanks to OTI's summer legal intern Ryan Morrison, who provided invaluable assistance with research and citations for these comments.

founded concerns about their online privacy. One recent survey indicated that over 80% of respondents were "concerned" or "very concerned" when asked about their online privacy, and scores of Americans have suffered the negative consequences of a data breach.[3] Nonetheless, Americans increasingly feel completely helpless to protect their own data privacy when they go online. As University of Pennsylvania Communications Professor Joseph Turow and his colleagues have found, "rather than feeling able to make choices, Americans believe it is futile to manage what companies can learn about them."[4]

While these privacy concerns apply to the whole Internet, they are sharpest in the context of the relationship between the customer and the BIAS provider. As "the gatekeeper" to the Internet, a BIAS provider has a unique window into a customer's behavior. In the course of shuttling packets of data, a BIAS provider can glean a great deal of information about a customer's personal habits and proclivities. This creates many opportunities for abuse and misuse of data.

OTI greatly appreciates the Commission's proposal, agrees with many of the recommendations in it, and provides the following recommendations to refine the proposed rules and ensure that sensitive consumer data is protected through a strong privacy regime.

---

[3] Freedman Consulting, "Poll Finds Strong Support for Expanding Online Privacy Protections and Internet Access" (Nov. 23, 2015), available at https://www.freedmanconsulting.com/documents/PrivacyandAccessResearchFindings_151123.pdf; Lee Rainie and Maeve Duggan, "Privacy and Information Sharing," The Pew Research Center (Jan. 14, 2016) https://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/.

[4] Joseph Turow et al., "The Tradeoff Fallacy" (Report from the Annenberg School for Communication, June 2015), available at https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

I. It is good public policy to establish strong consumer privacy protections for broadband Internet access customers, as the law requires

There are important policy reasons driving the law's concern with holding telecommunications access providers to high privacy standards. Through their role as network gatekeepers, BIAS providers have privileged access to an extraordinary wealth of private information about their customers. Customers, for their part, have no choice but to share this wealth of information with BIAS providers. But because broadband customers share the information for the specific purpose of enabling BIAS providers to effectively carry out the access service for which they are paid, the customers rightfully retain ownership of this information and do not expect it to be used in ways other than to provide service without their express permission. If BIAS providers are permitted nevertheless to make additional uses of customer information without first obtaining affirmative consent, customers will perceive that their privacy has been violated, which could in turn negatively impact their willingness to make full and unrestrained use of the network.

A. BIAS Providers have access to a wealth of highly private information about their customers and their customers' communications

OTI agrees with the FCC and the FTC that "ISPs are in a position to develop highly detailed and comprehensive profiles of their customers—and to do so in a manner that may be completely invisible."[5] As OTI has previously noted, "[a]t a

[5] NPRM, at ¶ 4 (quoting Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers at 56 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change/recommendations/120326privacyreport.pdf)(internal quotations omitted).

technical level, ISPs have a wide range of ways to gather and compile an extremely detailed profile about each subscriber."[6] Among other things, when BIAS providers monitor their customers' traffic, they may learn the content of unencrypted traffic, destination information for traffic, and information about connected devices and applications.

This raw data alone can be quite revealing—especially when unencrypted—but further analysis of even encrypted traffic could yield still more personal inferences about a customer's life. For example, traffic data could be analyzed to reveal details about the customer's health, finances, political views, employment status, and much more.[7] In the words of then–FTC Commissioner Julie Brill, "[e]ven if an ISP just looks at the IP addresses to which you connect and the time at which connections occur, it can get an intimate portrait of your interests, daily rhythms, habits—as well as those of all members of your household."[8] Brill also noted that data made available to BIAS providers "will become even more detailed and voluminous" as the Internet of Things expands.[9]

---

[6] *See* New America's Open Technology Institute, The FCC's Role in Protecting Online Privacy (Jan. 21, 2016) at 3, *available at* https://www.newamerica.org/oti/policy-papers/the-fccs-role-in-protecting-online-privacy/ ("OTI Privacy Paper").
[7] OTI Privacy Paper, at 5.
[8] Julie Brill, Comm'r, Fed. Trade Comm'n, *Net Neutrality and Privacy: Challenges and Opportunities*, Keynote Address at Georgetown Institute for Public Representation and Center for Privacy and Technology Symposium on Privacy and Net Neutrality at 6 (Nov. 19, 2015), *available at* https://www.ftc.gov/public-statements/2015/11/net-neutrality-privacy-challenges-opportunities.
[9] *Id.*

B. Customers cannot reasonably avoid sharing this information with BIAS Providers

Not only is the information to which BIAS providers enjoy privileged access highly private, but BIAS customers cannot reasonably avoid exposure of this sensitive data. As the FCC notes, "the use of information for the delivery of broadband services is inherent in the customer-broadband provider relationship."[10] OTI has noted that broadband customers "have no choice but to share [personal] information; to gain access to the Internet, they must connect through an ISP."[11] Individuals cannot simply connect their own devices to the Internet; rather, they must pay another party for access. They cannot route their own online traffic either; instead, they rely on BIAS providers to route traffic from Point A to Point B at their request.

Nor can customers escape BIAS providers that engage in particularly privacy-violative practices. Indeed, not only do consumers lack choice, and must go through *some* BIAS provider to get online, they often have no choice with respect to *which* BIAS provider to use because the BIAS market is often monopolistic. According to the FCC's *2016 Broadband Progress Report*, "[a]pproximately 51 percent of Americans have one option for a provider of 25 Mbps/3 Mbps fixed broadband service."[12] In most cases, therefore, BIAS customers will not be able to switch providers to avoid privacy-violative practices.

---

[10] NPRM, at ¶ 18.

[11] OTI Privacy Paper, at 2.

[12] *Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act*, 2016 Broadband Progress Report, 31 FCC Rcd 699, 736 ¶ 86 (2016).

Even in markets in which consumers may theoretically choose from among multiple available BIAS providers, high switching costs make it difficult to exercise the choice between providers.[13] As the Commission has previously found, consumers wishing to switch from one BIAS provider to another face significant barriers.[14] First, there may be significant financial costs, in terms of canceled contracts, installation fees, or bundle discount.[15] Second, these customers may have to invest a substantial amount of time and effort in the form of finding a new provider, installing new equipment, or taking time off of work to wait for technicians to come to their home.[16] Third, perceived switching costs may be even higher, further discouraging customers from switching.[17] Thus, there is a strong incentive for customers to stay at their current provider, even if they are unhappy with their provider's privacy- or security-related practices.

---

[13] Barbara van Schewick, Stanford Center for Internet and Society, *Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like* 33-38 (2012), http://cyberlaw.stanford.edu/downloads/20120611-NetworkNeutrality.pdf ("Switching costs in the market for Internet services are substantial. Consider first the obvious financial expenses that may be associated with switching providers.... Further, switching providers may require a customer to invest a significant amount of time and effort.")

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

[15] *Id*. at ¶ 36.

[16] *Id*.

[17] *Id*. at ¶ 37; *see generally*, *id*. at ¶ 81.

C. The context in which broadband customers share private information with BIAS Providers is specific and cabined

The context in which broadband customers share private information with BIAS providers is specific and accompanied by cabined expectations: the customers share the information with BIAS providers to facilitate provision of a service for which they have contracted. The information is therefore most appropriately thought of as on loan to, rather than transferred to, broadband providers. OTI agrees with the FCC's characterization of private information shared by customers for the purpose of receiving broadband service as a "possession" belonging to the customer.[18]

The context in which broadband customers share private information with BIAS providers is important. Over the past several years, the privacy field has shifted toward an understanding of privacy expectations as anchored to the *context* in which information is shared, rather than to the sensitivity of a particular piece of information. As prominent privacy scholar and philosopher Helen Nissenbaum explained in 2009, "finely calibrated systems of social norms . . . govern the flow of personal information in distinct social contexts," and "[i]nformation technologies alarm us when they flout these information norms." Worse, argued Nissenbaum, "are [technologies] that disregard entrenched norms because, as such, they threaten disruption to the very fabric of social life."[19] When considering whether or not a particular use or disclosure of information offends

---

[18] NPRM, at ¶ 12 ("the consumer who possesses private information must provide the broadband provider advanced approval for the use of that data").
[19] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* 3 (2009).

privacy, it is therefore important to consider the particular context in which information is shared.

