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

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

OPPOSITION OF THE CENTER FOR DEMOCRACY & TECHNOLOGY TO PETITIONS FOR RECONSIDERATION

Natasha Duarte
Chris Calabrese
Michelle De Mooy

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

March 6, 2017

Summary

Pursuant to Section 1.429(f) of the Commission's rules,[1] the Center for Democracy & Technology ("CDT")[2] respectfully submits this Opposition to the Petitions for Reconsideration regarding the Commission's 2016 broadband privacy order.[3] Specifically, CDT opposes Petitioners' efforts to reverse the broadband privacy rules entirely, to weaken the rules' notice and consent requirements, to narrow the scope of information covered under the rules, to narrow the scope of information considered "sensitive" under the rules, to weaken the data security and data breach notification requirements, and to eliminate or weaken the rules governing "pay-for-privacy" offers. Petitioners fail to raise new arguments or facts to support their positions that the Commission should reverse or significantly weaken the broadband privacy rules. The petitions simply rehash arguments that have been fully considered by the Commission in this proceeding.

The broadband privacy rules give customers meaningful control over their information, as well as critical data security protections, while maintaining flexibility for providers to use customer information with consent. The rules are consistent with the Federal Trade Commission (FTC)'s privacy and data security guidance and with the FTC's comments in this proceeding. The rules also fulfill the Commission's statutory authority to ensure that common carriers protect the confidentiality of customer information. Reversing or substantially weakening the rules would harm consumers and result in uncertainty for providers.

[1] 47 C.F.R. § 1.429(f).
[2] CDT is a nonprofit public interest organization dedicated to promoting openness, innovation, privacy, and freedom online.
[3] Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, *Report and Order*, FCC 16-148 (Oct. 27, 2016) ("Report and Order").("broadband privacy rules").

Table of Contents

I. Introduction

The broadband privacy rules fulfill the Commission's Congressional mandate to ensure that common carriers protect the confidentiality of their customers' information.[4] The rules fill a critical gap in information privacy and security by extending protections to broadband internet access services (BIAS) subscribers that already exist for other common carriers.[5] The Commission is the only agency with Congressional authority to ensure that internet service providers (ISPs) protect the confidentiality of the vast amounts of data they collect as a result of providing internet access. Reversing the broadband privacy rules would create enormous uncertainty regarding privacy and security protections for the sensitive personal information broadband customers must share with their ISPs.

The Commission created a balanced set of rules that give consumers meaningful control over their personal information while maintaining flexibility for telecommunications companies to use data for improving services, crafting new technologies, and advertising. The rules, which rely on informed consent, are grounded in established notice-and-choice processes and in the language of Section 222. Petitioners' efforts to weaken the rules are not supported by the record and contradict the Commission's own guidance. They would expose internet users to unnecessary privacy and data security risks and undermine consumer trust in the broadband market.

[4] 47 U.S.C. § 222.
[5] *See* Report & Order at ¶ 39.

II. The Commission must dismiss attempts to revive arguments already addressed by the Commission in this proceeding.

Petitioners fail to raise new arguments regarding the Commission's authority to promulgate the rules at issue, the consistency of the report and order with the FTC's privacy and data security frameworks, the scope of ISPs' insight into customers' online activity, the definition of Customer Proprietary Network Information (CPNI), the de-identification requirements, the sensitivity of web browsing and app usage history, the applicability of Section 222 to first-party marketing, the data breach notification requirements, and the constitutionality of requiring consent for the use and disclosure of CPNI. The Petitions repeat arguments and facts that the Commission addressed in the report and order. The Commission's rules provide that the Commission may dismiss Petitions for Reconsideration that "rely on arguments that have been fully considered and rejected by the Commission within the same proceeding" because they "plainly do not warrant consideration."[6] The Commission should dismiss those Petitions that do not present new facts or arguments and merely attempt to revisit issues considered and resolved in the report and order.

The petitions for reconsideration offer no new facts or arguments that would support a reversal of the Commission's report and order. The Commission's rules are supported by an ample record of evidence that is not negated by the new administration's political views. The Supreme Court has recognized a presumption against "changes in current policy that are not justified by the rulemaking record."[7] The Commission should not reverse course based on a mere rehashing of arguments already thoroughly addressed in this proceeding.

