**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 |
| | ) | |

# REPORT AND ORDER

**Adopted: October 27, 2016** **Released: November 2, 2016**

By the Commission: Chairman Wheeler and Commissioner Rosenworcel issuing separate statements; Commissioner Clyburn approving in part, concurring in part and issuing a statement; Commissioners Pai and O'Rielly dissenting and issuing separate statements.

## TABLE OF CONTENTS

## I. INTRODUCTION

1. In this Report and Order (Order), we apply the privacy requirements of the Communications Act of 1934, as amended (the Act) to the most significant communications technology of today—broadband Internet access service (BIAS). Privacy rights are fundamental because they protect important personal interests—freedom from identity theft, financial loss, or other economic harms, as well as concerns that intimate, personal details could become the grist for the mills of public embarrassment or harassment or the basis for opaque, but harmful judgments, including discrimination. In adopting Section 222 of the Communications Act, Congress recognized the importance of protecting the privacy of customers using telecommunications networks. Section 222 requires telecommunications

carriers to protect the confidentiality of customer proprietary information. By reclassifying BIAS as telecommunications service, we have an obligation to make certain that BIAS providers are protecting their customers' privacy while encouraging the technological and business innovation that help drive the many benefits of our increasingly Internet-based economy.

2. Internet access is a critical tool for consumers—it expands our access to vast amounts of information and countless new services. It allows us to seek jobs and expand our career horizons; find and take advantage of educational opportunities; communicate with our health care providers; engage with our government; create and deepen our ties with family, friends and communities; participate in online commerce; and otherwise receive the benefits of being digital citizens. Broadband providers provide the "on ramp" to the Internet. These providers therefore have access to vast amounts of information about their customers including when we are online, where we are physically located when we are online, how long we stay online, what devices we use to access the Internet, what websites we visit, and what applications we use.

3. Without appropriate privacy protections, use or disclosure of information that our broadband providers collect about us would be at odds with our privacy interests. Through this Order, we therefore adopt rules that give broadband customers the tools they need to make informed choices about the use and sharing of their confidential information by their broadband providers, and we adopt clear, flexible, and enforceable data security and data breach notification requirements. We also revise our existing rules to provide harmonized privacy protections for voice and broadband customers—bringing privacy protections for voice telephony and other telecommunications services into the modern framework we adopt today.

4. In response to the *NPRM*, we received more than 275,000 submissions in the record of this proceeding, including comments, reply comments, and *ex parte* communications from consumers; broadband and voice providers and their associations; public interest groups; academics; federal, state, and local governmental entities; and others. We have listened and learned from the record. In adopting final rules, we rely on that record and in particular we look to the privacy and data security work done by the Federal Trade Commission (FTC), as well as our own work adopting and revising rules under Section 222. We have also taken into account the concepts that animate the Administration's Consumer Privacy Bill of Rights (CPBR), and existing privacy and data security best practices.

5. The privacy framework we adopt today focuses on transparency, choice, and data security, and provides heightened protection for sensitive customer information, consistent with customer expectations. In adopting these rules we honor customer's privacy rights and implement the statutory requirement that carriers protect the confidentiality of customer proprietary information. These rules do not prohibit broadband providers from using or sharing customer information, but rather are designed to protect consumer choice while giving broadband providers the flexibility they need to continue to innovate. By bolstering customer confidence in broadband providers' 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.

## II. EXECUTIVE SUMMARY

6. Today we adopt rules protecting the privacy of broadband customers. We also revise our current rules to harmonize our rules for all telecommunications carriers. In this Order, we first offer some background, explaining the need for these rules, and then discuss the scope of the rules we adopt. In discussing the scope of the rules, we define "telecommunications carriers" that are subject to our rules and the "customers" those rules are designed to protect. We also define the information protected under Section 222 as customer proprietary information (customer PI).[1] We include within the definition of

[1] *See* 47 U.S.C. § 222(a) ("Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to . . . customers.").

customer PI three types of information collected by telecommunications carriers through their provision of broadband or other telecommunications services that are not mutually exclusive: (i) individually identifiable Customer Proprietary Network Information (CPNI) as defined in Section 222(h);[2] (ii) personally identifiable information (PII); and (iii) content of communications. We also adopt and explain our multi-part approach to determining whether data has been properly de-identified and is therefore not subject to the customer choice regime we adopt for customer PI.

7. We next adopt rules protecting consumer privacy using the three foundations of privacy—transparency, choice, and security:

8. *Transparency*. Recognizing the fundamental importance of transparency to enable consumers to make informed purchasing decisions, we require carriers to provide privacy notices that clearly and accurately inform customers about what confidential information the carriers collect, how they use it, under what circumstances they share it, and the categories of entities with which they will share it. We also require that carriers inform their customers about customers' rights to opt in to or opt out (as the case may be) of the use or sharing of their confidential information. We require that carriers present their privacy notice to customers at the point of sale, and that they make their privacy policies persistently available and easily accessible on their websites, applications, and the functional equivalents thereof. Finally, consistent with FTC best practices and with the requirements in the CPBR,[3] we require carriers to give their customers advance notice of material changes to their privacy policies.

9. *Choice*. We find that because broadband providers are able to view vast swathes of customer data, customers must be empowered to decide how broadband providers may use and share their data. In this section, we adopt rules that give customers of BIAS and other telecommunications services the tools they need to make choices about the use and sharing[4] of customer PI, and to easily adjust those choices over the course of time. In adopting rules governing customer choice, we look to the best practices framework recommended by the FTC in its 2012 Privacy Report[5] as well as the choice framework in the Administration's CPBR and adopt a framework that provides heightened protections for sensitive customer information. For purposes of the sensitivity-based customer choice framework we adopt today, we find that sensitive customer PI includes financial information, health information, Social Security numbers, precise geo-location information, information pertaining to children, content of communications, web browsing history, application usage history, and the functional equivalents of web browsing history or application usage history. With respect to voice services, we also find that call detail information is sensitive information. We also adopt a tiered approach to choice, by reference to consumer expectations and context that recognizes three categories of approval with respect to use of customer PI obtained by virtue of providing the telecommunications service:

---

[2] Consistent with the statutory definition of CPNI, we define CPNI with respect to BIAS providers as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship." *See infra* Part III.B.3.a(i).

[3] *See* Executive Office of the President, Administration Discussion Draft: Consumer Privacy Bill of Rights Act (2015), https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf ("2015 Administration CPBR Discussion Draft" or "CPBR").

[4] Section 222 addresses the conditions under which carriers may "use, disclose, or permit access to" customer information. 47 U.S.C. § 222(c)(1), (c)(3), (d), (f). For simplicity throughout this document we sometimes use the terms "disclose" or "share" in place of "disclose or permit access to."

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

- *Opt-in Approval.* We adopt rules requiring carriers to obtain customers' opt-in approval for use and sharing of sensitive customer PI (and for material retroactive changes to carriers' privacy policies). A familiar example of opt-in practices appears when a mobile application asks for permission to use geo-location information.
- *Opt-out Approval*. Balancing important governmental interests in protecting consumer privacy and the potential benefits that may result from the use of non-sensitive customer PI, we adopt rules requiring carriers to obtain customers' opt-out approval for the use and sharing of non-sensitive customer PI.
- *Congressionally-Recognized Exceptions to Customer Approval Requirements.* Consistent with the statute, we adopt rules that always allow broadband providers to use and share customer data in order to provide broadband services (for example to ensure that a communication destined for a particular person reaches that destination), and for certain other purposes.

10. *Data Security and Breach Notification*. At its most fundamental, the duty to protect the confidentiality of customer PI requires telecommunications carriers to protect the customer PI they collect and maintain. We encourage all carriers to consider data minimization strategies and to embrace the principle of privacy by design. To the extent carriers collect and maintain customer PI, we require BIAS providers and other telecommunications carriers to take reasonable measures to secure customer PI. To comply with this requirement, a carrier must adopt security practices appropriately calibrated to the nature and scope of its activities, the sensitivity of the underlying data, the size of the provider, and technical feasibility. We decline to mandate specific activities that carriers must undertake in order to meet the reasonable data security requirement. We do, however, offer guidance on the types of data security practices we recommend providers strongly consider as they seek to comply with our data security requirement, while recognizing that what constitutes "reasonable" data security evolves over time.

11. We also adopt data breach notification requirements. In order to ensure that affected customers and the appropriate federal agencies receive notice of data breaches that could result in harm, we adopt rules requiring BIAS providers and other telecommunications carriers to notify affected customers, the Commission, and the FBI and Secret Service unless the carrier is able to reasonably determine that a data breach poses no reasonable risk of harm to the affected customers. In the interest of expedient law enforcement response, such notice must be provided to the Commission, the FBI, and Secret Service within seven business days of when a carrier reasonably determines that a breach has occurred if the breach impacts 5,000 or more customers; and must be provided to the applicable federal agencies at least three days before notice to customers. For breaches affecting fewer than 5,000 customers, carriers must notify the Commission without unreasonable delay and no later than thirty (30) calendar days following the carrier's reasonable determination that a breach has occurred. In order to allow carriers more time to determine the specifics of a data breach, carriers must provide notice to affected customers without unreasonable delay, but within no more than 30 days.

12. *Particular Practices that Raise Privacy Concerns.* Next, we find that take-it-or-leave-it offerings of broadband service contingent on surrendering privacy rights are contrary to the requirements of Sections 222 and 201 of the Act, and therefore prohibit that practice. We also adopt heightened disclosure and affirmative consent requirements for BIAS providers that offer customers financial incentives, such as lower monthly rates, in exchange for the right to use the customers' confidential information. Because the record contains very little about financial incentive practices of voice providers, this section of the Order is limited to BIAS providers.

13. Next we address several other issues raised in our rulemaking, including dispute resolution; the request for an exemption for enterprise customers of telecommunications services other than BIAS; federal preemption; and the timeline for implementation.

14. *Dispute Resolution*. We reaffirm customers' right to use the Commission's existing dispute resolution procedures and commit to initiating a rulemaking on the use of mandatory arbitration

requirements in consumer contracts for broadband and other communications services, acting on a notice of proposed rulemaking in February 2017.

15. *Exemption for Enterprise Customers of Telecommunications Services other than BIAS.* Recognizing that enterprise customers of telecommunications services other than BIAS have different privacy concerns and the capacity to protect their own interests, we find that a carrier that contracts with an enterprise customer for telecommunications services other than BIAS need not comply with the privacy and data security rules we adopt today if the carrier's contract with that customer specifically addresses the issues of transparency, choice, data security, and data breach and provides a mechanism for the customer to communicate with the carrier about privacy and data security concerns. As with the existing, more limited business customer exemption from our existing authentication rules, carriers will continue to be subject to the statutory requirements of Section 222 even where this exemption applies.

16. *Preemption*. In this section, we adopt the proposal in the *NPRM* and announce our intent to continue to preempt state privacy laws, including data security and data breach laws, *only* to the extent that they are inconsistent with any rules adopted by the Commission. This limited application of our preemption authority is consistent with our precedent in this area and with our long appreciation for the valuable role the states play in protecting consumer privacy.

17. *Implementation Timeline.* The Order provides a timeline for orderly transition to the new rules with additional time given for small carriers to the extent that they may need to change their practices.

18. *Legal Authority*. Finally, the Order closes by discussing our legal authority to adopt the rules.