Nor is the contextual understanding of privacy that Nissenbaum described purely academic—on the contrary, this approach has resonated widely, including with policymakers across government. Multiple agencies have shifted toward this framework to better understand existing context-specific privacy laws and to inform decisions about how to regulate privacy moving forward. Indeed, "Respect for Context" appeared as one of the seven principles advanced in the White House's 2012 *Consumer Privacy Bill of Rights*, which cited Nissenbaum's work.[20] The White House stated, "[c]ompanies should limit their use and disclosure of personal data to those purposes that are consistent with both the relationship that they have with consumers and the context in which consumers originally disclosed the data, unless required by law to do otherwise."[21] The month after the White House report came out, the Federal Trade Commission's Report on *Protecting Consumer Privacy in an Era of Rapid Change* foregrounded contextual considerations as well. Responding to comments from the public and dialogue with other policymakers, the FTC rejected an approach to consumer choice it had previously proposed that considered whether information collection and use practices were "commonly accepted," instead setting forth "a modified approach that focuses on the context of the consumer's interaction with the business."[22]

---

[20] The White House, *Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* 15–16 (2012).

[21] *Id*. at 15.

[22] FTC, *Protecting Consumer Privacy in an Era of Rapid Change* iv (2012); *see* Alexis C. Madrigal, *The Philosopher Whose Fingerprints Are All Over the FTC's New*

(continued on next page)

As the FCC moves forward with this rulemaking, it must continue to examine, as it has begun to, how BIAS customers' privacy expectations are informed by the particular context of telecommunications service. The FCC recognizes that "the use of information for the delivery of broadband services is inherent in the customer-broadband provider relationship." OTI agrees. Where BIAS customers provide private information about their online activities and communications with BIAS providers solely for the purpose of facilitating connectivity and routing, it does not violate context-specific norms for the information to be used for that purpose. But the FCC should examine additional uses of that information with skepticism, as likely inconsistent with the customer-carrier relationship and with the context of the initial disclosure.

D. BIAS customers' personal information must be protected to encourage broadband adoption and use

Permissionless use of BIAS customers' personal information not only misappropriates data that belongs to customers and violates contextual norms, but also negatively impacts broadband adoption and use. In order for consumers to adopt and use broadband without hesitation or self-censorship, they must have utmost confidence that BIAS providers will carry out basic access and connectivity functions with integrity.

(footnote continued)
Approach to Privacy, The Atlantic (Mar. 29, 2012), http://www.theatlantic.com/technology/archive/2012/03/the-philosopher-whose-fingerprints-are-all-over-the-ftcs-new-approach-to-privacy/254365/ ("the recent Federal Trade Commission report, . . . which purports to lay out a long-term privacy framework for legislators, businesses, and citizens, uses the word context an astounding *85 times*!").

Indeed, research has broadly and consistently demonstrated that privacy concerns constitute a barrier to broadband adoption and use. For example, in 2010, an FCC survey on broadband adoption and use revealed that 57% of Internet non-adopters felt online activities made it too easy for theft of personal information.[23] Analysis of that survey led to the FCC concluding in the *National Broadband Plan* that concerns about online privacy and security "may limit [consumers'] adoption or use of broadband."[24] More recently, the National Telecommunications and Information Administration found, based on data collected by the Census Bureau in 2015,

> Forty-five percent of online households reported that [privacy and security] concerns stopped them from conducting financial transactions, buying goods or services, posting on social networks, or expressing opinions on controversial or political issues via the Internet, and 30 percent refrained from at least two of these activities.[25]

And in January this year, the City of Portland, Oregon's Office for Community Technology reported that in focus groups conducted by the city to improve the

---

[23] This number was reported in contrast to 39% of adopters who felt the same way. John Horrigan, *Broadband Adoption and Use in America* 17 (FCC Nat'l Broadband Plan, Working Paper No. 1, 2010), https://transition.fcc.gov/DiversityFAC/032410/consumer-survey-horrigan.pdf.

[24] FCC, *Connecting America: The National Broadband Plan* 17 (2010), https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf.

[25] Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NTIA (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

city's understanding of adoption challenges, privacy concerns were raised in every group.[26] The evidence is clear that privacy and security concerns can chill consumers' willingness to get online and to use the network to its full potential.

II. In accordance with the law and with the above policy considerations, the FCC should move forward swiftly to enact consumer privacy rules issuing from the proposal

The law aligns with the policy justifications outlined above. The Communications Act imbues the FCC with particularly strong consumer privacy authority as against telecommunications common carriers—a category that now includes BIAS providers. And apart from Title II, several additional sources of statutory authority support a broad and flexible approach to FCC rulemaking and enforcement of consumer privacy to ensure that communications networks, and the private information and communications contents conveyed through them, are well protected and well trusted.

The FCC asserts that "[f]undamentally, Section 222 obligates telecommunications carriers to protect the confidentiality of proprietary information, including proprietary information about their customers, and in furtherance of that obligation it requires carriers to seek approval before using or sharing customer proprietary network information."[27] OTI agrees. Section 222 of the Communications Act, "Privacy of customer information," places on carriers a general "duty to protect the confidentiality of proprietary information" and

---

[26] Angela Siefer, *Signs On Letter Encouraging FCC Protect Privacy Of Broadband Consumers*, NDIA (Jan. 26, 2016), http://www.digitalinclusionalliance.org/blog/2016/1/26/ndia-signs-on-letter-encouraging-fcc-protect-privacy-of-broadband-consumers.

[27] NPRM, at ¶ 297.

prohibits them from using or disclosing CPNI for purposes other than to provide service "[e]xcept as required by law or with the approval of the customer."[28]

In addition, OTI agrees with the FCC that additional relevant statutory authority derives from "a number of other statutory provisions, which provide authority to protect against unjust, unreasonable, and unreasonably discriminatory practices; interception or divulgence of communications; and the untimely deployment of advanced telecommunications services."[29] Of particular importance is Section 201, which, as the FCC notes, both the FTC and the FCC have found "can be read as prohibiting the same types of acts or practices" as Section 5 of the FTC Act. Under a Section 201 inquiry similar to the FTC's approach to Section 5 unfairness, the FCC would likely ask, as the FTC does, whether a BIAS provider's practice causes substantial injury, has no or insufficient countervailing benefits, and is not reasonably avoidable by consumers.[30] Such an inquiry could, for example, find that BIAS providers' use of customers' private information for purposes other than to provide service constitutes not only a Section 222 violation when done without prior affirmative consent, but also a Section 201 violation.

---

[28] 47 USC § 222(c)(1).
[29] NPRM, at ¶ 304
[30] Fed. Trade Comm'n, *FTC Policy Statement on Unfairness* (1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness ("The independent nature of the consumer injury criterion does not mean that every consumer injury is legally "unfair," however. To justify a finding of unfairness the injury must satisfy three tests. It must be substantial; it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided.").

III. The proposed framework strikes an appropriate balance between protecting BIAS customers and allowing BIAS providers to provide personalized services

The FCC has proposed a strong and comprehensive rule protecting customers of BIAS providers from potential misuse of their data. Below, OTI describes notable aspects of the Notice and potential improvements or pitfalls the FCC should avoid.