---

[6] 47 C.F.R. § 1.429(l)(3).

[7] *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto Ins. Co*., 463 U.S. 29, 42 (1983). *See also Massachusetts v. EPA*, 549 U.S. 497, 533–34 (2007) (rejecting the President's political agenda as sufficient to justify the EPA's refusal to regulate greenhouse gas emissions); *Good Samaritan Hosp. v. Shalala*, 508 U.S. 402, 417 (1993) ("[T]he consistency of an agency's position is a factor in assessing the weight that position is due.").

III. The Commission has the statutory authority to promulgate privacy rules applying to broadband providers, which are common carriers under Title II of the Communications Act of 1934.

The record extensively supports the Commission's authority under Section 222 of the Communications Act of 1934[8] to promulgate privacy rules applying to all telecommunications carriers.[9] Petitioners' arguments that Section 222 applies only to voice services were thoroughly addressed and rejected by the Commission.[10] Section 222 applies generally to "telecommunications carriers,"[11] which include broadband internet access service ("BIAS") providers.[12]

The record also supports the Commission's decision to define customer proprietary information (PI) to include both customer proprietary network information (CPNI) and personally identifiable information (PII), and to update the definition of CPNI to accommodate BIAS providers.[13] Section 222(a), which states that "every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to...customers," is a general grant of authority to protect customer PI.[14] As the Commission explained in *TerraCom*, "[I]t is clear that Congress used the term 'proprietary information' broadly to encompass all types of information that should not be exposed widely to the public, whether because that information is sensitive for economic reasons or for reasons of personal privacy."[15]

---

[8] 47 U.S.C. § 222.
[9] Report & Order at ¶¶ 334–42.
[10] *Id.* at ¶¶ 336–37.
[11] 47 U.S.C. § 222(a)–(c); Report & Order at ¶ 334.
[12] *See generally* Protecting and Promoting the Open Internet, 80 Fed. Reg. 19738 (2015) ("2015 Open Internet Order").
[13] *See* Report & Order at ¶¶ 46–105, 343–367.
[14] 47 U.S.C. § 222(a); Reply Comments of the Center for Democracy & Technology, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16–106 at 18 (July 6, 2016) ("CDT Reply Comments").
[15] *TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13330 (2014) ("*TerraCom NAL*").

The Commission's interpretation of PI to include PII and the content of communications is consistent with *TerraCom*. "Protecting PII and content is at the heart of most privacy regimes," and the Commission recognized in *TerraCom* "that the Communications Act protects them as customer PI because it 'clearly encompass[es] private information that customers have an interest in protecting from public exposure.'"[16]

The Commission's updated definition of CPNI accommodates BIAS providers while remaining true to the statutory definition of CPNI.[17] Each of the examples of CPNI set forth in the Commission's non-exhaustive list[18] is a type of "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service."[19] Petitioners offer no new support for their arguments that the Commission exceeded its authority in applying Section 222 to BIAS providers or by accordingly interpreting its definitions of customer PI and CPNI.

IV. Broadband subscribers rely on the Commission to protect the privacy and security of the personal information they must disclose to their ISPs.

The Commission is the only agency with jurisdiction to protect the confidentiality of information in the hands of BIAS providers. Common carriers are exempt from the FTC's authority under Section 5 to protect against unfair and deceptive trade practices.[20] The recent Ninth Circuit panel decision in *FTC v. AT&T Mobility*[21] underscored this jurisdictional issue. The three-judge panel held that the FTC had no Section 5 authority over any company operating

[16] Report & Order at ¶ 85 (quoting *TerraCom NAL* at 13330).
[17] Report & Order at ¶¶ 47–52.
[18] Report & Order at ¶ 53.
[19] CDT Reply Comments at 18 (quoting 47 U.S.C. § 222(h)(1)).
[20] 15 U.S.C. § 45(a)(2) (exempting "common carriers subject to the Acts to regulate commerce"); 15 U.S.C. § 44 (defining "Acts to regulate commerce" as including "the Communications Act of 1934 and all Acts amendatory thereof and supplementary thereto").
[21] 835 F.3d 993 (2016).

common carrier services.[22] Section 222 of the Communications Act of 1934 requires common carriers to protect the confidentiality of their customers' information and to get customer approval before using CPNI for purposes other than providing the common carrier service.[23] But the statute itself does not provide specific guidance on the steps BIAS providers must take to comply with the law. It is up to the Commission to interpret the statute as applied to BIAS providers and subscribers so that they are not left in the dark about how ISPs can use and share customers' personal information.