## III. ESTABLISHING BASELINE PRIVACY PROTECTIONS FOR CUSTOMERS OF TELECOMMUNICATIONS SERVICES

19. In this section, we adopt a set of rules designed to protect the privacy of customers of BIAS and other telecommunications services. The rules we adopt today find broad support in the record, and are consistent with and build on existing regulatory and stakeholder-driven frameworks, including the Commission's prior decisions and existing Section 222 rules, other federal privacy laws, state privacy laws, and recognized best practices. The framework for our baseline privacy protections focuses on providing transparency of carriers' privacy practices; ensuring customers have meaningful choice about the use and disclosure of their private information; and requiring carriers to adopt robust data security practices for customer information. In this section, we explain the rules we adopt to protect the privacy of customers of BIAS and other telecommunications services.

### A. Background and Need for the Rules

20. The Commission has a long history of protecting customer privacy in the telecommunications sector. Section 705 of the Communications Act, for example, is one of the most fundamental and oldest sector-specific privacy requirements, and protects the privacy of information carried by communications service providers.[6] As early as the 1960s the Commission began to wrestle with the privacy implications of the use of communications networks to provide shared access to computers and the sensitive, personal data they often contained.[7] Throughout the 1980s and 1990s, the

[6] 47 U.S.C. § 605.

[7] *See, e.g.*, Bernard Strassburg, Address to the Ass'n for Comp. Machinery, *The Marriage of Computers and Communications: Some Regulatory Implications* (Oct. 20, 1966), *in* 9 Jurimetrics J. 12-18 (1966), *available at* http://heinonline.org/HOL/Page?handle=hein.journals/juraba9&div=9&g_sent=1&collection=journals.

Commission imposed limitations on incumbent telephone companies' use and sharing of customer information.[8]

21. Then, in 1996, Congress enacted Section 222 of the Communications Act providing statutory protections to the privacy of the data that all telecommunications carriers collect from their customers. Congress recognized that telecommunications networks have the ability to collect information from consumers who are merely using networks as conduits to move information from one place to another "without change in the form or content" of the communications.[9] Specifically, Congress sought to ensure "(1) the right of consumers to know the specific information that is being collected about them; (2) the right of consumers to have proper notice that such information is being used for other purposes; and (3) the right of consumers to stop the reuse or sale of that information."[10]

22. Section 222(a) imposes a duty on all telecommunications carriers to protect the confidentiality of their customers' "proprietary information," or PI.[11] Section 222(c) imposes restrictions on telecommunications carriers' use and sharing of customer proprietary network information (CPNI) without customer approval, subject to certain exceptions including as necessary to provide the telecommunications service (or services necessary to or used in providing that telecommunications service), and as otherwise provided for by law.[12] While we recognize, applaud, and encourage existing and continued marketplace self-regulation and privacy innovations, Congress has made clear that telecommunications carriers' privacy practices must comply with the obligations imposed by Section 222. We therefore reject arguments that we rely entirely on self-regulatory mechanisms.[13]

23. Over the last two decades, the Commission has promulgated, revised, and enforced privacy rules for telecommunications carriers that are focused on implementing the CPNI requirements of Section 222. As practices have changed, the Commission has refined its Section 222 rules. For example, after the emergence and growth of an industry made possible by "pretexting"—the practice of improperly accessing and selling details of residential telephone calls—the Commission strengthened its Section 222 rules to add customer authentication and data breach notification requirements.[14] The current Section 222 rules focus on transparency, choice, data security, and data breach notification.

---

[8] *See Amendment of Section 64.702 of the Commission's Rules and Regulations*, Final Order, 77 FCC 2d 384 (1980) (*Computer II*), *recon.*, 84 FCC 2d 50 (1980), *further recon.*, 88 FCC 2d 512 (1981), *aff'd sub nom. Computer and Commc'n Indus. Ass'n v. FCC*, 693 F.2d 198 (D.C. Cir. 1982), *cert. denied*, 461 U.S. 938 (1983); *Amendment of Section 64.702 of the Commission's Rules and Regulations*, Phase I, 104 FCC 2d 958 (1986); *Application of Open Network Architecture and Nondiscrimination Safeguards to GTE Corp.*, Report and Order, 9 FCC Rcd 4922, 4944-45, para. 45 (1994); *Application of Open Network Architecture and Nondiscrimination Safeguards to GTE Corp.*, Memorandum Opinion and Order, 11 FCC Rcd 1388, 1419-25, paras. 73-86 (1995); *Furnishing of Customer Premises Equipment by Bell Operating Telephone Companies and the Independent Telephone Companies*, Report and Order, 2 FCC Rcd 143 (1987), *recon. on other grounds*, 3 FCC Rcd 22 (1987); *aff'd*, *Ill. Bell Tel. Co. v. FCC*, 883 F.2d 104 (D.C. Cir. 1989).

[9] *See* 47 U.S.C. § 153(50).

[10] *See* Joint Explanatory Statement of the Committee of Conference, 104th Cong., 2d Sess. 204; *see also* H.R. Rep. No. 204, 104th Cong., 1st Sess. 91 (1995).

[11] 47 U.S.C. § 222(a) ("Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunications carriers, equipment manufacturers, and customers. . . .").

[12] 47 U.S.C. § 222(c)(1). Section 222(d) enumerates exceptions to this prohibition. 47 U.S.C. § 222(d).

[13] *See, e.g.*, Electronic Transaction Association (ETA) Comments at 2; AT&T Comments at 1; Multicultural Media, Telecom and Internet Council et al. (MMTC et al.) Comments at 2; Interactive Advertising Bureau (IAB) Comments at 5 ("IAB believes that industry self-regulation is the preferred approach to address online privacy.").

[14] *See generally Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No.

(continued….)

24. Meanwhile, as consumer use of the Internet exploded, the FTC, using its authority under Section 5 of the FTC Act to prohibit "unfair or deceptive acts or practices in or affecting commerce,"[15] has entered into a series of precedent-setting consent orders addressing privacy practices on the Internet, held workshops and conferences, and issued influential reports about privacy.[16] Taken together, the FTC's privacy work has focused on the importance of transparency; honoring consumers' expectations about the use of their personal information and the choices they have made about sharing that information; and the obligation of companies that collect personal information to adopt reasonable data security practices. Because common carriers subject to the Communications Act are exempt from the FTC's Section 5 authority, the responsibility falls to this Commission to oversee their privacy practices consistent with the Communications Act.[17]

25. Last year the Administration proposed a Consumer Privacy Bill of Rights. The goal of the CPBR is to "establish baseline protections for individual privacy in the commercial arena and to foster timely, flexible implementations of these protections through enforceable codes of conduct developed by diverse stakeholders."[18] It recognizes that Americans "cherish privacy as an element of their individual freedom," and that "[p]reserving individuals' trust and confidence that personal data will be protected appropriately, while supporting flexibility and the free flow of information, will promote continued innovation and economic growth in the networked economy."[19]

26. Prior to 2015, BIAS was classified as an information service, which excluded such services from the ambit of Title II of the Act, including Section 222, and the Commission's CPNI rules.[20] Instead, broadband providers were subject to the FTC's unfair and deceptive acts and practices authority.[21] In the *2015 Open Internet Order*, we reclassified BIAS as a telecommunications service subject to Title II of the Act, an action upheld by the D.C. Circuit in *United States Telecom Ass'n v. FCC*.[22] While we granted BIAS forbearance from many Title II provisions, we concluded that application and enforcement of the privacy protections in Section 222 to BIAS is in the public interest and necessary for the protection of consumers.[23] However, we questioned whether "the Commission's current rules

(Continued from previous page)
96-115, WC Docket No. 04-36, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) (*2007 CPNI Order*).

[15] 15 U.S.C. § 45(a)(1).

[16] *See* FTC Staff Comments at 4-6.

[17] *See* 15 U.S.C. §§ 45(a)(2) (exempting "common carriers subject to the Acts to regulate commerce"), 44 (defining "Acts to regulate commerce" as including "the Communications Act of 1934 and all Acts amendatory thereof and supplementary thereto"); 47 U.S.C. § 153(51) (providing that "[a] telecommunications carrier shall be treated as a common carrier under [the Communications Act] only to the extent that it is engaged in providing telecommunications services"). *See also* FTC Staff Comments at 2, n.5.

[18] *See* 2015 Administration CPBR Discussion Draft, § 4(a)(1).

[19] *Id*.

[20] *See Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5736-42, paras. 314-27 (2015), *aff'd United States Telecom Ass'n v. F.C.C.*, 825 F.3d 674 (D.C. Cir. 2016) (*2015 Open Internet Order*) (discussing the historical classification of broadband Internet access service).

[21] *See* 15 U.S.C. § 45(a)(1) (prohibiting unfair or deceptive acts or practices in or affecting commerce).

[22] *2015 Open Internet Order*, 30 FCC Rcd at 5733, para. 306; *see also United States Telecom Ass'n v. F.C.C.*, 825 F.3d at 712.

[23] *2015 Open Internet Order*, 30 FCC Rcd at 5821-22, paras. 463-64 (concluding that "forbearance from the application of section 222 with respect to broadband Internet access service is not in the public interest . . . and that section 222 remains necessary for the protection of consumers . . . ."); *see also Enforcement Bureau Guidance: Broadband Providers Should Take Reasonable, Good Faith Steps to Protect Consumer Privacy*, Enforcement
(continued….)

implementing section 222 necessarily would be well suited to broadband Internet access service," and forbore from the application of these rules to broadband service, "pending the adoption of rules to govern broadband Internet access service in a separate rulemaking proceeding."[24]

27. In March 2016, we adopted the *Broadband Privacy NPRM*, which proposed a framework for applying the longstanding privacy requirements of the Act to BIAS.[25] In the *NPRM*, we proposed rules protecting customer privacy using the three foundations of privacy—transparency, choice, and security—and also sought comment on, among other things, whether we should update rules that govern the application of Section 222 to traditional telephone service and interconnected VoIP service in order to harmonize them with the results of this proceeding.[26]

28. A number of broadband providers, their associations, as well as some other commenters argue that because broadband providers are part of a larger online eco-system that includes edge providers, they should not be subject to a different set of regulations.[27] These arguments ignore the particular role of network providers and the context of the consumer/BIAS provider relationship, and the sector specific privacy statute that governs the use and sharing of information by providers of telecommunications services. Based on our review of the record, we reaffirm our earlier finding that a broadband provider "sits at a privileged place in the network, the bottleneck between the customer and the rest of the Internet"[28]—a position that we have referred to as a gatekeeper.[29] As such, BIAS providers can collect "an unprecedented breadth" of electronic personal information.[30]

(Continued from previous page)
Advisory No. 2015-03, 30 FCC Rcd 4849 (Enf, Bur. 2015) (*Enf. Bur. Privacy Advisory*) (providing guidance "to broadband providers about how the Enforcement Bureau intends to enforce Section 222 in connection with BIAS during the time between the effective date of the *Open Internet Order* and any subsequent Commission action providing further guidance and/or adoption of regulations applying Section 222 more specifically to BIAS").

[24] *2015 Open Internet Order*, 30 FCC Rcd at 5823, para. 467.

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

[26] *Id.* at 2510, para. 24.

[27] *See, e.g.*, NTCA—The Rural Broadband Association (NTCA) Comments at 11; *see also* CTIA—The Wireless Association (CTIA) Comments at 106; Letter from Mike Montgomery, Executive Director, CALinnovates, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-016, at 1-2 (filed Oct. 19, 2016).

[28] *See* Letter from Paul Ohm, Professor, Georgetown University Law Center, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 16-106 Attach., Testimony Before the Subcommittee on Communications and Technology, Committee on Energy and Commerce, U.S. House of Representatives at 3 (filed June 19, 2016) (Paul Ohm Testimony).

[29] *See 2015 Open Internet Order*, 30 FCC Rcd at 5629, para. 80 (noting that "once a consumer chooses a broadband provider, that provider has a monopoly on access to the subscriber").