A. Most of the proposed definitions are strong, though some should be changed to more comprehensively protect BIAS customers

The Notice proposes several strong definitions. However, some deserve special consideration as they raise difficult issues and some are not appropriately tailored to this context.

1. The 10% ownership threshold in the proposed definition of "affiliate" is too low for this context

The proposed definition of "affiliate" is too broad in reference to the provisioning of broadband service, and would consequently allow BIAS providers to apply a lower consent standard when sharing their customers' data with many entities that are functionally third parties. As currently proposed, "affiliate" will mean "a person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another person," and the term "own" will mean "to own an equity interest (or the equivalent thereof) of more than 10 percent."[31] The proposed rule allows BIAS providers to use and share customer PI with communications-related affiliates for marketing with only opt-out

[31] NPRM, at ¶ 30.

consent.[32] With such a low threshold for ownership in the definition of "affiliate," BIAS providers will have the ability to share customer PI, with only an opt-out requirement, more broadly than desired.

The FCC should not adopt a 10% threshold for the definition of "affiliate," because with only a 10% equity interest, it is unlikely the BIAS provider "own[s] or control[s]" the entity. In other contexts, such as at the US Small Business Administration and under Federal Reserve law, the equity ownership requirement to be an affiliate is as high as 50%.[33] In other privacy-specific contexts, including California's financial privacy law, the ownership threshold is 25%.[34] The FCC should adopt at least a 25% threshold definition of "affiliate" to better protect BIAS customers against unwanted disclosure and dissemination of their data.

2. The proposed definition of "customer" correctly includes former customers and applicants for BIAS service and should take into account multiple account holders in the household

The Notice proposes a definition of "customer" that includes current, former, paying, and nonpaying subscribers, as well as applicants for BIAS service.[35] OTI supports this inclusive definition of "customer." Including only current customers would be too narrow because of the strong incentives for BIAS providers to collect and retain data from all customers without limitation.

---

[32] *Id*. at ¶ 122
[33] U.S. Small Bus. Ass'n, *Small Business Compliance Guide Size and Affiliation* 7 (2010), https://www.sba.gov/sites/default/files/articles/affiliation_ver_03.pdf; 12 USC § 221a(b)(2) (2012).
[34] California Financial Information Privacy Act, Cal. Fin. Code § 4052(d)-(g).
[35] NPRM, at ¶ 31.

BIAS providers collect an enormous amount of data. A cursory review of BIAS provider privacy policies shows that there are few data points left uncollected. AT&T's privacy policy, for instance, states that it collects the following information from users:

- name,
- address,
- telephone number,
- email address,
- services provided,
- telephone numbers contacted by the customer,
- payment history,
- credit history,
- credit card numbers,
- Social Security number,
- security codes,
- service history,
- equipment type,
- device IDs,
- device status,
- serial numbers,
- settings,
- configuration,
- software,
- network performance information of equipment,
- usage information of equipment,
- wireless device location,
- number of text messages sent and received,
- voice minutes used,
- calling and texting records,
- bandwidth used,
- resources used,
- IP addresses,
- URLs visited,
- data transmission rates and delays,
- pages you visit,
- time spent on those pages,
- links or advertisements seen and followed,
- search terms entered,

- how often certain applications are opened,
- how long spent using apps,
- location (ZIP code and street address, whereabouts of wireless devices through cell towers, Wi-Fi routers, access points, and GPS),
- and TV viewing habits.[36]

It is clear that AT&T amasses a vast collection of data from each of its customers.

Additionally, BIAS providers' data collection and retention practices could be expanding because data storage costs have been steadily decreasing for years. As the White House noted in its seminal 2014 Big Data report, "the declining cost of collection, storage, and processing of data, combined with new sources of data like sensors, cameras, geospatial and other observational technologies," has meant that we now live in a "world of near-ubiquitous data collection."[37] Indeed, the precipitous decline in these computing and storage costs has been a tectonic force in shaping the era of Big Data. Between 1992 and 2002, the cost of computing power declined from $222 to a mere $0.06 per million transistors, and over the same time period, the cost of data storage decreased at a similar scale, from $569 to $0.03 per gigabyte.[38] The availability of cheap and plentiful data services is reflected in our mushrooming rates of data creation: IDC estimates that by 2020, the amount of

---

[36] *See AT&T Privacy FAQ*, AT&T, https://www.att.com/gen/privacy-policy?pid=13692 (last visited May 27, 2016). The policy does not mention the length of time the company retains the data.

[37] Exec. Off. of the President, *Big Data: Seizing Opportunities, Preserving Values* 4 (2014), https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

[38] John Hagel, *From Exponential Technologies to Exponential Innovation* 5 (2013), http://dupress.com/articles/from-exponential-technologies-to-exponential-innovation/.

data that we generate as a society will reach 44 zettabytes.[39] Today, it is no longer prohibitively difficult to amass and analyze troves of data at significant scale. For their part, BIAS providers can and likely do amass substantial data profiles that could represent years of intimate, personal, and sensitive behavioral information affecting millions of customers.

As data retention becomes easier and cheaper, BIAS providers no longer have practical barriers to retain indefinitely all data they collect from all of their customers. As customers cancel service, they would have no way to protect their data without additional legal protections. Under the proposed definition of "customer," the provider would have to make available a way for former customers to opt in or opt out of certain data disclosure and use, and give the former customer the ability to change his or her mind.[40] With these increased protections, customers will be able to leave their BIAS provider with the confidence that their data will not be exploited after the relationship is terminated.

The Notice also seeks comment on whether the rule should account for the fact that a single subscription can be used by multiple people in the household. OTI does not take a position on whether the FCC should require separate consent from each individual in the household. However, many BIAS providers allow customers

---

[39] IDC, *The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things*, IDC (Apr. 2014), http://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm.

[40] At ¶227, the Notice asks whether data retention periods would be appropriate. While OTI favors data retention periods, as data should not be kept indefinitely, giving former customers the choice over whether and how to use their data would be helpful as well. Former customers should also be given the choice of requiring the BIAS provider to delete their data entirely.

to create multiple accounts for other members of the household.[41] Separate accounts for other members of the household provide a straightforward mechanism for providing notice of privacy practices and acquiring opt-in or opt-out consent for those practices. Each account can have its own dashboard or other mechanism for providing notice and consent. Thus, in that way, the FCC's rule should reflect that "each user with a login be treated as a distinct customer" requiring notice and consent.[42]

3. The FCC has appropriately defined customer PI to include CPNI and PII

Section 222 imposes multiple obligations on the FCC to ensure telecommunications service providers protect the confidentiality of customer information. The first, in Section 222(a), is the general obligation to "protect the confidentiality of proprietary information of . . . customers." The second obligation, as it relates to customers, is protecting the confidentiality of CPNI. While these are related obligations, they are distinct.[43] It is clear that Congress intended the FCC to protect customer information generally because of its use of broad, vague language

---

[41] For example, Comcast allows for up to 6 additional users for its XFINITY service, and Charter allows for up to 7 users. *See XFINITY My Account*, Comcast, https://customer.xfinity.com/help-and-support (last visited May 27, 2016); *see also Manage Charter Usernames*, Charter Comm., http://www.charter.net/support/my-account/manage-charter-usernames/ (last visited May 27, 2016).

[42] NPRM, at ¶ 34.