Because the FTC and the FCC share jurisdiction over companies operating online, both agencies must enforce meaningful privacy and security protections in order to achieve comprehensive protection for internet users.[24] Petitioners argue that two different sets of privacy rules—one for ISPs and another for edge providers—will cause confusion.[25] However, the existence of two different, sector-specific standards for protecting internet users' privacy is inevitable under current U.S. law. Even if the report and order were rescinded or weakened, BIAS providers would remain under a statutory obligation to "protect the confidentiality" of customers' "proprietary information" and not to use or disclose it, with certain exceptions,

---

[22] *AT&T Mobility*, 835 F.3d at 1003. *See also* Harold Feld, *Understanding the Ninth Circuit's Decision in* AT&T Mobility v. FTC, PUBLIC KNOWLEDGE (Aug. 31, 2016), https://www.publicknowledge.org/news-blog/blogs/understanding-the-ninth-circuits-decision-in-att-mobility-v-ftc ("[Under *AT&T Mobility*,] once a company acquires the 'status' of a common carrier for any line of business, it becomes exempt [from Section 5] . . . . This exemption, based on the 'status' of the entity as a common carrier, applied to the entity's non-common carrier businesses as well. . . . [I]f either Congress or the courts reversed the FCC's Title II reclassification, consumers would be without any protection for either mobile broadband or DSL—both of which are offered by phone companies that have 'common carrier status' based on their voice offerings.").

[23] 47 U.S.C. § 222(a), (c).

[24] *See* Frank Pallone Jr. & Terrell McSweeny, *New Rules Intended to Protect Your Online Privacy Are Already Under Threat*, SLATE (Feb. 9, 2017), http://www.slate.com/articles/technology/future_tense/2017/02/consumer_privacy_rules_for_internet_service_providers_are_under_threat.html.

[25] *See, e.g.*, Petition for Reconsideration by the United States Telecom Association, *in the matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16–106, at 1 (2017) ("USTelecom Petition"); Petition for Reconsideration of NCTA–the Internet & Television Association, *in the matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16–106, at 2 (2017) ("NCTA Petition").

without "the approval of the customer."[26] The FCC also has the authority to enforce against "unjust or unreasonable" practices.[27] In *TerraCom*, the Commission "found that the failure to protect customers' private information was an unjust and unreasonable practice under Section 201(b)."[28] Petitioners' calls to bring ISPs and edge providers under the same privacy rules ignore the realities of statutory privacy law.

V. Reversing or substantially weakening the broadband privacy rules would subject BIAS providers and customers to harmful regulatory uncertainty.

Without clear privacy rules, ISPs would ultimately be subject to the Commission's discretion in enforcing Section 222's confidentiality requirements and Section 201(b)'s prohibition against unjust and unreasonable practices.[29] The threat of enforcement without clear guidance about what constitutes a violation could chill innovation and cause economic loss. The record supports the need for clear privacy and security guidance for both industry and consumers. As the Commission explained,

> By bolstering customer confidence in carriers' treatment of confidential customer information, we also promote the virtuous cycle of innovation in which new uses of the network lead to increased end-user demand for broadband, which drives network improvements, which in turn lead to further innovative network uses, business growth and innovation.[30]

Industry experts raised concerns about regulatory uncertainty in 2015, when the FCC in its Open Internet Order declined to extend existing voice CPNI rules to BIAS providers. Industry experts argued that subjecting providers to case-by-case enforcement of Section 222 without clear rules created "significant risks for broadband providers and their business partners, and

[26] 47 U.S.C. § 222(a), (c).
[27] 47 U.S.C. § 201(b).
[28] Report & Order at ¶ 87 (citing *TerraCom NAL*, 29 FCC Rcd at 13325, ¶ 2).
[29] *See* sources cited *supra* notes 27–28.
[30] Report & Order at ¶ 5.

uncertainty for consumers as to how customer information can be used and shared."[31] This is the same harmful uncertainty providers and customers will be left with if the FCC reverses course in this proceeding.