[30] Letter from Kathleen McGee, Bureau Chief, Bureau of Internet and Technology, New York State Attorney General, to Tom Wheeler, Chairman, FCC, WC Docket No. 16-106 at 2 (filed June 30, 2016) (NY Attorney General June 30, 2016 *Ex Parte*) (also claiming that BIAS providers can collect "not only a consumer's name, address and financial information but also every website he or she visited, the links clicked on those websites, geo-location information, and the content of electronic communications"); *see also, e.g.*, Ghostery Apr. 29, 2016 *Ex Parte* Attach. at 3-5; Consumer Action Comments at 1; Consumer Watchdog Comments at 4 ("The ISP is in a unique position to amass deeply revealing personal profiles, share the data with third parties or use it for its own purposes."); Public Knowledge et al. Comments, Attach. Public Knowledge White Paper, Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World at 51-52, 55-56 (Public Knowledge White Paper); American Association for Justice (AAJ) Comments at 8 (explaining that "BIAS providers are now privy to an extensive amount of personal information about their customers"); Electronic Frontier Foundation (EFF) Comments at 1.

29. We disagree with commenters that argue that BIAS providers' insight into customer online activity is no greater than large edge providers because customers' Internet activity is "fractured" between devices, multiple Wi-Fi hotspots, and different providers at home and at work.[31] As commenters have explained, "customers who hop between ISPs on a daily basis often connect to the same networks routinely,"[32] and as such, over time, "each ISP can see a substantial amount of that user's Internet traffic."[33]

30. While we recognize that there are other participants in the Internet ecosystem that can also see and collect consumer data,[34] the record is clear that BIAS providers' gatekeeper position allows them to see every packet that a consumer sends and receives over the Internet while on the network, including, absent encryption, its contents.[35] By contrast, edge providers only see a slice of any given consumers Internet traffic. As explained in the record, edge providers' visibility into consumers' web browsing activity is necessarily limited. According to the record, only three companies (Google, Facebook, and Twitter) have third party tracking capabilities across more than 10 percent of the top one million websites, and none of those have access to more than approximately 25 percent of web pages.[36] In contrast, a BIAS provider sees 100 percent of a customer's unencrypted Internet traffic.[37]

31. At the same time, users have much more control over tracking by web third parties than over tracking by BIAS providers. A range of browser extensions are largely effective at blocking

[31] *See, e.g.*, Peter Swire, Associate Director, The Institute for Information Security & Privacy at Georgia Tech, et al., Working Paper, Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others at 24-25 (filed May 27, 2016) (Peter Swire Working Paper); *see also* AT&T Comments at 4; CTIA Comments at 7-8.

[32] National Consumers League (NCL) Reply at 11.

[33] *See, e.g.*, Upturn Comments at 6.

[34] *See, e.g.*, Peter Swire Working Paper at 4 (stating that "non-ISPs are increasingly gathering commercially valuable information about online user activity from multiple context"); National Black Caucus of State Legislators (NBCSL) Comments at 1 ("Webmail, Internet videos, social media, and other firms, and even devices like open-source smartphones, all track and use enormous volumes of sensitive data"); Advanced Communications Law & Policy (ACLP) Comments at 13; Howard Beales Comments at 5 ("Each provider has particular insights into the consumer's online activities, but there is no entity in a 'unique' position to assemble a 'comprehensive' picture of online behavior."); Consumer Workers of America (CWA) Comments at 2-3 ; International Center for Law & Economics (ICLE) Comments at 9 ; AT&T Comments at 3 (arguing that "ISPs have *less*, not more, comprehensive visibility than many edge providers into their users' online activities"); Verizon Comments at 18 (asserting that "repeated and prolonged interactions provide social networking sites with access to vast amounts of commercially valuable information about their users, including user-generated content and metadata, which they use to facilitate targeted advertising"); CenturyLink Comments at 6 (arguing that to "the extent that user information (for example, web browsing activity and location information) is visible to the user's broadband provider, it also is visible to, and collected by, various third-party entities").

[35] *See, e.g.*, Paul Ohm Testimony at 3; EFF Comments at 1 ("No edge provider enjoys the ability to see everything a consumer does online. The technology now available for telecommunications providers allows for the possibility that every communications, activity, and movement can be tracked in real or near-real time.").

[36] *See* Dillon Reisman and Arvind Narayanan, Princeton Center for Information Technology Policy, WC Docket No. 16-106, *Ex Parte* Presentation at 32 (filed June 17, 2016) (Reisman and Narayanan June 17, 2016 *Ex Parte*) (showing that Google and Twitter are present on approximately 20 percent of websites and Facebook is present on approximately 25 percent of websites). By "third party tracking capability," we mean any method by which one party injects a tracking mechanism into a customer's traffic in order to monitor the customer's activity when the customer interacts with other parties. Cookies are a common third party tracker, but there are many other methods. *See id*. at 31 (explaining that "[t]hird parties on the web are any resources (images, tracking pixels, advertisements, code, etc.) loaded on a webpage that come from domains that are not the main domain you visited").

[37] *See* Reisman and Narayanan June 17, 2016 *Ex Parte* at 32.

prominent third parties, "but these tools do nothing to stop data collection on the wire."[38] Further, Professor Nick Feamster explains that unlike other Internet participants that see Domain Name System (DNS) lookups only to their own domains (e.g., google.com, facebook.com, netflix.com), BIAS providers can see DNS lookups every time a customer uses the service to go to a new site.[39]

32. Return Path explains additional unique data to which only BIAS providers have access:

> Many BIAS customers are assigned a dynamic ('changing') IP address when they connect to their provider. In these cases, each time a consumer's computer (or router) is rebooted, the ISP dynamically assigns a new IP address to the networking device. While the BIAS provider will have a record of precisely which user was connected to an IP address at a specific point in time, any third party will not, unless they subpoena the BIAS provider for data.[40]

Furthermore, as Mozilla explains, "[b]ecause these are paid services, [the broadband provider has] the subscriber's name, address, phone number and billing history. The combination gives ISPs a very unique, detailed and comprehensive view of their users that can be used to profile them in ways that are commercially lucrative."[41]

33. We agree with commenters that point out that encryption can significantly help protect the privacy of consumer content from BIAS providers.[42] However, 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.[43] Moreover, research shows that encrypted web traffic

[38] *Id.* at 35.

[39] *See* Feamster Edge Provider Comments at 2; *see also* Upturn Comments at 6 ("DNS queries are almost never encrypted.").

[40] Return Path Comments at 3.

[41] Mozilla Comments at 4-5.

[42] *See* National Cable & Telecommunications Association (NCTA) Reply at 21-24; AT&T Comments at 3-4; Howard Beales Comments at 4; CenturyLink Comments at 7; CTIA Comments at 14; Comcast Comments at 28 (explaining that if traffic is "encrypted using [Hypertext Transfer Protocol] HTTPS, the ISP only sees the top-level domain used to deliver packets, but otherwise is prevented from seeing either the contents of packets received or transmitted by the customer, or the full website address . . . of the websites that the customer visits"); Employment and Training Association (ETA) Comments at 6-7; Information Technology and Innovation Foundation (ITIF) Comments at 3-5; T-Mobile Comments at 5.

[43] Public Knowledge et al. Comments at 6 ("At an even more basic level, the timing of packet traffic can reveal data about a subscriber."); *see also id*. ("Traffic timing can reveal the hours when a subscriber is awake, asleep, or at work. It can reveal a person's religious beliefs (as with observance of the Sabbath), or unexpected changes in lifestyle, such as holidays, new relationships, or lost jobs."); Paul Ohm Testimony at 4 ("When you visit a website protected by the most widespread form of encryption in use, https or http over TLS, even though your BIAS provider cannot tell which individual page you are visiting on the website, it still can tell the domain name of the website you are communicating with, how often you return, roughly how much data you send and receive, and for how long each visit lasts."); Greenlining Institute and Media Alliance (Greenlining Institute) Comments at 5-6; Mozilla Comments at 4 ("All of a user's network traffic goes through their ISP, which means they have unfettered access to usage patterns and metadata. Usage patterns and metadata can be as revealing, or in some ways even more revealing, than content. Furthermore, users typically don't think about the potential for disclosure of private information that can come from metadata."); Software & Information Industry Association (SIIA) Comments at 3 ("Broadband service providers are unique in their ability to see the domains that their subscribers visit, even in cases where a website uses encryption.").

can be used to infer the pages within an encrypted site that a customer visits, and that the amount of data transmitted over encrypted connections can also be used to infer the pages a customer visits.[44]

34. The record also indicates that truly pervasive encryption on the Internet is still a long way off, and that many sites still do not encrypt.[45] We observe that several commenters rely on projections that 70 percent of Internet traffic will be encrypted by the end of 2016.[46] However, a significant amount of this encrypted data is video traffic from Netflix, which, according to commenters, accounts for 35 percent of North American Internet traffic.[47] Moreover, "raw packets make for a misleading metric."[48] As further explained by one commenter "watching the full Ultra HD stream of The *Amazing Spider-Man* could generate more than 40GB of traffic, while retrieving the WebMD page for 'pancreatic cancer' generates less than 2MB."[49] What's more, research shows that approximately 84 percent of health websites, 86 percent of shopping websites, and 97 percent of news websites remain unencrypted.[50] These types of websites generate less Internet traffic but contain "much more personalized data."[51] We encourage continued efforts to encrypt personal information both in transit and at rest. At the same time, our policy must account for the fact that encryption is not yet ubiquitous and, in any event, does not preclude BIAS providers from having unique access to customer data.[52]

35. Thus, the record reflects that BIAS providers are not, in fact, the same as edge providers in all relevant respects. In addition to having access to all unencrypted traffic that passes between the user and edge services while on the network, customers' relationships with their broadband provider is different from those with various edge providers, and their expectations concomitantly differ. For example, customers generally pay a fee for their broadband service, and therefore do not have reason to

[44] *See* Narayanan and Reisman Reply at 6; *see also* Upturn Comments at 8 ("A growing body of computer science research demonstrates that a network operator can learn a surprising amount about the contents of encrypted traffic without breaking or weakening encryption. By examining the features of the traffic — like the size, timing and destination of the encrypted packets — it is possible to uniquely identify certain web page visits or otherwise reveal information about what those packets likely contain."); Feamster ISP Data Use Comments at 4.

[45] *See* Upturn Comments at 3-6 (explaining that the fraction of total Internet traffic that is encrypted is a poor proxy for the privacy interests of a typical user, as 85 percent of the top 50 sites in each of health, news, and shopping categories still fail to encrypt browsing by default); *see also* Letter from Arvind Narayanan, Assistant Professor of Computer Science, Princeton University, to Chairman Tom Wheeler, FCC, WC 16-106 at 2 (filed May 27, 2016) (Narayanan Comments) (explaining that in their research, "we find that only 14.2% of the top 55,000 websites default to HTTPS on their home pages as of January 2016. This number falls to 8.6% on the top 1 million websites. Only a further 2.9% of the top 55,000 sites even offer HTTPS as an option").

[46] *See* Sandvine Comments at 10 (forecasting that "by the end of 2016, global Internet traffic will be more than 70% encrypted, with some networks surpassing the 80% threshold"); *see also* Peter Swire Working Paper at 7; AT&T Reply at 19; Comcast Comments at 5; USTelecom Reply at 5.

[47] *See* Free Press Reply at 11; Reisman and Narayanan June 17, 2016 *Ex Parte*, Attach., Part 2: ISPs and Privacy at 1 ("The percentage of traffic that is encrypted is not the right choice of metric since it is skewed by video statistics, especially Netflix."); *see also* NCL Reply at 9 (stating that "video streaming websites such as Netflix, which itself accounts for roughly 35 percent of North American internet traffic, are moving towards encryption").