[43] *See Verizon Cal., Inc. v. FCC*, 555 F.3d 270, 273 (D.C. Cir. 2009) (agreeing with the FCC that "proprietary information" under Section 222(b) includes information outside the definition of CPNI).

in Section 222(a).[44] In addition, Congress had specific concerns about CPNI, which led it to enact Section 222(c).[45]

The FCC has correctly recognized that these obligations are separate.[46] OTI is already on the record in agreement with the FCC on this point. In response to a Petition for Reconsideration filed in the Lifeline docket challenging the FCC's authority to require that Lifeline eligibility applications be kept reasonably secure, OTI and a coalition of consumer and privacy organizations argued that Sections 222(a) and 222(c) contemplate distinct, but related obligations to protect consumer privacy; that the specific provisions of 222(c) do not eliminate the general duty imposed by 222(a); and that the legislative history of Section 222 is consistent with this interpretation.[47]

Drawing from its interpretation of Sections 222(a) and 222(c) as establishing distinct obligations for BIAS providers, the Commission has proposed to define a broad category of protected information, called "customer PI," which includes both CPNI (as contemplated by the statute) and personally identifiable information ("PII"). In general, customer PI encompasses private data that customers have an interest in protecting against public exposure.[48] OTI supports this approach. With

---

[44] *City of Arlington, Tex. v. FCC*, 133 S. Ct. 1863 (2013); *Chevron, U.S.A., Inc. v. Nat. Res. Def. Council, Inc.*, 467 U.S. 837 (1984); Harold Feld. et al., *Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World* 16-19 (Public Knowledge, White Paper, Feb. 2016), https://www.publicknowledge.org/documents/protecting-privacy-promoting-competition-white-paper ("PK White Paper").
[45] PK White Paper, at 17.
[46] NPRM, at ¶¶ 56-57.
[47] *Lifeline and Linkup Reform and Modernization*, Opposition to Petition for Partial Reconsideration of Appalshop *et al.*, WC Docket No. 11-42 (filed Oct. 9, 2015).
[48] NPRM, at ¶ 57.

such broad protection, customers have increased choice over how their BIAS providers use and disclose their data.

CPNI should be defined as the statute requires, but should also include port information. The definition of CPNI should mimic the statute but should also be interpreted broadly for the broadband context.[49] CPNI is defined in the statute 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."[50] This definition clearly captures data such as service plan information (as a "type" of use, among others), geolocation ("location" of use), MAC addresses ("destination" and "technical configuration" of use), IP addresses ("destination" and "location" of use), and traffic statistics ("type" and "amount" of use). OTI supports these categories of data as types of CPNI.

The FCC should also include port information within the definition of CPNI. Port information clearly fits within the definition of CPNI.[51] Ports are part of the header on a packet of information, and the port determines how the service will use the packet's data.[52] Ports are generally separated into different uses. For instance, port 80 is used for HTTP traffic and port 443 is used for HTTPS traffic. Some ports are very specific, and information about traffic traveling to those ports may reveal even more detailed information about a BIAS customer's use of the service. For example, port 194 is used for Internet Relay Chat and port 666 for the 1993 video

[49] OTI Privacy Paper, at 7.
[50] 47 USC § 222(h)(1)(a).
[51] It may even be considered "content" depending on how specific the use for the particular port is.
[52] PK White Paper, at 47.

game Doom.[53] Thus, port data is either content and must be opt-in under Section 705, or is related to the "type" of telecommunications use and fits within the CPNI definition.

PII should be defined broadly, but some types of data need further explanation. PII should also be defined broadly.[54] The FCC must, as it has proposed to do, adopt a definition of PII that takes into account the fact that de-identified data can often be re-identified. Re-identification poses tangible threats to privacy, in part because once it has been disclosed, data cannot be taken back, and as time goes on, the chances of re-identification increase.[55] A recent study found that supposedly de-identified datasets from medical records, search queries,[56] social network data,[57] genetic information,[58] geolocation data,[59] and taxi-cab history[60]

---

[53] *See* "List of TCP and UDP port numbers," Wikipedia (visited May 26, 2016), *available at* https://perma.cc/S7RS-8VXT. Other video games also have their own ports (e.g., Battlefield 4 is 3659), as well as specific software and cloud services, such as Dropbox (port 17500). *Id.*

[54] OTI supports the FCC's rationale for including name, address, and telephone number as PII. Subscriber lists do not exist for broadband, and therefore customers expect that information to stay private.

[55] Arvind Narayanan, Johanna Huey, & Edward W. Felten, *A Precautionary Approach to Big Data Privacy* 5 (Mar. 15, 2015), http://randomwalker.info/publications/precautionary.pdf (Narayanan *et al.*, *Precautionary Approach*).

[56] *See* Michael Barbaro and Tom Zeller, Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, New York Times (Aug. 9, 2006), http://www.nytimes.com/2006/08/09/technology/09aol.html.

[57] Ratan Dey, Yuan Ding, and Keith W. Ross, *The High-School Profiling Attack: How Online Privacy Laws Can Actually Increase Minors' Risk* 1 (2013), https://www.petsymposium.org/2013/papers/dey-profiling.pdf.

[58] Melissa Gymrek et al., *Identifying Personal Genomes by Surname Inference*, 339 Science 321, 321-24 (2013).

[59] Philippe Golle & Kurt Partridge, *On the Anonymity of Home/Work Location Pairs,* Pervasive Computing, Seventh International Conference, Nara Japan (May 11-14, 2009), *available at* https://crypto.stanford.edu/~pgolle/papers/commute.pdf.

could all be used to specifically identify individuals.[61] Thus, even with the best intentions of those releasing data, re-identification can pose problems for subjects of the datasets. The FCC's rule should protect against that risk.

The list of PII data points proposed in the Notice is comprehensive and should be adopted. However, some data points should be explained further to ensure both BIAS providers and the public know what is protected by the customer PI rules. For instance, what does the FCC consider "other online contact information"? Would this include any username for any website that allows for contact with the customer? Or does it include only usernames on communications platforms? What does the FCC consider a "persistent online identifier" other than unique cookies? Also, what is included in "information relating to family members"? Does that mean PII related to family members, or something different? Answers to these questions will be important to ensure BIAS providers do not experiment with what constitutes PII.

Last, customer PI should remain an open category. As BIAS providers further develop their services, new types of data may need to be categorized as CPNI or PII, and thus will merit protection under the FCC's scheme. This is particularly relevant for "linkable" data, because whether data is "linkable" to a customer may change over time depending on the availability of other datasets or developments in data science. Thus, the FCC should consider future requests from the public to redefine certain data as customer PI.

(footnote continued)

[60] Vijay Pandurangan, *On Taxis and Rainbows: Lessons from NYC's improperly anonymized taxi logs*, Medium (June 21, 2014), https://medium.com/@vijayp/of-taxis-and-rainbows-f6bc289679a1.

[61] Narayanan, *et al.*, *Precautionary Approach*.

4. Any use or disclosure of content of communications must be with opt-in consent

The FCC seeks comment on how to treat the content of customer communications.[62] Any use or disclosure of the content of communications of customers by BIAS providers, including by or with affiliates, should be done only with express, opt-in consent. Section 705 of the Communications Act expressly states "no person . . . transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception . . . ." This special protection of content should be honored through the broadband privacy rules promulgated pursuant to this rulemaking.

Relatedly, the FCC should recognize packet contents as communications contents. The proposal seeks comment on "whether the use of [deep packet inspection "DPI"] for purposes other than providing broadband services, and reasonable management thereof, should be prohibited or otherwise subject to a heightened approval framework."[63] It should. DPI can reveal extremely sensitive information about BIAS customers' online activities and communications, including content. Recognizing packet contents as communications contents, and establishing an opt-in standard for content, would honor BIAS customers' reasonable expectation that their provider is not inspecting their traffic for purposes other than to provide service.

---

[62] NPRM, at ¶ 67.
[63] NPRM, at ¶ 264.

5. OTI supports the proposed definitions of opt-in and opt-out, but the FCC should not remove the waiting period for opt-out

OTI supports the definitions for opt-out and opt-in. However, OTI does not support the FCC's proposal to eliminate the 30-day waiting rule for opt-out approval.