Far from reinventing the regulatory wheel, the report and order simply provides the clarity and uniform standards that ISPs need in order to comply with statutory law and avoid unexpected enforcement actions. Without clear guidance, providers' obligations and customers' rights under Section 222 would be undefined, causing unnecessary confusion and expenses for all parties.

VI. The FCC's rules facilitate the consumer trust necessary for a healthy broadband market

Strong privacy rules are justified in the broadband context because of the special access to sensitive information ISPs enjoy.[32] The internet is a public necessity, and most Americans must choose among a very small number of broadband providers serving their area.[33] In order to access the internet, customers have no choice but to disclose large amounts of personal information, including browsing history and location information, to their ISPs.[34] This relationship demands an especially high degree of trust on the part of customers that ISPs will not misuse their information. This trust must be backed up by clear and meaningful privacy and data security protections.

---

[31] Marty Stern, Sam Castic, & Christian Dippon, *FCC Open Internet Order Creates Uncertainty and Risk*, CORPORATE COUNSEL (July 27, 2015), http://www.nera.com/content/dam/nera/publications/2015/016071507K&L_unlocked.pdf.

[32] Report & Order at ¶¶ 28–37.

[33] *See* DAVID N. BEEDE, U.S. DEP'T OF COMMERCE, COMPETITION AMONG U.S. BROADBAND SERVICE PROVIDERS (Dec. 2014) ("[As of 2013], only 37 percent of the population had a choice of two or more providers at speeds of 25 Mbps or greater . . ."); Report & Order at ¶ 36.

[34] *See* Report & Order at ¶¶ 28–35; AARON RIEKE, DAVID ROBINSON & HARLAN YU, WHAT ISPS CAN SEE: CLARIFYING THE TECHNICAL LANDSCAPE OF THE BROADBAND PRIVACY DEBATE, UPTURN (March 2016), https://www.teamupturn.com/static/reports/2016/what-isps-can-see/files/Upturn%20-%20What%20ISPs%20Can%20See%20v.1.0.pdf. ("Upturn White Paper").

ISPs have a broad window into their customers' online activities.[35] As the Commission put it, "the BIAS provider is the on-ramp to the internet for the subscriber and thus sees all domains and IP addresses the subscriber visits or apps he or she uses while using BIAS."[36] This is true despite growing use of encryption. Petitioners erroneously argue that encryption technologies effectively block ISPs from having a comprehensive view of customers' online activities.[37] While encryption is becoming widely adopted, a significant amount of internet traffic remains unencrypted, and whether traffic is encrypted or not is often not the decision of the user.[38] Moreover, the record shows that "even with encryption, by virtue of providing BIAS, BIAS providers maintain access to a significant amount of private information about their customers' online activity, including what websites a customer has visited, how long and during what hours of the day the customer visited various websites, the customer's location, and what mobile device the customer used to access those websites."[39]

A person's internet traffic—even just domain-level information—can reveal the most intimate details about his or her life. The record shows that "a user's browsing history can provide a record of her reading habits . . . as well as information about her video viewing habits, or who she communicates with via email, instant messaging, social media, and video and voice tools. . . . Browsing history can easily lead to divulging other sensitive information, such as when and with what entities she maintains financial or medical accounts, her political beliefs, or attributes like gender, age, race, income range, and employment status."[40]

---

[35] *See* sources cited *supra* note 34.
[36] Report & Order at ¶ 182.
[37] *See* NCTA Petition at 13–14; USTelecom Petition at 9–10; Petition for Reconsideration of CTIA, *in the matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16–106, at 7 (Jan. 3, 2017).
[38] *See* Report & Order at ¶ 34; Upturn White Paper at 3–6.
[39] Report & Order at ¶ 33. *See also* Upturn White Paper at 6–9.
[40] Report & Order at ¶ 183, *See also* Upturn White Paper at 7–9.

Broadband customers cannot avoid disclosing this sensitive information to their providers if they want to access the internet.[41] Moreover, because of the limited number of options in the broadband market, in many cases consumers can't shop around for the most privacy-protective ISP.[42] With so few choices regarding where to subscribe and how much private information to disclose, broadband users need choice regarding *how* their data is used in order to use BIAS services with confidence. The Commission's rules are designed to provide better notice and clear consent options so that customers won't be left in the dark about their ISPs' information practices. The rules give subscribers meaningful choice without jeopardizing the flexibility of ISPs to use data.