[48] Reisman and Narayanan June 17, 2016 *Ex Parte* at 13.

[49] Upturn Comments at 3. Upturn also explains that devices such as "smart thermostats, home voice integration systems, and other appliances, fail to encrypt at least some of the traffic that they send and receive." *Id*. at 5.

[50] Reisman and Narayanan June 17, 2016 *Ex Parte* at 18.

[51] *See* NCL Reply at 9.

[52] *See* Narayanan Comments at 2 (explaining challenges to encryption that many "third parties do not support encryption, and that this impedes the adoption of HTTPS by websites"); *see also* Upturn Comments at 4 ("In order for a site to migrate to HTTPS without triggering warnings in its users' browsers, each one of the third-party partners that site uses on its pages must support HTTPS.").

expect that their broadband service is being subsidized by advertising revenues as they do with other Internet ecosystem participants.[53] In addition, consumers have a choice in deciding each time whether to use—and thus reveal information—to an edge provider, such as a social network or a search engine, whereas that is not an option with respect to their BIAS provider when using the service.[54]

36. While some customers can switch BIAS providers, others do not have the benefit of robust competition, particularly in the fixed broadband market. Moreover, we have previously observed that "[b]roadband providers have the ability to act as gatekeepers even in the absence of 'the sort of market concentration that would enable them to impose substantial price increases on end users.'"[55] Their position is strengthened by the high switching costs customers face when seeking a new service, which could deter customers from changing BIAS providers if they are unsatisfied the providers' privacy policies.[56] Moreover, even if a customer was willing to switch to a new broadband provider, the record shows consumers often have limited options.[57] We note, as stated in the 2016 *Broadband Progress Report*, approximately 51 percent of Americans still have only one option for a provider of fixed broadband at speeds of 25 Mbps download/3 Mbps upload.[58] Given all of these factors, we conclude

[53] *See, e.g.*, OTI Comments at 7 ("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 a loan to, rather than transferred to, broadband providers."); *see also* Consumer Federation of California (CFC) Comments at 5 ("When engaging in a transaction, a consumer may be required to provide personal information . . . . The consumer expectation is that the information is provided to complete the transaction, and not for other purposes.").

[54] *See, e.g.*, Feamster Edge Provider Comments at 3 ("For example, in many cases, a user may register with an edge provider using a pseudonym. The user may simply elect not to provide certain personal information or data to a social network, or even to not use the social network at all.").

[55] *2015 Open Internet Order*, 30 FCC Rcd at 5633, para. 84.

[56] *See* New York State Attorney General Reply at 1-2 ("Consumers cannot avoid a BIAS provider the way consumers can avoid (without penalty), or otherwise freely and easily choose between, search engines or other websites, or smartphone applications."); CFC Comments at 6-7 (explaining that if a consumer wants to switch BIAS providers, the consumer must undertake the time-consuming, and often difficult, process of finding and establishing broadband service with a new provider, which requires a new contract and possibly new equipment. The consumer must also terminate service with the existing provider, which may cause the consumer to incur financial penalties.); *2015 Open Internet Order*, 30 FCC Rcd at 5631, para. 81 ("Among the costs that consumers may experience are: high upfront device installation fees; long-term contracts and early termination fees; the activation fee when changing service providers; and compatibility costs of owned equipment not working with the new service. Bundled pricing can also play a role, as 'single-product subscribers are four times more likely to churn than triple-play subscribers.' These costs may limit consumers' willingness and ability to switch carriers if such a choice is indeed available."). *But see* CTIA Comments at 15-16 (asserting that in the market for wireless broadband, providers are adopting practices that drive down switching costs, e.g., "they are moving away from term-contracts with cancellation penalties, and offering to pay switching costs for new customers"); Free State Foundation Comments at 5-6; Howard Beales Comments at 3 (claiming BIAS providers "are not protected by uniquely high costs of switching that might justify different treatment").

[57] CFC Comments at 6 ("Even if a consumer could easily substitute a BIAS provider, consumers are usually limited to the local dominant telephone provider and the local dominant cable television provider. Consumers do not have a wide variety of choices in BIAS providers. They can only use the services of BIAS providers who have invested in the infrastructure to deliver high-speed Internet in their local area."); Paul Ohm Testimony at 3 ("It is also appropriate for Congress to protect the privacy of information sent through a BIAS provider because of the relative lack of choice consumers enjoy for BIAS services").

[58] *See 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*, 31 FCC Rcd 699, 736,
(continued….)

that, contrary to assertions in the record,[59] BIAS providers hold a unique position in the Internet ecosystem, and disagree with commenters that assert that rules to protect the privacy of broadband customers are unnecessary.[60]

37. As discussed above and throughout this Order, our sector-specific privacy rules are necessary to address the distinct characteristics of telecommunications services. The record demonstrates that strong customer privacy protections will encourage broadband usage and, in turn investment.[61] We further find that when consumers are confident that their privacy is protected, they will be more likely to adopt and use broadband services.[62] As aptly explained by Mozilla, "[t]he strength of the Web and its economy rests on a number of core building blocks that make up its foundational DNA. When these building blocks are threatened, the overall health and well-being of the Web are put at risk. Privacy is one of these building blocks."[63] The privacy framework we adopt today will bolster consumer trust in the broadband ecosystem, which is essential for business growth and innovation.[64]

### B. Scope of Privacy Protections under Section 222

38. In adopting rules to protect the privacy of customers of BIAS and other telecommunications services, we must begin by specifying the entities and information at issue. We look to the language of the statute to determine the appropriate scope of our implementing rules. As discussed above, Section 222(a) specifies that telecommunications carriers have a duty to protect the confidentiality of proprietary information of and relating to their customers, while Section 222(c) provides direction about protections to be accorded "customer proprietary network information." We therefore first adopt rules identifying the set of "telecommunications carriers" that are subject to our rules and define the

(Continued from previous page)
para. 86 (2016) (*2016 Broadband Progress Report*) (explaining further that in rural areas, only 13 percent of Americans have more than one option for service compared to 44 percent in urban areas).

[59] *See, e.g.*, NCTA Comments at 54 ("The NPRM fails to cite any empirical evidence to support the notion that consumers believe there should be different privacy and data protection regimes depending upon whether their data is used by an ISP rather than by a search engine, Web site, app provider, or any of the advertising, analytics or other third party entities working with such edge providers."); Howard Beales Comments at 3 (claiming BIAS providers "do not pose a unique or more comprehensive privacy risk than other participants in the Internet ecosystem");CTIA Comments at 7 (arguing "ISPs' access to online consumers' personal information in this ecosystem is neither comprehensive nor unique").

[60] *See, e.g.*, American Advertising Federation (AAF) et al. Comments at 2; Association of National Advertisers (ANA) Comments at 9 (arguing the Commission, offers insufficient evidence that privacy concerns are legitimate or that they will result in tangible harm to consumers); T-Mobile Comments at 11 ("The NPRM also fails to identify a problem with BIAS provider practices that needs to be remedied, or to demonstrate that the existing privacy framework or the marketplace is not protecting consumers."); SIIA Comments at 4.

[61] NCL Reply at 13 ("Despite claims that the Commission's reclassification of BIAS as a common carrier under Title II will discourage investment and impose costs, the telecommunications industry had a strong financial year in 2015); *see also id*. (explaining that "AT&T's net income was over $13 billion, which marked a 60 percent increase from 2014").

[62] *See* Public Knowledge et al. Reply at 7; OTI Comments at 10-11 (reporting that in January 2016, the City of Portland, Oregon's Office for Community Technology reported that in focus groups conducted by the city to improve the city's understanding of adoption challenges, privacy concerns were raised in every group); *see also 2016 Broadband Progress Report*, 31 FCC Rcd at 751-52, para. 126 (finding that consumers fearful of the loss of privacy may be less likely to use broadband connectivity, thus decreasing the demand for broadband investment and deployment); FTC Staff Comments at 2 (stating that "while consumers continue to increase their online presence, privacy and security are important not just for consumers but is also a crucial component for building trust in the online marketplace").

[63] Mozilla Comments at 1.

[64] *Broadband Privacy NPRM*, 31 FCC Rcd at 2557, para. 167.

"customers" these rules protect. Next we define "customer proprietary information" and include within that definition "individually identifiable customer proprietary network information," "personally identifiable information," and content of communications.

### 1. The Rules Apply to Telecommunications Carriers and Interconnected VoIP Providers

39. For purposes of the rules we adopt today to implement Section 222, we adopt a definition of "telecommunications carrier" that includes all telecommunications carriers providing telecommunications services subject to Title II, including broadband Internet access service (BIAS). We also include interconnected VoIP services, which have been covered since 2007.[65] Although not limited to voice services, our existing rules have been focused on voice services.[66] When we reclassified BIAS as a telecommunications service, we recognized that our existing CPNI rules were not necessarily well suited to the broadband context, and we therefore forbore from applying the existing Section 222 rules to BIAS.[67] As part of this rulemaking we have explored what privacy and data security rules we should adopt for BIAS and whether we can harmonize our rules for voice and BIAS. Throughout this Order we find that it is in the interests of consumers and providers to harmonize our voice and broadband privacy rules. We therefore adopt a single definition of telecommunications carrier for purposes of these rules, and except as otherwise provided, adopt harmonized rules governing the privacy and data security practices of all such telecommunications carriers.

40. Because we adopt a single definition of telecommunications carrier we need not change the definitions of "telecommunications carrier or carrier" currently in our rules implementing Section 222.[68] We do amend the definition of telecommunications service to conform to the definition of telecommunications carrier. We also observe that because BIAS is now a telecommunications service, BIAS providers are now telecommunications carriers within the meaning of those rules. To remove any doubt as to the scope of these rules, we define BIAS for purposes of our rules pursuant to Section 222 identically to our definition in the *2015 Open Internet Order*.[69] We define "broadband Internet access service provider" or "BIAS provider" to mean a person engaged in the provision of BIAS.[70] Under the

[65] *See 2007 CPNI Order*, 22 FCC Rcd at 6929, para. 3.

[66] *See generally Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Declaratory Ruling, 28 FCC Rcd 9609, 9611-12, paras. 9-11 (2013) (*2013 CPNI Declaratory Ruling*).

[67] *2015 Open Internet Order*, 30 FCC Rcd at 5822-23, para. 466.

[68] *See* 47 CFR § 64.2003(o), (p) (defining "telecommunications carrier or carrier" and "telecommunications service"). In accordance with these definitions, we continue to consider entities providing interconnected VoIP service to be telecommunications carriers for the purposes of these rules. *See infra* Part IV.E. The Commission has not classified interconnected VoIP service as telecommunications service or information service as those terms are defined in the Act, and we need not and do not make such a determination today. *See* 47 U.S.C. § 153(24), (53) (defining "information service" and "telecommunications service"); *2007 CPNI Order*, 22 FCC Rcd at 6929, para. 3 (extending application of the CPNI rules to providers of interconnected VoIP service).

[69] Specifically, a broadband Internet access service is "a mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up Internet access service. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence, or that is used to evade the protections set forth in this part." 47 CFR § 8.2(a); *2015 Open Internet Order*, 30 FCC Rcd at 5682, para. 187; *see also* INCOMPAS Comments at 3 (distinction in BIAS definition between mass market and business services should apply in Section 222 context); Information Technology Industry Council (ITIC) Comments at 6 (the definition of BIAS should exclude Internet intermediary services and "over the top" services).

[70] As used in the foregoing sentence and in the definition of "customer" below, a "person" includes any individual, group of individuals, corporation, partnership, association, unit of government, or legal entity, however organized.

(continued….)