Opt-out approval should not be instant. There are many factors a customer may consider in deciding whether to allow a BIAS provider to use information in certain ways, in addition to simply needing time to read the notice provided by the BIAS provider. Customers may not (likely will not) know immediately whether they want the BIAS provider to, for instance, share data with affiliates for the purpose of advertising—it may take a few days to express a negative decision. The FCC's proposal does not take this lag time into account. This problem arises in part because, for any opt-out use, the proposal allows the BIAS provider to simultaneously send the notice to the customer and begin using and disclosing the data at issue. There would likely be no recourse for the customer to have the shared information deleted if they later decided to opt out of the sharing. The damage will have been done. While a 30-day waiting period may not be the appropriate length, the FCC should impose a seven calendar day waiting period to recognize that customers may need time to decide whether to opt out of certain data uses.

6. The FCC should adopt a cabined definition of "communications-related services" with procedural safeguards to create opportunities for public engagement in the event the category is broadened over time

The FCC seeks comment on how best to define "communications-related services."[64] OTI supports a definition of communications-related services that is limited to telecommunications, cable, and satellite services regulated by the FCC.

As an initial matter, the FCC should not carry over the definition of communications-related services from its current Section 222 rules, under which the category is defined as "telecommunications services, information services typically provided by telecommunications carriers, and services related to the provision or maintenance of customer premises equipment." This definition would be ill-suited to the broadband privacy context because it is too ambiguous to be useful, and because it could expand over time—without any meaningful input from the public—to include services that have nothing to do with BIAS provision and that raise competitive concerns.

On the first point, it is difficult even for communications and privacy lawyers to understand with any clarity what services are information services "typically" provided by BIAS providers, and not "retail consumer services provided using Internet Web sites." In the phone context, voicemail is an easy example of an information service typically provided by phone service providers; analogously, email might be an example of an information service typically provided by BIAS providers. But what of an information service that a BIAS provider charges extra for, that is available both via an app on a connected device and via a browser-

[64] NPRM, at ¶ 71.

accessible web portal? It is not clear whether such a service would be considered to be "provided using Internet Web sites" or not. Nor would it be easily ascertainable when a type of service that is increasing in its availability crosses the line into the "typically provided" category.

Relatedly, it would be problematic to allow a newly developing type of service to cross that line and become classified as a communications-related service without any meaningful opportunity for public engagement and consultation. A service that is not communications-related one day, and for which use of CPNI to advertise therefore is subject to an opt-in standard, could the very next day be communications-related, subject to the opt-out standard. This would violate consumer expectations. It also could raise competitive concerns, as BIAS providers presumably would have much greater freedom to leverage CPNI to boost marketing even of information services that come to be "typically" provided by BIAS providers but that really have nothing to do with BIAS.[65]

A better approach would be to define the category as telecommunications, cable, and satellite services regulated by the FCC. This approach would clarify the boundaries of the category, improving consumers', advocates', and BIAS providers' understanding of where the line is to be drawn between opt-in and opt-out notice

[65] For example, if the vast majority of BIAS providers eventually offer their own over-the-top streaming video services, they could leverage CPNI to gain an anticompetitive advantage over streaming video services unaffiliated with BIAS providers. By analyzing information about its customers' application usage, traffic statistics, traffic destination, and browsing patterns, a BIAS provider could deduce with high confidence virtually everything there is to know about what streaming video service(s) its customers currently use, what its customers like to watch, and how, when, and where they like to watch it. The BIAS provider could then use that information to power highly targeted marketing practices designed to steal customers away from other streaming video services.

standards. By creating clear boundaries for the category, this definition would also establish a requirement that the FCC conduct a rulemaking before broadening the category, ensuring stakeholders would have a procedural opportunity to weigh in at that time. Finally, limiting the category to services regulated by the FCC would ensure that even if it allowed the lower opt-out consent standard to apply to the use of CPNI for services that are not BIAS but that are communications-related, the FCC would retain close regulatory oversight over downstream uses permitted under the opt-out standard.

7. Section 222 protects the aggregate information of CPNI only, and it does not make sense to allow BIAS providers to attempt to aggregate PII

In general, OTI supports the definition of aggregate information as proposed in the Notice because it tracks with the statutory language in Sections 222(c)(3) and 222(h)(2). However, the rule should be strictly limited to aggregate CPNI; it should require opt-in consent for the use of aggregate PII.

The FCC proposes to treat de-identified, but non-collective CPNI as individually identifiable CPNI, rather than allowing such data to fall under the exception for use and disclosure of aggregate customer data.[66] OTI agrees. Indeed, OTI was signatory to the 2013 Petition for Declaratory Ruling on this very question.[67] Aggregate information is defined by the statute to include two elements, (1) "collective data that relates to a group or category of services or customers" and

[66] NPRM, at ¶ 165.
[67] Petition of Public Knowledge *et al.* for Declaratory Ruling Stating that the Sale of Non-Aggregate Call Records by Telecommunications Providers without Customers' Consent Violates Section 222 of the Communications Act., WC Docket No. 13-306 (filed Dec. 11, 2013); NPRM, at ¶ 165.

(2) "from which individual customer identities and characteristics have been removed."[68] If a BIAS provider seeks to make use of data as "aggregate" data, then the information must be both collective and de-identified. Any data not meeting both requirements is not "aggregate."

The FCC's proposed definition of aggregate customer PI is at odds with its definition of PII. The Notice proposes to define aggregate customer PI as "collective data that relates to a group or category of services or customers, *from which individual customer identities and characteristics have been removed*."[69] The proposed rule further states "[a] BIAS provider may use, disclose, and permit access to aggregate customer PI . . . if the BIAS provider . . . determines that the aggregated customer PI *is not reasonably linkable* to the specific individual" or device.[70] In another portion of the Notice, the FCC proposes to define "personally identifiable information" as any data that is "linked or linkable" to an individual.[71] Therefore, the proposed rule allows BIAS providers to aggregate customer PI, which includes PII, but then requires the BIAS provider to remove PII from the aggregate data because PII is, by definition, linkable to an individual or device. Rather than allow BIAS providers to experiment with whether they can find a type of PII that can be aggregated under the rule, the FCC should narrow the definition of aggregate customer PI to aggregate CPNI only.

---

[68] 47 USC § 222(h)(2).
[69] NPRM, at ¶ 74 (emphasis added).
[70] NPRM, at Appendix A, 64.7002(g) (emphasis added); *Id*. at ¶ 157.
[71] NPRM, ¶ at 61.

8. The FCC should adopt a definition of "breach" that includes both unintentional breaches and breaches of customer PI

OTI supports the FCC's proposed definition of "breach." In particular, OTI urges the FCC to move forward with adoption of a definition that includes both unintentional breaches and breaches of customer PI.

The definition of "breach" should, as the FCC proposes, classify accidental security failures as breaches. This approach is necessary for at least four reasons. First, consumers may need to take action to protect themselves against inadvertent breaches of private information, which could harm consumers just as much as intentional breaches. For example, in the event that an agent of a BIAS provider accidentally distributed covered information to multiple parties (for example, by email), neither the distribution nor the access would be intentional, but one of the recipient parties could nevertheless use the breached information in harmful ways, or further share it with additional unauthorized parties.[72]

Second, many breaches go undetected, and therefore in many instances a discovered security failure may not in fact be the first failure of its kind. This year's *Data Breach Investigations Report*, published by Verizon based on information about tens of thousands of data breaches suffered across several industries, reports

[72] In February 2016, the State of California reviewed reported data breaches from between 2012 and 2015. It found that of all breaches caused by "error" by employees or agents, 46 percent were "misdelivery" of data (sent to unintended recipient), and 35 percent were unintentionally displaying data on a public website. Kamala Harris, California Data Breach Report, Cal. Dept. of Justice (Feb. 2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf ("California Data Breach Report").

that the average time between breach and detection is growing.[73] According to Neal O'Farrell, the founder of security firm Privide, even relatively sophisticated large firms are often unaware they have suffered a breach until they begin to see compromised data appear on the black market.[74] In the words of O'Farrell, "hackers don't leave traces."[75] Because there is often a time gap between a breach incident and discovery of the breach—some breaches are never discovered at all—many detected breaches cannot be presumed to be the only or the first of their nature. Thus if an accidental breach is discovered, there is a possibility that a malicious breach took place as well.