VII. The broadband privacy rules already give providers great leeway with respect to notice and consent mechanisms and the use of customer information for marketing.

A. The rules do not prohibit BIAS providers from using customer data for any purpose, including marketing

Petitioners argue that the report and order is too restrictive and that the Commission should adopt more flexible standards,[43] but the broadband privacy rules already incorporate a great deal of flexibility for providers. The rules do not prohibit providers from using customer data for any purpose, including marketing.[44] They simply require that providers notify their customers and get consent to use proprietary information for purposes other than providing the subscription service.[45] "Customer notification is [] among the least intrusive and most effective measures at [the Commission's] disposal for giving customers tools to make informed privacy decisions."[46] Contrary to petitioners' claims, the rules do nothing to prevent providers from

[41] Report & Order at ¶ 31.
[42] *See* sources cited *supra* note 33.
[43] *See* USTelecom Petition at 13–17; CTIA Petition at 8–11.
[44] Report & Order at ¶ 5.
[45] *Id.* at ¶¶ 5–9.
[46] *Id.* at ¶ 122.

engaging in data analytics or targeted marketing, as long as they enter into informed agreements with their customers. This flexible notice-and-choice approach is consistent with the FTC's privacy regime and with the FIPPs.[47]

B. The rules avoid imposing specific requirements on BIAS providers as to the content and format of privacy notices.

Under the rules, providers can decide the content and format of privacy notices. The Commission exercised regulatory restraint and "decline[d] to be prescriptive about either the format or specific content of privacy policy notices in order to provide flexibility to providers and to minimize the burden of compliance levied by [the] requirement."[48] To make compliance even easier, the Commission directed the Consumer Advisory Committee "to convene a multistakeholder process to develop a model privacy policy notice that will serve as [an optional] safe harbor for [the Commission's] notice requirements."[49] That process is currently underway.

Petitioners argue, without support, that the rules requiring privacy notifications at "point of sale" are "unnecessarily inflexible."[50] In fact, the record supports that point of sale is the most effective time to notify customers of data use policies and choices.[51] The moment when a subscriber is signing up and paying for service is the moment at which information and options about the ISP's use of her data are most relevant.[52] The Commission also eliminated the periodic

---

[47] *See generally, e.g.*, FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (May 2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf ("2000 FTC Privacy Report"); FEDERAL TRADE COMMISSION, 2014 PRIVACY AND DATA SECURITY UPDATE at 1 (2014), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.
[48] Report & Order at ¶ 123.
[49] *Id.*
[50] CTIA Petition at 19.
[51] Report & Order at ¶¶ 138–39.
[52] *Id.*

notice requirements from the voice CPNI rules, reducing providers' notice burdens and the potential for notice fatigue.[53]

C. The Commission adopted a sensitivity-based framework to give BIAS providers more freedom to use non-sensitive information.

The Commission revised its original NPRM to incorporate greater flexibility by requiring opt-in consent only for the use and sharing of sensitive information.[54] Petitioners asked the Commission to adopt such a sensitivity-based framework in their comments.[55] The Commission found this framework to be "more properly calibrated to customer and business expectations" and "consistent with the framework recommended by the FTC in its comments."[56] Under this framework, the notice-and-consent burden correlates with the risk to customers created by using or disclosing the information.

The Commission's sensitivity framework is not only consistent with FTC standards but also incorporates greater flexibility for providers to use non-sensitive customer information with a lower burden of approval. Opt-out consent for non-sensitive information means that consumers will have to take affirmative action to *avoid* agreeing to the use and sharing of their non-sensitive information. This approach protects consumers while giving petitioners what they asked for: rules that calibrate notice and consent burdens according to customer expectations about how ISPs use their information.

[53] *Id.* at ¶ 137.
[54] *Id.* at ¶¶ 172–76.
[55] *See, e.g.*, NCTA Comments at 3; USTelecom Comments at 23.
[56] Report & Order at ¶ 173.

D. The rules allow BIAS providers to use customer data to market certain services, including bundles, without additional consent.