*2015 Open Internet Order*'s definition of BIAS, the term BIAS provider does not include "premises operators – such as coffee shops, bookstores, airlines, private end-user networks (e.g., libraries and universities), and other businesses that acquire broadband Internet access service from a broadband provider to enable patrons to access the Internet from their respective establishments."[71] Moreover, consistent with the *2015 Open Internet Order*,[72] our rules do not govern information that BIAS providers obtain by virtue of providing other non-telecommunications services, such as edge services that the BIAS provider may offer like email, websites, cloud storage services, social media sites, music streaming services, and video streaming services (to name a few).[73]

### 2. The Rules Protect Customers' Confidential Information

41. Section 222 governs how telecommunications carriers treat the "proprietary" and "proprietary network" information of their "customers."[74] For purposes of the rules we adopt today implementing Section 222, we define "customer" as (1) a current or former subscriber to a telecommunications service; or (2) an applicant for a telecommunications service. We adopt a single definition of customer, because we agree with those commenters that argue that harmonizing the definition of "customer" for both BIAS and other telecommunications services will ease consumer expectations, reduce confusion, and streamline compliance costs for BIAS providers, especially small providers.[75] We also find that voice and BIAS customers face similar issues related to the protection of their private information when they apply for, subscribe to, and terminate their telecommunications services.[76]

42. In adopting this definition of customer, we find that BIAS providers' and other telecommunications carriers' duty to protect customer proprietary information under Section 222 begins when a person applies for service and continues after a subscriber terminates his or her service. Our existing rules for voice services apply only to current customers.[77] We are, however, persuaded by commenters that argue that the existing rule's limitation to current subscribers is too narrow.[78] As data

(Continued from previous page)
*Cf. Preserving the Open Internet*, Report and Order, 25 FCC Rcd 17905, 17937, para. 54 n.172 (2010) (*2010 Open Internet Order*); 47 CFR § 54.8(a)(6).

[71] *2015 Open Internet Order*, 30 FCC Rcd at 5685, para. 191.

[72] *See, e.g.*, *2015 Open Internet Order*, 30 FCC Rcd at 5773, para. 377 (explaining that email and cloud-based storage are "separable information services" from the broadband Internet access service).

[73] *See* Letter from Loretta Polk, Vice President & Associate General Counsel, NCTA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1-2 (filed Oct. 20, 2016) (NCTA Oct. 20, 2016 *Ex Parte*).

[74] *See* 47 U.S.C. § 222(a), (c).

[75] *See* American Cable Association (ACA) Comments at 57 (supporting "a single privacy and data security framework" and harmonization of Section 222 rules and definitions); Rural Wireless Association (RWA) Reply at 7 ("Harmonization provides several benefits, including increased provider efficiency, better customer understanding, and higher compliance rates."). Nex-Tech explains that "because it is already subject to the CPNI rules as a provider of voice service, Nex-Tech has aligned its [BIAS] policies and procedures with respect to customer information with its compliance of the Commission's voice CPNI rules. Nex-Tech and WTA . . . generally believe this is common across the board for RLECs." Letter from Patricia Cave, Director, Government Affairs, WTA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1 (filed April 25, 2016) (WTA & Nex-Tech Apr. 25, 2016 *Ex Parte*).

[76] *See, e.g.*, *TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13332-35 (2014) (*TerraCom NAL*) (voice services).

[77] 47 CFR § 64.2003(f).

[78] *See, e.g.*, OTI Comments at 14 ("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.").

storage costs decrease and computing power increases, previous barriers to data analysis based on cost, time, or feasibility are receding.[79] BIAS providers and other telecommunications carriers have the technical ability to retain and use applicant and customer information long after the application process or termination of service.[80] If our rules do not protect applicants, consumers would lack basic privacy protections when they share any confidential information in order to apply for a telecommunications service. Similarly, current customers would be penalized for switching providers given that the "losing" carrier would be free to stop protecting the confidentiality of any private information it retains.[81] These outcomes would run counter to our firm commitment to promote broadband adoption, competition, and innovation.[82] Making this change is consistent with the 2014 Notice of Apparent Liability issued in *TerraCom*, in which we explained that that "the carrier/customer relationship commences when a consumer applies for service."[83]

43. We disagree with commenters that assert that including prospective and former customers within the definition of customer could unduly burden providers.[84] If carriers want to limit their obligations with respect to applicants and former customers, they can and should adopt data minimization practices and destroy applicants' and former customers' confidential information as soon as practicable, in a manner consistent with any other applicable legal obligations.

44. In addition, for purposes of these rules, we find it appropriate to attribute all activity on a subscription to the subscriber. We recognize that multiple people often use the BIAS or voice services purchased by a single subscriber. For example, residential fixed broadband and voice services often have a single named account holder, but all household members and their guests may use the Internet connection and voice service purchased by that subscriber. Likewise, enterprise customers may have many users on the same account. And, for mobile services, multiple users using separate devices may

[79] *See, e.g.*, FTC, Big Data: A Tool for Inclusion or Exclusion?, at 1 (2016), https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report (2016 FTC Big Data Report) ("A common framework for characterizing big data relies on the 'three Vs,' the volume, velocity, and variety of data, each of which is growing at a rapid rate as technological advances permit the analysis and use of this data in ways that were not possible previously."); Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values at 1 (2014), https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (2014 Administration Big Data Report) ("The collection, storage, and analysis of data is on an upward and seemingly unbounded trajectory, fueled by increases in processing power, the cratering costs of computation and storage, and the growing number of sensor technologies embedded in devices of all kinds.").

[80] *See, e.g.*, OTI Comments at 14 ("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."). *But see* WISPA Reply at 26-28 (stating that the rules should not protect applicants and former customers).

[81] *See* Rafi Goldberg, NTIA, Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online *Activities* (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities (discussing, *inter alia*, how privacy concerns can deter many Americans from engaging in important economic and civic online activities).

[82] 47 U.S.C. § 1302(a); *see generally 2016 Broadband Progress Report*, 31 FCC Rcd 699.

[83] *TerraCom NAL*, 29 FCC Rcd at 13333, para. 23. In *TerraCom* we observed, *inter alia*, that "consumers applying for telecommunications services have a reasonable expectation that the carrier will protect the confidentiality of the [proprietary information] they provide as part of that transaction" and that the carriers themselves treated applicants as "customers" in their forms and policies. *Id.* at 13332-35, paras. 21-28.

[84] *See* WISPA Comments at 23-24 (asserting that applicants should be excluded because they can review a provider's privacy policy before sharing personal information); CTIA Comments at 95 (asserting that inclusion would hinder providers' ability to solicit prospective customers); Sprint Comments at 4; T-Mobile Comments at 56; INCOMPAS Comments at 9-10 (including former customers could hinder providers' ability to try to win them back); NTCA Comments at 13-17 (asserting that other industries are not required to protect applicant and former customers beyond FTC standard; the inclusion will burden small providers).

share one account.[85] However, treating each individual user as a separate customer would be burdensome because the provider does not have a separate relationship with each of those users, outside of the relationship with the subscriber. To minimize burdens on both providers and customers, we find it is reasonable to define "customer" to include users of the subscription (such as household members and their guests), but treat the subscriber as the person with authority to make privacy choices for all of the users of the service.[86] As such, we disagree with commenters who argue that every individual using a BIAS subscription should qualify as a distinct customer with separate privacy controls.[87]

45. We recognize that some BIAS or voice subscriptions identify multiple users. For example, some mobile BIAS providers offer group plans in which each person has their own identified device, user ID, and/or telephone number. If a BIAS or other telecommunications provider is already treating each user as distinct and the subscriber authorizes the other users to control their account settings, we encourage carriers to give these users individualized privacy controls.[88]

### 3. Scope of Customer Information Covered by These Rules

46. In this section, we define the scope of information covered by the rules implementing Section 222. Specifically, we import the statutory definition of customer proprietary network information (CPNI) into our implementing rules, and define customer proprietary information (customer PI) as including individually identifiable CPNI, personally identifiable information (PII), and content of communications. We recognize that these categories are not mutually exclusive, but taken together they identify the types of confidential customer information BIAS providers and other telecommunications carriers may collect or access in connection with their provision of service. Below, we provide additional guidance on the scope of these categories of customer information in the telecommunications context.

#### a. Customer Proprietary Network Information

47. Consistent with the preexisting voice rules, we adopt the statutory definition of customer proprietary network information (CPNI) for all telecommunications services, including BIAS. Since this is our first opportunity to address this definition's application to BIAS, to offer clarity we provide guidance on the meaning of CPNI as it applies to BIAS. We focus on Section 222(h)(1), which defines CPNI to mean:

> (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service

[85] *See, e.g.*, Paul Vixie Comments at 3-4; Center for Digital Democracy (CDD) Comments at 14 (asserting that the rules should protect each user in a household).

[86] *See* Common Sense Kids Action Comments at 9 (supporting a "'customer dashboard' in which a main subscriber can set different privacy preferences for different devices or log-ins."). *See infra* Part III.H.2.

[87] *See* Access Now Comments at 4. *But see* Sprint Comments at 4-5 (including "all conceivable users of the network would lead to unworkable obligations for providers"); Security and Software Engineering Research Center ($S^2$ERC) Comments at 5-6 (only the account holder should qualify as a customer); NTCA Comments at 17-18 (same).

[88] *See* OTI Comments at 17-18 ("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."); CDD Comments at 14 ("[T]hose with a login (or are identified as a distinct customer by the subscriber) should be provided with the same fair treatment for their privacy."); Access Now Comments at 4 (supporting protections for users other than the primary account holder); Paul Vixie Comments at 3-4 (same); Consumer Federation of California Comments at 14 (same).

> received by a customer of a carrier; except that [CPNI] does not include subscriber list information.[89]

We agree with commenters that, due to its explicit focus on telephone exchange and telephone toll service, Section 222(h)(1)(B) is not relevant to BIAS.[90]

48. We interpret the phrase "made available to the carrier by the customer solely by virtue of the carrier-customer relationship" in Section 222(h)(1)(A) to include any information falling within a CPNI category that the BIAS provider collects or accesses in connection with the provision of BIAS.[91] This includes information that may also be available to other entities. We disagree with commenters who propose that the phrase "made available to the carrier by the customer solely by virtue of the carrier-customer relationship" means that *only* information that is *uniquely* available to the BIAS provider may satisfy the definition of CPNI.[92] These commenters contend that if a customer's information is available to a third party, it cannot qualify as CPNI, focusing on the term "solely" in the clause. However, the term "solely" modifies the phrase "by virtue of," *not* the phrase "made available to the carrier." We therefore conclude that "solely by virtue of the carrier-customer relationship" means that information constitutes CPNI under Section 222(h)(1)(A) if the provider acquires the information as a product of the relationship and not through an independent means.[93]

49. We also agree with the Center for Democracy and Technology that the fact that third-parties might gain access to the same data when a consumer uses their services "does not negate the fact that the BIAS provider has gained access to the data only because the customer elected to use the BIAS provider's telecommunications service."[94] The statute is silent as to whether such information might be available to other parties, which indicates that Congress did not intend for the definition of CPNI to hinge on such information being solely available to the customers' carrier.[95] Indeed, in the voice context, CPNI certainly is available to other parties besides the customer's carrier and Section 222 protects that data. For example, when a customer calls someone else, CPNI is also made available to the recipient's carrier and intermediaries facilitating the completion of the call. Furthermore, we find that commenters' narrow definition of CPNI is inconsistent with the privacy-protective purpose of the statute.[96] We agree with

[89] 47 U.S.C. § 222(h)(1).

[90] *See* 47 U.S.C. § 222(h)(1)(B); Comcast Comments at 78-79 (BIAS "does not fit the definition of either" telephone exchange service or telephone toll service); NTCA Comments at 19 (agreeing that (h)(1)(B) is inapplicable to BIAS); *accord* USTelecom Comments at 6.