Third, although breach notification is most often promoted as a useful way to encourage customers to take extra precautions to protect themselves from possible harmful misuses of breached data at times when the risk of such misuse is high, breach notification serves another, equally important purpose: it drives covered entities to improve their data security practices so that they may avoid the reputational harm that results from a breach. A security failure that results in an accidental breach of customers' private information is a security failure nevertheless. Defining "breach" to include such accidents, and consequently forcing BIAS providers to notify their customers and suffer the reputational

---

[73] Verizon, *2016 Data Breach Investigations Report* 10 (2016), http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/ ("The bad news is, the detection deficit . . . is getting worse.").
[74] Megon Leonhardt, *Cybersecurity Breaches Not Rare, Just Undetected*, WealthManagement.com (Sept. 11, 2014), http://wealthmanagement.com/technology/cybersecurity-breaches-not-rare-just-undetected.
[75] *Id.*

consequences when such accidents occur, will help ensure that BIAS providers adopt data security best practices.

Fourth, as the FCC oversees BIAS providers' privacy and security practices, it will need to be aware of security vulnerabilities and security and privacy failures so that it can monitor industry practices, identify struggling actors, and work with BIAS providers to improve practices over time. If, in contrast, the FCC were to adopt a definition of "breach" that omitted inadvertent security failures, the FCC would not be notified of those failures, and its ability to effectively guide providers and enforce the rules would be diminished accordingly.

The definition of breach must also, as the FCC proposes, include customer proprietary information. Customer proprietary information, such as financial details included in applications for Lifeline service, can include highly sensitive information that must be adequately protected. The FCC seeks comment on its "authority to extend [its] proposed breach reporting requirements to breaches of all customer PI," and it unquestionably has this authority. Section 222(a), from which the FCC's general Title II privacy authority issues, explicitly places on telecommunications carriers "a duty to protect the confidentiality" of customer proprietary information.[76] There could scarcely be a plainer meaning of this language than that it requires carriers to undertake measures to secure private information—a requirement the FCC is empowered to oversee.

[76] 47 USC § 222(a).

B. Meaningful notice of privacy protections requires informing customers of specific privacy practices, and making the opt-in/opt-out process simple and easy

OTI supports the FCC's proposal regarding privacy notices. The FCC recognizes that transparency is crucially important and that there is widespread agreement that privacy policies should be clear, conspicuous, and understandable.[77] Unfortunately for consumers, companies continue to have unclear and inconspicuous privacy policies,[78] or fail to follow the policies they provide.[79] While the proposed rule will address some of these issues, there are several areas in which the Notice can be improved.

1. The proposed categories of information that must be disclosed in privacy notices should require more detail

The FCC proposes to require specific disclosures in privacy policies. There are four categories of information that must be disclosed, each has strengths and weaknesses.

---

[77] NPRM, at ¶ 82.

[78] *See* Ranking Digital Rights, 2015 Corporate Accounability Index 3 (2015), https://rankingdigitalrights.org/index2015/assets/static/download/RDR-4pager.pdf ("Disclosure about collection, use, sharing, and retention of user information is poor. Even companies that make efforts to publish such information still fail to communicate clearly with users about what is collected about them, with whom it is shared, under what circumstances, and how long the information is kept."); *see also 2015 Corporate Accountability Index: Privacy*, Ranking Digital Rights, https://rankingdigitalrights.org/index2015/categories/privacy/ (last visited May 24, 2016).

[79] *See* FTC, Privacy & Data Security Update: 2015 2-4 (2016), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2015/privacy_and_security_data_update_2015-web_0.pdf (listing the various privacy policy violations by companies in 2015).

The first category is "types of customer PI collected and how they are used and disclosed."[80] This category requires BIAS providers to disclose the types of customer PI the BIAS provider collects through its broadband service, how the BIAS provider uses, and under what circumstances it discloses, each type of customer PI that it collects, and the categories of entities that will receive customer PI and the purposes for which the customer PI will be used. These specific disclosures will help customers understand how their data will be used by the BIAS provider. However, the FCC should ensure that BIAS providers are disclosing the practices they actually undertake, rather than a list of actions the BIAS provider "may" undertake. Disclosing a series of actions the provider "may" undertake is not helpful for customers to make informed decisions about data use and disclosure. Moreover, BIAS providers should disclose more than simply the "categories of entities" that will receive customer PI. They should have to disclose the entities to which they actually sell, so customers can make an informed decision about whether to opt-in or opt-out.[81] These disclosures should be easy to read, for instance using a bulleted list.

The second category is "customer rights with respect to their PI."[82] This category requires BIAS providers to inform customers of their ability to opt-in or opt-out, that their decision does not affect their quality of service, and that the

---

[80] NPRM, at ¶ 83.

[81] Under the current proposal, a BIAS provider could simply claim they sell to "advertisers" for "advertising," but this does not give the customer much of an understanding of how their data will be used or who will be buying it. Additionally, different advertising companies may handle data differently, and a customer should be aware of that to be able to make a more informed determination.

[82] NPRM, at ¶ 83.

decision applies until the customer changes his or her mind. The FCC should ensure that this notice is at the beginning and the end of the privacy notice, or is made conspicuous through another mechanism that is obvious and apparent to the customer to increase the chance that customers will read and understand that portion of the notice.

The third category is "requirements intended to increase transparency of privacy notices."[83] This category is designed to ensure BIAS providers take certain steps to ensure readability of the privacy policy. The FCC should make clear it will enforce this provision if inadequate privacy policies are brought to its attention. For instance, sites that incorporate endless scrolling make it extraordinarily difficult for users to find privacy policies.[84] If BIAS providers use that type of website, they should have to disclose their privacy policies at the top of their site or in another prominent area of the site.

The fourth category is "timing of notice."[85] This category requires BIAS providers to provide privacy notices before a customer purchases broadband and requires the policy to be persistently available online. This category should also include that the notice should be provided to customers when the BIAS provider first intends to make use of or disclose the data, when it seeks the opt-in or opt-out consent as discussed in paragraph 140 of the Notice. Additionally, the FCC should require BIAS providers to send a yearly reminder to customers about the opt-in/opt-

---

[83] NPRM, at ¶ 83.
[84] Armen Ghazarian, Infinite Scrolling: Is It Good or Bad for Your Website?, Designmodo (Mar. 6, 2014), http://designmodo.com/infinite-scrolling/ (describing the "footer problem").
[85] NPRM, at ¶ 83.

out choices the customer has made.[86] This would provide a useful opportunity for customers to rethink their decisions on a regular basis. Last, the BIAS provider should inform the customer, through its privacy notice, of these multiple opportunities to review the privacy policy and change their mind.

2. The FCC should require other data practices to be disclosed as well and should adopt the "consumer-facing privacy dashboard"

The proposed categories do not include everything that would be relevant for customers to make an informed choice. Data security practices should also be disclosed. Customers may even be comforted by a BIAS provider that takes proactive steps to protect data and reduce security risks, and customers should be so informed.

Data retention and deletion policies are also important to customers and should be disclosed. The amount of time a BIAS provider may retain data, or when the data will be deleted, will likely factor into the decision of whether to allow BIAS providers to disclose or allow access to their data. There may be less risk to the customer if data will be deleted after, for instance, one year, as opposed to being retained (and thus used and disclosed to third parties) indefinitely.