The rules explicitly allow providers to use customer data to market "bundled" services without additional opt-in or opt-out consent.[57] Petitioners argue that the report and order unduly restricts the use of customer information for first-party marketing, which petitioners claim "quintessentially falls within the context of the carrier-customer relationship."[58] Petitioners cite "bundles" as the primary example of products that fall within the quintessential carrier-customer relationship.[59] In fact, the rules already allow providers to infer customers' consent to use their data for marketing "service offerings within the scope of service to which they already subscribe," including but not limited to "communications services commonly bundled together with the subscriber's telecommunications service."[60] These rules directly contradict Petitioners' false implications that first-party marketing of bundles is restricted.

E. The rules regarding financial incentives are permissive and flexible.

Petitioners mischaracterize as burdensome the Commission's rules regarding pay-for-privacy offerings, which include a flexible standard and prohibit only the most harmful and extreme practices. First, the Commission prohibits only "take-it-or-leave-it" offers, which make broadband service "contingent on customers surrendering their privacy rights."[61] Second, the rules generally allow providers to offer financial incentives in exchange for surrendering some privacy.[62] Providers offering such deals must simply provide additional notice and obtain opt-in consent, so that customers are aware of the trade-offs and the Commission may monitor these

[57] *Id.* at ¶ 204.
[58] CTIA Petition at 9.
[59] *Id.* at 11.
[60] Report & Order at ¶ 204.
[61] *Id.* at ¶¶ 294–97.
[62] *Id.* at ¶¶ 298–303.

offerings to ensure that they are not overly coercive.[63] This is exactly the type of flexible standard that petitioners asked for in their comments.[64]

F. The rules do not impinge on BIAS providers' collection of customer data or its use for providing and improving BIAS service.

At least one petitioner objected to the rules on the false grounds that they restrict ISPs' necessary collection and use of customer data to "improve network performance, or develop and provide services that are necessary to or used in the provision of telecommunications services, such as technical support for customers that encounter connection problems . . . ."[65] This plainly misunderstands the rules. The Report and Order makes it clear that BIAS providers can infer consent to use and share *all* customer PI "in order to provide the telecommunications service . . . or provide services necessary to, or used in, the provision of such telecommunications service."[66] These activities include "research to improve and protect networks or telecommunications."[67] Moreover, there are no restrictions on the collection of customer PI by BIAS providers.

VIII. The Commission's broadband privacy rules are already in harmony with the FTC's privacy and data security guidance.

Petitioners call on the Commission to harmonize the CPNI rules for BIAS providers with the FTC's privacy and data security guidance.[68] However, the report and order already mirrors the FTC's guidance and enforcement regime in many significant ways. In fact, the Commission made a large number of revisions to its original NPRM in order to harmonize the broadband

---

[63] *Id.*
[64] NCTA Comments 71-72; Ex Parte Presentation of CTIA, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16–106 (Aug. 25, 2016), 2-3.
[65] USTelecom Petition at 16. Providers are limited to inferring consent to use non-sensitive information for internal analytics to "improve products and services and to develop or improve their offerings or marketing campaigns generally," but this limitation to non-sensitive information does not apply when the provider is using data to improve network performance or provide services necessary to the provision of the telecommunications service.
[66] Report & Order at ¶ 201.
[67] *Id.* at ¶ 209.
[68] *See* USTelecom Petition at 1; NCTA Petition at 12–16; CTIA Petition at ii.

privacy rules more closely with the FTC's framework and to incorporate the FTC's comments and suggestions for the broadband privacy rules.

At their cores, the broadband privacy rules and the FTC's privacy standards are both "notice-and-choice" regimes in keeping with the Fair Information Practice Principles (FIPPs).[69] Both regimes are permissive and rely on truthful disclosures and agreements between providers and users. They generally require companies that collect data to give their users clear and conspicuous notice[70] of such collection and sharing and to honor privacy agreements between the user and a given service provider, website, platform, or app.[71] Neither regime prohibits any particular data collection, use, or sharing practice, nor prescribes specific protection measures.