[91] *See* CDT Reply at 19; OTI Reply at 5-6.

[92] *See* CTIA Comments at 44 (arguing that unlike voice context, many types of BIAS CPNI are available to third parties); USTelecom Comments at 6-7 ("the same data, and even more, is available to other members of the Internet ecosystem"); Cincinnati Bell Tel. Co. (Cincinnati Bell) Comments at 6 (information "sent onto the open Internet in order to make the service work" should not qualify as CPNI); CenturyLink Comments at 15-16 (information "easily obtained by multiple parties . . . cannot be deemed CPNI"); NTCA Comments at 21-22 (arguing that source IP addresses should not be protected because customers share them with third parties).

[93] *See, e.g.*, OTI Reply at 5-6 ("Whether other online entities have access to this information is irrelevant to the statutory determination. . . . The mere fact that third parties have access to similar or even identical information does not factor into the statute because that information was not provided *to the carrier by the customer*."). We note, for clarity, that both inbound and outbound traffic are made available to the carrier by the customer solely by virtue of the carrier-customer relationship. The directionality of the traffic is irrelevant as to whether it satisfies the statutory definition of CPNI.

[94] CDT Reply at 19.

[95] *See, e.g.*, OTI Reply at 5-6.

[96] *See U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1236 (10th Cir. 1999) ("[T]he specific and dominant purpose of § 222 is the protection of customer privacy."); CDT Reply at 19 ("[I]t does not follow that BIAS providers should be able (continued….)

some commenters' assertions that when a BIAS provider acquires information wholly apart from the carrier-customer relationship, such as purchasing public records from a third party, that information is not CPNI.[97]

50. However, consistent with the Commission's *2013 CPNI Declaratory Ruling*, we find that information that a BIAS provider causes to be collected or stored on a customer's device, including customer premises equipment (CPE) and mobile stations, also meets the statutory definition of CPNI.[98] The "fact that CPNI is on a device and has not yet been transmitted to the carrier's own servers also does not remove the data from the definition of CPNI, if the collection has been done at the carrier's direction."[99]

51. BIAS providers also have the ability, by virtue of the customer-carrier relationship, to create and append CPNI to a customer's Internet traffic. For example, if a carrier inserts a unique identifier header (UIDH), that UIDH is CPNI because, as we will discuss in greater detail below, it is information in the application layer header that relates to the technical configuration, type, destination, and amount of use of a telecommunications service.[100]

52. We do not believe it is necessary to categorize all personally identifiable information (PII) as CPNI, as suggested by Public Knowledge.[101] While we agree with Public Knowledge's sentiment that PII is confidential information that deserves protection under the Act, and we agree that some information is both PII and CPNI, we find that the Act categorizes and protects all PII as proprietary information, under Section 222(a), as discussed below.[102]

#### (i) Guidance Regarding Information that Meets the Statutory Definition of CPNI in the Broadband Context

53. In keeping with the Commission's past practice,[103] we decline to set out a comprehensive list of data elements that do or do not satisfy the statutory definition of CPNI in the broadband context.[104] We agree with commenters that "no definition of CPNI should purport or aim to be comprehensive and exhaustive, as technology changes quickly and business models continually seek new ways to monetize

(Continued from previous page)
to freely share sensitive information simply because some other actors are already privy to it. That the data exists in the hands of certain other entities does not mean that further dissemination by the BIAS provider no longer implicates consumer privacy.").

[97] *See* CTIA Comments at 49 ("Data acquired from third parties falls wholly outside of this definition."); *accord* Comcast Comments at 75-76.

[98] *See 2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9618, para. 27. CPE is "equipment employed on the premises of a person (other than a carrier) to originate, route, or terminate telecommunications." 47 U.S.C. § 153(16); *see also* 47 CFR § 64.2003(h). A mobile station is "a radio-communication station capable of being moved and which ordinarily does move." 47 U.S.C. § 153(34). *See infra* para. 80.

[99] *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9618, para. 27.

[100] *See infra* para. 76; *See Cellco P'ship, d/b/a Verizon Wireless*, Order, 31 FCC Rcd 1843 (Enf. Bur. 2016) (*Verizon UIDH Consent Decree*).

[101] *See* Public Knowledge Comments at 27-28; Public Knowledge White Paper at 60-61. *See also infra* Part III.B.3.c.

[102] *See infra* Part III.B.3.b.

[103] *See 2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9617, para. 24 n.54.

[104] *See Broadband Privacy NPRM*, 31 FCC Rcd at 2514, para. 40; *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9617, para. 24 n.54.

and market user data."[105] In the past, the Commission has enumerated certain data elements that it considers to be voice CPNI—including call detail records (including caller and recipient phone numbers, and the frequency, duration, and timing of calls) and any services purchased by the customer, such as call waiting; these data continue to be voice CPNI going forward.[106] Similarly, we follow past practice and identify a non-exhaustive list of the types of information that we consider to constitute CPNI in the BIAS context. We find that such guidance will help provide direction regarding the scope of providers' obligations and help to increase customers' confidence in the security of their confidential information as technology continues to advance.[107] We find that the following types of information relate to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and as such constitute CPNI when a BIAS provider acquires or accesses them in connection with its provision of service:

- Broadband Service Plans
- Geo-location
- MAC Addresses and Other Device Identifiers
- IP Addresses and Domain Name Information
- Traffic Statistics
- Port Information
- Application Header
- Application Usage
- Application Payload
- Customer Premises Equipment and Device Information

54. We will first give a brief overview of the structure of Internet communications, to help put these terms in context, and then discuss why each of these types of information, and other related components of Internet Protocol packets, qualify as CPNI.

**(a) Background — Components of an Internet Protocol Packet**

55. The layered architecture of Internet communications informs our analysis of CPNI in the broadband context. While the concept of layering is not unique to the Internet, layering plays a uniquely prominent role for Internet-based communications and devices. For that reason, we begin with a brief technical overview of the layered structure of Internet communications.

56. Multiple layers—often represented as a vertical stack—comprise every Internet communication. Each layer in the stack serves a particular logical function and uses a network protocol that standardizes communication between systems,[108] enabling rapid innovation in Internet-based

[105] Access Now Comments at 4. *Accord* Electronic Frontier Foundation (EFF) Comments at 3 (supporting illustrative examples instead of a comprehensive list).

[106] *2007 CPNI Order*, 22 FCC Rcd at 6931; *see also* 47 CFR § 64.2003(d); 47 CFR § 64.5103(c).

[107] *See* EFF Comments at 3 ("Illustrative examples . . . will provide useful guidance for providers and reduce compliance costs without risking obsolescence."); Jon Peha Reply at 6 (broad definition of CPNI necessary given BIAS providers' gatekeeping role).

[108] *See* James F. Kurose & Keith W. Ross, Computer Networking: A Top-Down Approach 47-50 (6th ed. 2013) (Kurose & Ross).

protocols and applications.[109] Within one device, information is typically transmitted vertically through the various layers.[110] When an application sends data over the Internet, the process begins with application data moving downwards through the layers. Each layer adds additional networking information and functionality, wrapping the output of the layers above it with a "header." The communication sent out over the Internet—consisting of the application data wrapped in headers from each layer—is called a "packet."[111] When a device receives data over the Internet, the reverse process occurs. Data moves upwards through the layers; each layer unwraps its associated information and passes the output upward, until the application on the recipient's device recovers the original application data.[112] As a component of their provision of service, BIAS providers may analyze each of these layers for reasonable network management.[113]

57. Common representations of the Internet's architecture range from four to seven layers.[114] To highlight design properties relevant to the broadband CPNI analysis, we describe a five-layer model in this explanation. From top to bottom, the layers are: application payload, application header, transport, network, and link. We will briefly describe each of the five layers, from top to bottom:

58. *Application Payload.* The information transmitted to and from each application a customer runs is commonly referred to as the application layer payload.[115] The application payload is the substance of the communication between the customer and the entity with which she is communicating. Examples of application payloads include the body of a webpage, the text of an email or instant message, the video served by a streaming service, the audiovisual stream in a video chat, or the maps served by a turn-by-turn navigation app.

59. *Application Header*. The application will usually append one or more headers to the payload; these headers contain information *about* the application payload that the application is sending or requesting. For example, in web browsing, the Uniform Resource Locator (URL) of a webpage constitutes application header information. In a conversation via email, instant message, or video chat, an application header may disclose the parties to the conversation.[116]

60. *Transport Layer*. Below the application header layer is the transport layer, which forwards data to the intended application on each device and can manage the flow of communications from one device to another device.[117] Port numbers are an example of data within the transport layer header; a port number specifies which application on a device should handle a network communication.

---

[109] *See, e.g.*, David D. Clark et al., *Tussle in Cyberspace: Defining Tomorrow's Internet*, 13 IEEE/ACM Transactions on Networking 462-475 (2005); Kurose & Ross at 49-53.

[110] Across all devices, equivalent layers perform the equivalent functions. This compatibility and interoperability is typically represented as horizontal relationships. Kurose & Ross at 53-55.

[111] *See* Internet Engineering Task Force, Requirements for Internet Hosts – Communications Layers, RFC 1122 (Oct. 1989), https://tools.ietf.org/html/rfc1122.

[112] *See* Kurose & Ross at 53-55.

[113] *See id.* at 756-60.

[114] *See id.* at 47-55; Internet Engineering Task Force, Requirements for Internet Hosts – Communications Layers, RFC 1122 (Oct. 1989), https://tools.ietf.org/html/rfc1122.

[115] *See, e.g.*, Kurose & Ross at 55.

[116] *See id.*, Chapter 2.

[117] *See id.*, Chapter 3. Two transport protocols are widely deployed on the Internet: the Transmission Control Protocol (TCP), which ensures that data arrives intact, and the User Datagram Protocol (UDP), which provides fewer guarantees about data integrity. *Id.*

61. *Network Layer*. The network layer is below the transport layer, and contains information used to route packets across the Internet from one device to another device. Almost all Internet traffic uses the Internet Protocol (IP) at the network layer.[118] IP addresses are the most common example of data at the network layer; an IP address in a network header indicates the sender or recipient of an Internet packet.[119]

62. *Link Layer*. The final layer is the link layer, which is below the network layer. Link layer protocols route data between devices on the same local network. For example, devices on the same wired or wireless network can usually communicate directly with each other at the link layer.[120] MAC addresses are an example of data at the link layer, and a wide range of link technologies (Ethernet, DOCSIS, Wi-Fi, and Bluetooth, among others) use them. A MAC address functions as a globally unique device identifier, ensuring that every device on a local network has a distinct address for sending and receiving data.[121]

**(b) Specific Examples of CPNI in the BIAS Context**

63. With this understanding of the architecture of Internet communications, we can now examine how the components of an IP data packet map to the statutory definition of CPNI.[122] Below, we provide guidance addressing how various data elements constitute CPNI under Section 222.

64. *Broadband Service Plans*. We find that broadband service plans meet the statutory definition of CPNI in the broadband context because they relate to the quantity, type, amount of use, location, and technical configuration of a telecommunications service.[123] We agree with NTCA that "information related to a customer's broadband service plan can be viewed as analogous to voice telephony service plans,"[124] which the Commission has long considered to be CPNI in the voice context.[125] These plans detail subscription information, including the type of service (e.g., fixed or mobile; cable or fiber; prepaid or term contract), speed, pricing, and capacity (e.g., data caps). These data relate to the "type" of telecommunications service to which the customer subscribes, as well as how the BIAS provider will adjust the "technical configuration" of their network to serve that customer. Information pertaining to subscribed capacity and speed relate to the "quantity" of services the customer purchases, as well as the "amount" of services the customer consumes. Service plans often include the

[118] *See id.*, Chapter 4.