The FCC should also require BIAS providers to provide an easy mechanism for customers to ask for disclosure of the customer PI the provider has collected regarding that customer. This functionality is required by Section 222(c)(2), but it

[86] These notices should be sent to *all* users, not just those that have opted out of certain data uses and disclosures.

should be made part of the customer portal.[87] Being able to see what data the provider has collected will be extremely important for customers to make their decisions about whether to opt in or opt out. If the BIAS provider has more information about the customer than the customer is comfortable sharing with third parties or having used in various ways, then that customer may decide not to allow the BIAS provider to engage in those activities. It is impossible for a customer to make a truly informed decision about opting in or out when he or she does not know what information the BIAS provider actually has.

Last, all of this privacy-related information should be presented in a simple, easy-to-read interface. OTI supports the FCC's proposed "consumer-facing privacy dashboard" that would consolidate all privacy-related information and allow customers to control all of their data decisions in one place.[88] The dashboard would also provide BIAS providers a mechanism for informing customers in advance of when privacy policies change in a material way.[89]

C. Customers must be able to choose how BIAS providers use their data, and the default must be opt-in consent in most, if not all, circumstances

It is important the FCC allow customers to choose how BIAS providers use and disclose their data. Opt-in consent is the most important mechanism for ensuring customers give consent to a provider's data practices. It is the centerpiece

---

[87] "A telecommunications carrier shall disclose CPNI, upon affirmative written request by the customer, to any person designated by the customer." 47 USC § 222(c)(2). The customer can and should designate him or herself as the person to receive the customer data.
[88] NPRM, at ¶ 95.
[89] *Id.* at ¶¶ *96-97*.

of this proposal and the FCC should reject calls to change its opt-in regime to an opt-out regime. In addition, the FCC should strengthen some of the aspects of the rule that are less protective of customers' data.

1. The FCC's proposal for implied consent for use of data for marketing purposes is unlawful

The FCC's proposed "implied consent" category includes certain uses that are unlawful under Section 222.[90] In the Notice, the FCC takes a broad interpretation of Section 222 and its exceptions. Section 222(c)(1) allows a BIAS provider to "use, disclose, or permit access to individually identifiable [CPNI] in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service." The FCC interprets that language to allow BIAS providers to use all customer PI to market additional broadband offerings in the same category of service (a term which is itself unclear) without "customer approval."[91]

Section 222(c)(1) does not extend to marketing uses of customer PI. As an initial matter, the statute allows only very narrow uses of CPNI without "approval of the customer."[92] In this instance, the FCC has explicitly stated it would not require customer approval. Thus, the use must be contemplated by Section 222(c)(1) or must fall under an exception under Section 222(d). There is no exception for marketing under Section 222(d), so it would have to fit into either

[90] *Id*. at ¶¶ 111-121.
[91] *Id*. at ¶ 111
[92] 47 USC § 222(c)(1).

"services necessary to" or services "used in" the provision of a telecommunications service. Neither applies. Marketing is not a service "necessary to" the provision of telecommunications service. The telecommunications service provided by a BIAS provider is *access* to the Internet. A BIAS provider need not market its services to physically provide access to the Internet to that customer. Further, marketing is not a service "used in" providing physical access to the Internet either, it is a separate part of the business. Thus, implied consent for marketing purposes is unlawful under the statute.[93]

2. The FCC should not extend the statutory exceptions beyond CPNI unless there is a specific reason for doing so

In the Notice, the FCC proposes to expand all of the statutory exceptions to Section 222 to cover customer PI, not just CPNI.[94] But the FCC should not extend coverage of these exceptions to customer PI unless, in each case, there is a persuasive reason for excepting PII. PII encompasses a broad category of information that is linked or linkable to a customer, including name, address, Social Security number, date and place of birth, mother's maiden name, phone numbers, Internet browsing history, financial information, shopping records, medical and health information, race, religion, sexual identity or orientation, and a variety of other data points. Many of these will not be useful for specific exceptions. Expanding the exceptions may therefore only harm customers by increasing the number of people who have access to the information and increasing the chance of

[93] 47 CFR § 64.2005 has a similar implied consent rule for telephone CPNI, which the FCC should also amend as it is also unlawful.
[94] NPRM, at ¶ 115.

breach, identity theft, or other harm. If BIAS providers believe they need to disclose PII for these reasons, then it is incumbent upon them to persuade the public why.

3. The FCC should favor opt-in consent over opt-out in as many circumstances as possible because the statute requires customer "approval"

The Notice proposes specific circumstances where opt-out is appropriate, rather than opt-in. Specifically, BIAS providers can seek opt-out consent in narrow circumstances: when using data, or sharing data with communications-related affiliates, for marketing of communications-related services to that customer.[95] All other uses and disclosure of, and access to, data require opt-in consent.[96]

The FCC should consider requiring opt-in for all data use, disclosure, and access practices other than those undertaken to provide service. Section 222(c) states telecommunications service providers shall not use CPNI "[e]xcept … with the approval of the customer."[97] The FCC should interpret "the approval of the customer" by its plain meaning, and require some active consent to the provider's data practices. Providing notice that a customer may or may not read and then assuming silence is consent does not comport with the plain meaning of the statute.

---

[95] NPRM, at ¶ 122.
[96] *Id*. at ¶ 127.
[97] 47 USC § 222(c)(1).

4. The rule should give customers multiple opportunities to opt into certain data use and disclosure practices

The Notice proposes to require notice of use and disclosure practices at the point of sale, and again when the BIAS provider first intends to use or disclose that data in a manner requiring customer approval, and requires privacy policies to be persistently available to customers through a link on their homepage.[98] OTI supports this proposal.

Providing customers multiple opportunities to decide whether to opt into or out of a particular practice is a good policy. First, consumers generally cannot adequately account for privacy harms that result from information disclosure far in the future.[99] Second, circumstances may have changed, particularly if customers can access the information BIAS providers have collected about them. Third, customers are bombarded with information from their BIAS providers when they first sign up for service, and switching services often coincides with moving homes, a stressful event itself. Customers may make hasty decisions in the moment simply to obtain Internet access. Customers may therefore appreciate the reminder that they have the opportunity to change their mind.

---

[98] NPRM, at ¶¶ 87, 140.

[99] *See* Daniel Solove, *Why the Law Often Doesn't Recognize Privacy and Data Security Harms*, TeachPrivacy (July 9, 2014), https://www.teachprivacy.com/law-often-doesnt-recognize-privacy-data-security-harms/ ("harm from privacy and data security violations may occur long after the violation. If data was leaked, an identity theft might occur years later, and a concrete injury might not materialize until after the statute of limitations has run.").

D. Customer data must be secure

Data breaches are a common part of people's lives. According to the Privacy Rights Clearinghouse, there have been 3,126 data breaches since 2010 (approximately 1.5 data breaches per day).[100] However, BIAS providers have a special duty under Section 222(a) to "protect the confidentiality of proprietary information of . . . customers." Failing to take precautions against data breaches clearly violates that duty. Given BIAS providers' special relationship to their customers, and their ability to see a broad scope of information that travels over their networks, OTI supports the FCC's proposed procedural requirements to help prevent data breaches.

BIAS providers should also have to encrypt their data at rest and, when applicable, in transit. The FCC has recognized the importance of encryption in previous enforcement actions. In its Notice of Apparent Liability against TerraCom and YourTel America, the FCC concluded that "the lack of encryption clearly evidences the unjust and unreasonable nature of the Companies' data security practices."[101] The FCC should require encryption of customer data because failing to use encryption to protect private information is unjust and unreasonable, and puts customers at unnecessary risk of data breaches.