The specific notice requirements imposed by the FCC and FTC are also in harmony. Both agencies enforce "clear and conspicuous" notice of data collection, use, and sharing practices,[72] as well as notice of and affirmative consent to "material retroactive changes" in privacy policies.[73] The Commission added point-of-sale notice to its rules, in accordance with FTC guidance and findings, to account for the fact that broadband internet is a paid subscription service.[74] Providing notice and choice at the point of sale for BIAS has the same effect as

---

[69] *See* Report & Order at ¶ 5 ("The privacy framework we adopt today focuses on transparency, choice, and data security . . . ."). *See generally, e.g.*, 2000 FTC Privacy Report; ROBERT GELLMAN, FAIR INFORMATION PRACTICES: A BASIC HISTORY (Dec. 22, 2016), http://bobgellman.com/rg-docs/rg-FIPshistory.pdf.

[70] *See* Report & Order at ¶ 140 (requiring "[c]lear, [c]onspicuous, and [p]ersistent notice"); 2000 FTC Privacy Report at 14 ("consumers should be given clear and conspicuous notice of an entity's information practices before any personal information is collected . . .").

[71] *See, e.g.*, ENFORCING PRIVACY PROMISES, FEDERAL TRADE COMMISSION, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises ("When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up to these promises.").

[72] *See supra* note 70.

[73] *See* FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (Dec. 2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf (laying out a set of principles including "affirmative express consent for material retroactive changes to privacy policies"); Report & Order at ¶ 9 (requiring opt-in approval (i.e. affirmative express consent) for material retroactive changes to privacy policies).

[74] Report & Order at ¶¶ 137–39.

providing notice and choice at the moment before a user downloads an app or subscribes to a social media platform.

In revising its de-identification standards, the Commission adopted the exact same de-identification framework enforced by the FTC.[75] This harmonized standard would allow a company operating both BIAS and non-BIAS services to combine data obtained from the provision of both services and de-identify all of the data according to the same standard.

The Commission also harmonized its rules with FTC standards by adopting a sensitivity-based framework,[76] at the request of Petitioners in their earlier comments.[77] In their comments, FTC staff strongly supported the sensitivity-based framework that the Commission ultimately adopted.[78]

In a further effort to harmonize its rules with the FTC framework, the Commission abandoned its original proposal to require enumerated data security requirements.[79] Instead, the Commission adopted a flexible data security standard that mirrors the FTC's data security standard for non-common carriers.[80] Both standards require companies to take reasonable measures to protect the security of customer information.[81]

Petitioners' arguments for weakening the data breach notification standards in the report and order contradict their calls to harmonize the broadband privacy rules with FTC standards.[82] The Commission adopted a harm-based trigger for data breach notifications in part because the

---

[75] *Id.* at ¶ 106.
[76] *Id.* at ¶¶ 172–200.
[77] *See, e.g.*, NCTA Comments at 3; USTelecom Comments at 23.
[78] Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16–106, at 20–23 (May 27, 2016) ("FTC Staff Comments").
[79] Report & Order at ¶¶ 235–37.
[80] *Id.* at ¶ 238 ("The rule we adopt today requires that every BIAS provider . . . take reasonable measures to protect customer PI from unauthorized use, disclosure, or access."); DATA SECURITY, FEDERAL TRADE COMMISSION, https://www.ftc.gov/datasecurity ("The touchstone of the FTC's approach to data security is reasonableness: a company's data security measures must be reasonable . . . .") (last visiting March 6, 2017).
[81] *Supra* note 80.
[82] *See, e.g.*, USTelecom Petition at 18–20.

FTC "supports an approach that requires notice unless a company can establish that there is no reasonable likelihood of economic, physical, or other substantial harm."[83] Petitioners ignore the FTC's support and argue for a lower standard simply because a few states employ it.[84] Petitioners offer no additional support for adopting a data breach notification standard below that which the FTC supports.

As the foregoing section illustrates, the Commission extensively revised its original NPRM to harmonize the broadband privacy rules with the FTC's frameworks and guidance for protecting privacy and data security and to incorporate the FTC's feedback. Thus, petitioners calls for harmonization ring hollow.

IX. Web browsing history is among the most revealing information internet users can disclose and should be considered sensitive.