[119] *See id*.

[120] *See id.*, Chapter 5.

[121] *See id.*

[122] In this section, we provide guidance on what data elements constitute CPNI; this is distinct from the question of whether a data element constitutes *individually identifiable* CPNI and is thus "customer proprietary information." *See infra* Appx. A, § 64.2002(f).

[123] *See* 47 U.S.C. § 222(h)(1)(A).

[124] NTCA Comments at 20.

[125] *See 2007 CPNI Order*, 22 FCC Rcd at 6931, para. 5; *see also Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended; 2000 Biennial Regulatory Review—Review of Policies and Rules Concerning Unauthorized Changes of Consumers' Long Distance Carriers*, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860, 14864, para. 7 (2002) (*2002 CPNI Order*). In 2011, the Sixth Circuit agreed with AT&T's argument that information in a service plan "clearly constitutes CPNI" in the voice context. *CMC Telecomm, Inc. v. Mich. Bell Tel. Co.*, 637 F.3d 626, 630 (6th Cir. 2011).

customer's address (for billing purposes or to identify the address of service), which relates to the location of use of the service.

65. *Geo-location*. Geo-location is information related to the physical or geographical location of a customer or the customer's device(s), regardless of the particular technological method used to obtain this information. Providers often need to know where their customers are so that they can route communications to the proper network endpoints. The Commission has already held that geo-location is CPNI,[126] and Congress emphasized the importance of geo-location data by adding Section 222(f).[127]

66. We disagree with commenters who ask us to draw technology-based distinctions for what types of location information are sufficiently precise to qualify as geo-location CPNI.[128] BIAS providers can use many types of data—either individually or in combination—to locate a customer, including but not limited to GPS, address of service, nearby Wi-Fi networks, nearby cell towers, and radio-frequency beacons.[129] We caution that these and other forms of location information in place now or developed in the future constitute geo-location CPNI when made available to the BIAS provider solely by virtue of the carrier-customer relationship.

67. *Media Access Control (MAC) Addresses and Other Device Identifiers*. We conclude that device identifiers, such as MAC addresses, are CPNI in the broadband context because they relate to the technical configuration and destination of use of a telecommunications service.[130] Link layer protocol headers convey MAC addresses, along with other link layer protocol information.[131] A MAC address uniquely identifies the network interface on a device, and thus uniquely identifies the device itself (including the device manufacturer and often the model).[132] MAC addresses relate to the technical configuration and destination of communications because BIAS providers use them to manage their networks and route data packets to the appropriate network device.[133] For the same reasons, we conclude that other device identifiers and other information in link layer protocol headers are CPNI in the

[126] *See 2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9616, para. 22 ("The location of a customer's use of a telecommunications service also clearly qualifies as CPNI."); 47 U.S.C. § 222(h)(1)(A).

[127] Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, § 5, 113 Stat. 1285, 1289 (1999) (codified at 47 U.S.C. § 222(f) ("Authority to use location information")).

[128] *See, e.g.*, CTIA Comments at 135 (urging rules to "cover only precise GPS location information"); Future of Privacy Forum Reply at 6-7; NCTA Comments at 61.

[129] *See, e.g.*, Future of Privacy Forum Comments at 20-25; $S^2$ERC Comments at 6; Farsight Security Comments at 5.

[130] *See* 47 U.S.C. § 222(h)(1)(A). *See also* CDT Reply at 18-19; Letter from Laura Moy, Institute for Public Representation, Counsel, New America's Open Technology Institute, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 4-6 (filed Oct. 13, 2016) (OTI Oct. 13, 2016 *Ex Parte*).

[131] *See supra* Part III.B.3.a(i)(a).

[132] *See, e.g.*, Kurose & Ross at 463-65. *Cf.* NTCA Comments at 21 ("a MAC address is associated to a device"). *See also* CDT Reply at 19 ("It is believed that some future forms of BIAS network architectures may remove the need for a network modem, making available a MAC address farther up into the BIAS provider's network outside of the home network."); EFF Comments at 3-4 (device identifiers implicate customers' privacy interests and should be protected). The Commission has previously recognized that unique device identifiers such as an "electronic serial number" are "call data information" in the TRS CPNI context. 47 CFR § 64.5103(c).

[133] *See* Kurose & Ross at 463-65; Front Porch Comments at 2 ("ISPs use this address for internal network management purposes, including access permissions, data consumption, and service tier monitoring."); CDT Comments at 13-14 ("MAC addresses and other device identifiers relate to the destination of a telecommunications service because they are used to route packets to individual devices connected to a network."); NCTA Comments at 62-63 ("device identifiers or other data elements . . . may be used by broadband providers to facilitate email traffic routing"). We disagree with Sandvine, which argues that link layer information such as MAC addresses do not relate to the technical configuration of network traffic or the destination of packets. *See* Sandvine Comments at 22-23.

broadband context because they relate to the technical configuration and destination of use of a telecommunications service.[134]

68. *Internet Protocol (IP) Addresses and Domain Name Information*. We conclude that source and destination IP addresses constitute CPNI in the broadband context because they relate to the destination, technical configuration, and/or location of a telecommunications service.[135] An IP address is a routable address for each device on an IP network,[136] and BIAS providers use the end user's and edge provider's IP addresses to route data traffic between them.[137] As such, source and destination IP addresses are roughly analogous to telephone numbers in the voice telephony context.[138]

69. We agree with those commenters that argue that the IP addresses a customer uses and those with which she exchanges packets constitute CPNI because both source and destination IP addresses relate to the destination of use of a telecommunications service; one links to the destination for inbound traffic while the other links to the destination for outbound traffic.[139] IP addresses are also frequently used in geo-location.[140] As Public Knowledge explains, "IP addresses can easily be mapped to geographic locations, meaning that both the subscriber and the service can be located."[141] IP addresses relate to technical configuration because BIAS providers configure their systems to use IP addresses in the network layer to communicate data packets between senders and receivers.[142]

70. We disagree with commenters who argue that a customer's IP address is not CPNI. Some commenters argue that a customer's IP address is not CPNI because the BIAS provider assigns the

[134] For a brief overview of Internet architecture and layering, see *supra* Part III.B.3.a(i)(a).

[135] *See* 47 U.S.C. § 222(h)(1)(A).

[136] *See* Internet Engineering Task Force, The Internet Numbers Registry System, RFC 7020 (2013), https://tools.ietf.org/html/rfc7020 (discussing non-reserved globally unique unicast IP addresses assigned through the Internet Numbers Registry System).

[137] *See, e.g.*, Kurose & Ross at 130, 331-63.

[138] The Commission has previously held telephone numbers dialed to be CPNI. *See 2007 CPNI Order*, 22 FCC Rcd at 6931, para. 5. Further, our CPNI rules for TRS providers recognize IP addresses as call data information. 47 CFR § 64.5103(c). By this analogy, we mean only that both are "roughly similar numerical identifiers" used to route telecommunications. *See* Internet Society June 6, 2016 *Ex Parte* at 2. We do not intend to imply that IP addresses are or should be administered in the same manner as telephone numbers. *See id*. at 1-2 (discussing the differences in each identifier's governance). This definitional change to our regulations in no way asserts Commission jurisdiction over the assignment or management of IP addressing.

[139] *See* Comcast Comments at 78 ("IP addresses identify the 'logical' location of a device for purposes of routing Internet traffic" (footnote omitted)); CDT Comments at 14 (citations omitted); Sandvine Comments at 22-23 (IP addresses relate to destination); NCTA Comments at 62 ("IP addresses . . . may be used by broadband providers to facilitate email traffic routing" (citation omitted)); CDT Comments at 14 ("IP addresses are the destinations to which BIAS providers deliver packets and also may be associated with physical locations."); $S^2$ERC Comments at 6-7.

[140] *See, e.g.*, CDD Comments at 15; CDT Comments at 14. A BIAS provider is uniquely capable of geo-locating an IP address. Most notably, in the case of mobile broadband Internet access service, the provider knows the geo-location of the cell towers to which the customer's device connects and can use this to determine the customer's device location.

[141] Harold Feld, et al., Public Knowledge, Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World 47 (2016) (Public Knowledge White Paper) (citing Dan Jerker B. Svantenson, *Geo-Location Technologies and Other Means of Placing Borders on the "Borderless" Internet"*, 23 J. Marshall J. Computer & Info. L. 101, 109–11 (2004)).

[142] *See supra* Part III.B.3.a(i)(a); Sandvine Comments at 22-23 (arguing that IP addresses relate to technical configuration).

IP address to the customer,[143] and thus it is not "made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[144] This reading of the text undermines the privacy-protective purpose of the statute. First, as the Commission has previously held, information that the provider causes to be generated by a customer's device or appended to a customer's traffic, in order to allow the provider to collect, access, or use that information, can qualify as CPNI if it falls within one of the statutory categories.[145] Second, while the provider generates and assigns the number that will become the customer's IP address, that number is ultimately just a proxy for the customer, translated into a language that Internet Protocol understands. But for the carrier-customer relationship, the customer would not have an IP address. Other commenters argue that IP addresses should not qualify as CPNI because "this information is necessarily sent onto the open Internet in order to make the service work."[146] However, as discussed above, whether information is available to third parties does not affect whether it meets the statutory definition of CPNI.[147]

71. We also disagree with commenters who assert that dynamic IP addresses[148] do not meet the statutory definition of CPNI. As Return Path explains, "[w]hile the BIAS provider will have a record of precisely which user was connected to [a dynamic] IP address at a specific point in time, any third party will not."[149] A dynamic IP address may be used for a shorter period of time than a static IP address.[150] But a dynamic IP address still meets the statutory definition of CPNI because it relates to the technical configuration, type, destination, and/or location of use of a telecommunications service, for the reasons discussed above.

72. We also conclude that information about the domain names visited by a customer constitute CPNI in the broadband context. Domain names (e.g., "fcc.gov") are common monikers that the

[143] *See, e.g.*, Comcast Comments at 77; NCTA Comments at 21.

[144] 47 U.S.C. § 222(h)(1)(A).

[145] *See 2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9618, para. 27; *Verizon UIDH Consent Decree*, 31 FCC Rcd at 1843-44, paras. 2-5.

[146] Cincinnati Bell Comments at 6; *accord* Comcast Comments at 81; William Rinehart Comments at 3 (Rinehart); *see also* S$^2$ERC Comments at 6-7 (arguing that IP addresses are widely accessible, but also can be "sensitive information"); Peter Swire & Justin Hemmings (Swire & Hemmings) Reply at 7-8 (arguing that IP addresses are available to intermediaries between the customer and the content provider).

[147] *See supra* para. 49.

[148] A dynamic IP address is one that the BIAS provider can change. *See generally* Network Working Group, Internet Eng'g Task Force, *RFC 2131: Dynamic Host Configuration Protocol* (1997), https://tools.ietf.org/html/rfc2131; Network Working Group, Internet Eng'g Task Force, *RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6)* (2003), https://tools.ietf.org/html/rfc3315.

[149] Return Path Comments at 3. *See also, e.g.*, Comcast, Comcast Legal Response Ctr., *Law Enforcement Handbook (Rev. May 1, 2015)* at 10 (2015), https://www.comcast.com/~/Media/403EEED5AE6F46118DDBC5F8BC436030.ashx (noting that Comcast retains dynamic IP address log files for 180 days).