---

[100] *Chronology of Data Breaches, Security Breaches 2005–Present*, Privacy Rights Clearinghouse, https://www.privacyrights.org/data-breach (last visited May 27, 2016). These breaches occurred despite FTC guidance on data security practices. *See, e.g.*, Fed. Trade Comm'n, *Start with Security: A Guide for Business* 1 (2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

[101] *TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13331 ¶ 32 (2014).

E. Data breach notification should be mandatory for all BIAS providers and should follow the timeline proposed in the notice

OTI supports the data breach notification timetables proposed in the Notice and the specific breach notification content requirements.[102] Further, the FCC should not employ certain mechanisms it seeks comment on in the Notice.

The FCC should not employ any of the various triggers it proposes.[103] BIAS providers should not be making independent decisions about whether to notify their customers based on any perceived potential future harm or based on some specific type of potential future harm. This needlessly complicates a straightforward requirement: if a BIAS provider experiences a data breach, it should notify its customers because customers own the data and need to be able to make an informed decision about how to respond. If, for instance, a data breach occurs because of an employee mistake or some other seemingly innocuous circumstance, then the provider can explain that to the customer and let the customer decide how to handle responding. A BIAS provider should not be able to decide, based on its own judgment of harm, that it need not inform the customer of a breach. This prevents customers from protecting themselves if they feel it is appropriate. By allowing BIAS providers to keep some breaches out of the public eye, this also unnecessarily insulates BIAS providers from the negative consequences that otherwise stem from breaches and serve as an important disincentive to practice lax security.

---

[102] NPRM, at ¶¶ 234, 243.
[103] *Id*. at ¶¶ 237-38.

BIAS providers should also notify customers under the timetables proposed, not "without unreasonable delay" or as "expeditiously as possible."[104] Such unclear and flexible deadlines, again, would increase the likelihood of harm to customers and complicate a straightforward requirement that is not unduly burdensome.

F. Other coercive practices should be banned or should require opt-in consent from the customer

The FCC seeks comment on, but does not propose to ban or restrict, a series of practices that implicate privacy. The FCC should take action with respect to the following practices.

1. Service offers conditioned on the waiver of privacy rights should be strictly prohibited

The Notice proposes to prohibit BIAS providers from making service offers contingent on customers waiving their privacy rights.[105] OTI supports this proposal. However, the FCC needs to clarify what a "service offer" entails. Without a clear definition, BIAS providers will easily circumvent this prohibition by taking a broad interpretation and making all but one of their service offers contingent on waiving privacy rights, while the one offer with strong privacy protections could be prohibitively expensive. This circumvention should not be allowed. To define service offer, the FCC should follow the Open Internet Order, which states

[104] *Id.* at ¶ 241.
[105] *Id.* at ¶ 258.

> [f]ixed and mobile broadband Internet access service providers also price and differentiate their *service offerings* on the basis of the quality and quantity of data transmission the offering provides. AT&T U-Verse, for instance, offers four "Internet Package[s]" at different price points, differentiated in terms of the "Downstream Speeds" they provide. On the mobile side, monthly data allowances—i.e., caps on the amount of data a user may transmit to and from Internet endpoints—are among the features that factor most heavily in the pricing of service plans.[106]

Based on the above language, one potential definition for "service offer" is an offer for Internet access at substantially the same performance characteristics and commercial terms. In that case, the FCC's rule could build a definition of "service offer" based off the enhanced transparency provisions of the Open Internet Order, and require that each particular combination of performance characteristics, network practices, and commercial terms that a BIAS provider offers must be available with all privacy options. This would allow customers to have choices regarding which services to purchase without having to give up their privacy entirely.

---

[106] *In the Matter of Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC 5601, 5756 ¶ 353 (2015) ("2015 Open Internet Order")(emphasis added).

2. Pay-for-privacy regimes should be prohibited

Pay-for-privacy regimes are deeply problematic. BIAS providers have already begun experimenting with these plans. AT&T has its "GigaPower" plan,[107] and Verizon has its "Verizon Selects" plan, which provides the customer "points" for allowing Verizon to collect all kinds of data about him or her.[108] These programs are concerning because they could be crafted to induce or, worse, coerce customers into giving up privacy protections all so BIAS providers can further develop their advertising businesses. These programs are not appropriate in an era when customers are increasingly concerned about privacy.

3. Persistent tracking technologies injected at the network level should be prohibited

The FCC seeks comment on how to treat persistent tracking technologies, like UIDH headers (the Verizon "Supercookie") and similar technologies. Persistent identifiers injected at the network level, such as UIDH headers, should be prohibited. Such technologies can facilitate collection of extensive information about BIAS customers without customers' knowledge, and are not easily defeated by customers. Worse, unlike information that customers must provide so that BIAS providers can route their broadband traffic, persistent trackers injected at the

---

[107] NPRM, at ¶ 259.

[108] Verizon Selects FAQ, Verizon Wireless, https://www.verizonwireless.com/support/verizon-selects-faqs/ (in exchange for tracking a customer's every move online, the customer receives "an extra 2,500 Verizon Smart Rewards bonus points when you first join the program and another 500 points every month for each eligible line on your account that is part of Verizon Selects," which can be used to redeem rewards through "Smart Rewards," Verizon's version of a credit card rewards program).

network level are not necessary to provide the service. And particularly problematic is the fact that these technologies introduce new privacy and security threats. For example, in the midst of the controversy surrounding the UIDH header, Verizon asserted that it introduced the UIDH header only to power its own advertising platform. That the technology turned out to be trackable by third parties, who were able to use it to collect information about Verizon customers' browsing habits, was reportedly unintentional on the part of Verizon.[109]

Persistent tracking technologies injected by BIAS providers at the network level are unjust and unreasonable practices, and should be prohibited.

4. Forced arbitration should be prohibited

One of the central principles of this proposal is consumer choice. The Notice makes repeated reference to enabling customers to choose how BIAS providers may use their data and ensuring that customers are informed about data practices. Forced arbitration clauses fly in the face of this principle. It would be incongruous to give consumers so much control over their data, only to have disputes about misuse of that data end up in forced arbitration, which so heavily favors the companies who hire the arbitrators. Real justice does not occur in arbitration.[110] But in a court or at the FCC, consumers may find adequate enforcement and protection. Thus, forced arbitration clauses should not be allowed.

---

[109] *See* Julia Angwin & Jeff Larson, *Somebody's Already Using Verizon's ID to Track Users*, ProPublica (Oct. 30, 2014), https://www.propublica.org/article/somebodys-already-using-verizons-id-to-track-users.

[110] Peter Schroeder, *Consumer Bureau: Forced Arbitration a Bad Deal for Consumers*, The Hill (Mar. 10, 2015), http://thehill.com/policy/finance/235195-consumer-bureau-forced-arbitration-a-bad-deal-for-consumers.

Further, the FCC should ensure that there is an easy and clear process for consumer complaints at the FCC.[111] This, along with prohibiting forced arbitration, will ensure customers have proper avenues of redress for privacy violations.

CONCLUSION

OTI supports the FCC's Notice. It is a strong proposal that, if adopted, will finally provide some transparency, choice, and security to the private information that BIAS customers have no choice but to provide in order to receive service. The FCC should move swiftly to adopt rules that improve consumer privacy protections in the BIAS context and improve clarity for consumers, advocates, and BIAS providers alike.

/s/
Laura M. Moy, Esq.

Institute for Public Representation
Georgetown Law
600 New Jersey Avenue, NW
Suite 312
Washington, DC 20001
(202) 662-9547

Counsel for New America's Open Technology Institute

/s/
Eric G. Null, Esq.

Sarah J. Morris, Esq.
Emily Hong

New America's Open Technology Institute
740 15th St, NW
Suite 900
Washington, DC 20005

Filed May 27, 2016

[111] OTI Report, at 7.