The websites an internet user visits, perhaps more than any other data, have the potential to reveal the most sensitive, intimate details about his or her life. Browsing history can reveal a person's medical conditions, sexual preferences, financial status, political associations, and religious practices.[85] It can allow companies to infer information about internet users that they purposefully avoided disclosing, such as whether a woman is pregnant based on her shopping habits.[86] Misuse of this information not only undermines internet users' trust but can also cause serious tangible harm. For example, one internet user reported searching for help with a potential

[83] Report & Order at ¶ 264 (quoting Discussion Draft of H.R._, Data Security and Breach Notification Act of 2015, Before the Subcomm. on Commerce, Manufacturing, and Trade of the H. Comm. On Energy and Commerce, 114th Cong. 15 (2015), http://docs.house.gov/meetings/IF/IF17/20150318/103175/HHRG-114-IF17-Wstate-RichJ-20150318.pdf, (prepared statement of Jessica Rich, Dir. of the Bureau of Consumer Prot., Fed. Trade Comm'n)).
[84] *See, e.g.*, CTIA Petition at 19.
[85] Report & Order at ¶ 183, *See also* Upturn White Paper at 7–9.
[86] *See* Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before her Father Did*, FORBES (Feb. 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#f6a99cd66686.

alcoholism problem only to see targeted ads for the nearest liquor stores.[87] Yet, petitioners argue that only a narrow, enumerated list of information found in web browsing history should be considered sensitive.[88]

Petitioners' only support for narrowing the definition of sensitive information is a non-exhaustive list of categories deemed sensitive by the FTC.[89] However, the Commission has already rightfully rejected this argument on the grounds that "the FTC does not claim to define the outer bounds of sensitive information with this list."[90] In fact, "in its comments to this proceeding, the FTC clearly indicated that its list was non-exhaustive."[91] As the record indicates, asking ISPs to sift through subscribers' internet traffic to separate sensitive from non-sensitive information would defeat the privacy protections designed to shield the sensitive information in the first place.[92] The FTC staff comments also supported requiring opt-in consent for the content of communications, which FTC staff defined to include "search terms, . . . books read . . . [and] movies watched," all of which and more can be gleaned from web browsing and app usage history.[93]

Moreover, it's not always clear whether browsing history would reveal information in one of the enumerated categories. For example, one could assume that a webmd.com URL could reveal health information, but what about whole30.com, the website for a popular eating plan? While some users may visit Whole30 websites because of dietary preference or curiosity, others may do so because of health issues like obesity, heart disease, or celiac disease. Sensitive information can often be inferred from seemingly non-sensitive data.

---

[87] *See* Note to Self, The Search for Your Identity (Feb. 7, 2017), http://www.wnyc.org/story/privacy-paradox-day-2-challenge/.
[88] *See* USTelecom Petition at 5–7; CTIA Petition at 6–8.
[89] *See, e.g.*, CTIA Petition at 6–8.
[90] Report & Order at ¶ 178.
[91] *Id.* (citing FTC Staff Comments at 19-20).
[92] Report & Order at ¶ 187.
[93] FTC Staff Comments at 20.

The volume of browsing and app usage history that ISPs have access to amplifies its sensitivity. BIAS providers don't just have access to a few disparate pieces of web browsing data. They have access to a near-complete picture of the websites, and possibly individual pages, a subscriber visits. This fulsome record can provide contextual details that reveal even richer information about a person's life than a few sensitive URLs standing alone. This information can be even more revealing when combined with data such as the total volume and patterns of a subscriber's internet use and her physical location.

As explained above, the rules do not prohibit BIAS providers from using and sharing their customers' sensitive information. They simply require that providers notify their customers and get permission first. This burden is consistent with FTC standards and the FIPPs and is commensurate with the risk of exposure to customers when ISPs use and share their sensitive data.

X. Conclusion

Internet users depend upon the Commission to provide them with control over the sensitive data they must disclose to their ISPs. The Commission passed a well-supported, common-sense set of rules that protect consumers while maintaining flexibility for BIAS providers to use customer data with consent. Consumers should not lose this control because of a change in the administration. CDT urges the Commission to maintain its balanced broadband privacy rules and to dismiss petitioners' repetitious arguments for weakening or reversing them.

Respectfully submitted,

/s/ Natasha Duarte
Center for Democracy & Technology
1401 K St. NW, Suite 200
Washington, D.C. 20005
202.407.8822
Natasha@cdt.org