[150] We note that these potential privacy benefits of dynamic IP addresses depend upon the specific network configuration and practices of the BIAS provider. For example, a provider may assign a dynamic IP address to a customer for a long period of time, such that it is effectively equivalent to a static IP address. In certain configurations (e.g., IPv6 without privacy extensions), a dynamic IP address can be *more* revealing than a static IP address, because it includes other network identifiers (such as a MAC address). *See, e.g.*, Network Working Group, Internet Eng'g Task Force, *RFC 3041: Privacy Extensions for Stateless Address Autoconfiguration in IPv6* at 3 (2001), https://tools.ietf.org/html/rfc3041; Comcast, Comcast Legal Response Ctr., *Law Enforcement Handbook (Rev. May 1, 2015)* at 10, https://www.comcast.com/~/Media/403EEED5AE6F46118DDBC5F8BC436030.ashx (noting that Comcast retains dynamic IP address log files for 180 days).

customer uses to identify the end point to which they seek to connect.[151] Domain names also translate directly into IP addresses. Because of this easy translation, domain names relate to the destination and technical configuration of a telecommunications service.

73. As discussed above, Internet traffic is communicated through a layered architecture, including a network layer that uses protocol headers containing IP addresses to route communications to the intended devices.[152] Similar to IP addresses, other information in the network layer protocol headers is CPNI in the broadband context. BIAS providers configure their networks to use this information for routing, network management, and security purposes. These headers will also indicate the total size of the packet.[153] As such, other information in the network layer protocol headers relates to the technical configuration and amount of use of a telecommunications service.[154]

74. *Traffic Statistics*. We conclude that traffic statistics meet the statutory definition of CPNI in the broadband context because they relate to the amount of use, destination, and type of a telecommunications service.[155] We use the technology-neutral term "traffic statistics" to encompass any quantification of the communications traffic, including short-term measurements (e.g., packet sizes and spacing) and long-term measurements (e.g., monthly data consumption, average speed, or frequency of contact with particular domains and IP addresses).[156] We believe that traffic statistics are analogous to call detail information regarding the "duration[] and timing of [phone] calls" and aggregate minutes used in the voice telephony context, both of which are CPNI.[157] BIAS providers use traffic statistics to optimize the efficiency of their networks and protect against cyber threats, but can also use this data to draw inferences that implicate the amount of use, destination, and type of a telecommunications service. For example, BIAS providers can use traffic statistics to determine the amount of use (e.g., date, time, and duration), and to identify patterns such as when the customer is at home, at work, or elsewhere, or reveal other highly personal information. Traffic statistics related to browsing history and other usage can reveal the "destination" of customer communications. Further, a BIAS provider could deduce the "type" of application (e.g., VoIP or web browsing) that a customer is using based on traffic patterns, and thus the purpose of the communication.

75. *Port Information.* We conclude that port information is CPNI in the broadband context because it relates to the destination, type, and technical configuration, of a telecommunications service.[158] A port is a logical endpoint of communication with the sender or receiver's application, and consequently

[151] *See* Feamster ISP Data Use Comments at 5. Whether or not the customer uses the BIAS provider's in-house DNS lookup service is irrelevant to whether domain names satisfy the statutory definition of CPNI. *See* Farsight Security Comments at 7.

[152] *See supra* Part III.B.3.a(i)(a).

[153] CDT Comments at 14 (citing Internet Eng'g Task Force, *RFC 791: Internet Protocol - DARPA Internet Program Protocol Specification* 12 (1981), https://tools.ietf.org/html/rfc791).

[154] *See* CDT Comments at 13-14; EFF Comments at 3-4.

[155] *See* 47 U.S.C. § 222(h)(1)(A); *see also* EFF Comments at 4.

[156] There are many common forms of traffic statistics, such as IPFIX, and we believe it is important to focus on how BIAS providers use these data, rather than single out particular technologies. *See* Feamster ISP Data Use Comments at 2-7.

[157] *2007 CPNI Order*, 22 FCC Rcd at 6930-31, para. 5; *see also* 47 CFR § 64.5103(c); *2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9617, para. 25; *2007 CPNI Order*, 22 FCC Rcd at 6936, para. 13 n.45.

[158] *See* 47 U.S.C. § 222(h)(1)(A); OTI Comments at 20-21; CDT Comments at 14-15 ("Essentially, ports are a more granular form of destination information than IP and MAC addresses, indicating [to] which applications particular packets may be destined."); Public Knowledge White Paper at 47-48.

relates to the "destination" of a communication.[159] The transport layer protocol header of a data packet contains the destination port number, which determines which application receives the communication.[160] Port numbers identify or at least provide a strong indication of the type of application used, and thus the purpose of the communication, such as email, web browsing, or other activities.[161] BIAS providers configure their networks using port information for network management purposes, such as to block certain ports to ensure network security. As such, these practices relate to the "technical configuration" of the telecommunications service. We agree with commenters that other transport layer protocol header information is CPNI in the broadband context because it relates to the technical configuration and amount of use of a telecommunications service.[162] BIAS providers use other header information in this layer to configure their networks and monitor for security threats. For example, because UDP headers indicate packet size, they can reveal the amount of data the customer is consuming, and because TCP headers include sequence numbers, they can reveal information about a customer's device configuration.[163]

76. *Application Header*. We conclude that application header information is CPNI in the broadband context because it relates to the destination, type, technical configuration, and amount of use of a telecommunications service.[164] As discussed above, the top-most layer of network architecture is the application layer; IP data packets contain application headers to instruct the recipient application on how to process the communication.[165] Application headers contain data for application-specific protocols to help request and convey application-specific content.[166] The application header communicates

[159] *See* CDT Comments at 14 ("Network ports are subaddresses within the internet protocol and are used by operating systems to sort and deliver packets to individual applications.").

[160] *See* Network Working Group, Internet Eng'g Task Force, *RFC 1180: A TCP/IP Tutorial* 23, 24 (1991), https://tools.ietf.org/html/rfc1180 ("Well-defined port numbers are dedicated to specific applications." *Id*. at 24). Port destinations are analogous to telephone extensions in the voice context.

[161] *See* NTCA Comments at 22 (port information "can be used to discern whether a person was using email or browsing the Internet"); CDT Comments at 14-15 ("For instance, ports 109 and 110 indicate the use of the Post Office Protocol (POP), marking the packet as an email transmission, while port 1214 indicates the use of the Kazaa peer-to-peer file sharing protocol."); OTI Comments at 20-21 ("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 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 game Doom."). Though sometimes port numbers may not reveal anything of significance, *see, e.g.*, Farsight Security Comments at 8 ("One result of the widespread use of perimeter firewalls is that 'everything' seems to tunnel its traffic over port 80. Port numbers have largely gone from reliable clues to the type of application generating traffic seen on the wire to either: [e]verything over port 80, or [e]verything over a random dynamic port."), they often do, and therefore we conclude that they relate to the destination, type, or technical configuration of the service. *See, e.g.*, Internet Assigned Numbers Authority, *Service Name and Transport Protocol Number Registry* (Oct. 17, 2016), http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml; *see generally* Internet Eng'g Task Force, *RFC 6335: Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry* (2011), https://tools.ietf.org/html/rfc6335.

[162] *See* CDT Comments at 14-15 ("At the transport layer, the two most common protocols, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) include header fields specifying source and destination ports as well as packet size.").

[163] *Id*.

[164] *See* 47 U.S.C. § 222(h)(1)(A); CDT Comments at 15 (discussing the uses of application headers).

[165] *See supra* Part III.B.3.a(i)(a).

[166] *See* Ctr. for Democracy & Tech., *Applying Communications Act Consumer Privacy Protections to Broadband Providers* (2016), https://cdt.org/files/2016/01/2016-01-20-Packets_Layers_fnl.pdf (CDT White Paper). Application headers are analogous in the voice telephony context to a customer's choices within telephone menus used to route calls within an organization (e.g., "Push 1 for sales. Push 2 for billing."). *See Broadband Privacy NPRM*, 31 FCC Rcd at 2517, para. 50.

information between the application on the end user's device and the corresponding application at the other endpoint of the communication.[167] For example, application headers for web browsing typically use the Hypertext Transfer Protocol (HTTP) and contain the Uniform Record Locator (URL), operating system, and web browser; application headers for email typically contain the source and destination email addresses.[168] The type of applications used, the URLs requested, and the email destination all convey information intended for use by the edge provider to render its service. Application headers can also reveal information about the amount of data being conveyed in the packet.[169] BIAS providers may configure their networks using application headers for network management or security purposes.

77. Consistent with our decision in the *2013 CPNI Declaratory Ruling*, we agree with commenters[170] that any information that the BIAS provider injects into the application header, such as a unique identifier header (UIDH), is also CPNI in the broadband context.[171] BIAS providers sometimes append information to application headers, in particular HTTP headers, in order to uniquely tag communications with a specific subscriber account.[172] Like other application header information, these data relate to the technical configuration, type, destination, and amount of use of a telecommunications service.

78. *Application Usage*. We conclude that information detailing the customer's use of applications is CPNI in the broadband context because it relates to the type and destination of a telecommunications service.[173] Unlike an application payload, which contains the substance of a communication in an IP packet, application usage information is data that reveals the customer's use of an application more generally. A BIAS provider often collects application usage information through its provision of service.[174] Sometimes application usage information is quantified—similar to traffic statistics—into short-term or long-term measurements. Such information can reveal the type of applications the customer uses and with whom she communicates. As such, to the extent that the BIAS

[167] *See* Kurose & Ross at 51; CDT Comments at 15; CDT White Paper.

[168] *See* CDT Comments at 15. Application headers may also include information relating to persistent identifiers, use of encryption, and virtual private networks (VPNs). Email headers may also include the subject line.

[169] For example, HTTP has a field called "Content-Length." *See* Network Working Group, Internet Eng'g Task Force, *RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1* at 119 (1999), https://www.ietf.org/rfc/rfc2616.txt.

[170] *See* CDT Comments at 15 ("These identifiers also encompass each element of CPNI, relating [to] the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service to an individual subscriber.").

[171] *See 2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9618, para. 27; *Verizon UIDH Consent Decree*, 31 FCC Rcd at 1843-44, paras. 1-5.

[172] *See* CDT Comments at 15 ("In the practice known as 'HTTP header injection,' BIAS providers add a new HTTP header line after the message leaves the customer's browser. This header serves as a unique marker identifying all HTTP messages sent from a single subscriber account.").

[173] *See* 47 U.S.C. § 222(h)(1)(A).

[174] *See* T-Mobile, *T-Mobile Privacy Policy* (Nov. 25, 2015), http://www.t-mobile.com/company/website/privacypolicy.aspx#fullpolicy ("We may also collect information about applications on your device, the fact that an application has been added, when an application is launched or fails to launch, and length of time an application has been running."); AT&T, *AT&T Privacy Policy* (July 24, 2015), https://www.att.com/gen/privacy-policy?pid=2506#print (AT&T collects "how often you open an application, how long you spend using the app and other similar information."); Sprint, *Sprint Corporation Privacy Policy* (July 22, 2016), https://www.sprint.com/legal/privacy.html (Sprint collects information about "applications purchased, applications downloaded or used, and other similar information."); Verizon, *Verizon Full Privacy Policy*, http://www.verizon.com/about/privacy/full-privacy-policy (last visited Oct. 5, 2016) (Verizon collects "application and feature usage").

provider directs the collection or storage of such information, we conclude that it is CPNI.[175] For the reasons discussed above, we disagree with commenters who contend that we should not consider such information to be CPNI because it is also available to other parties.[176]

79. *Application Payload.* We conclude that the application payload, which is the part of the IP packet containing the substance of the communication between the customer and entity with which the customer is communicating, can be considered CPNI.[177] Examples of application payloads include the body of a webpage, the text of an email or instant message, the video shared by a streaming service, the audiovisual stream in a video chat, or the maps served by a ride-sharing app. It is available to the carrier only because of the customer-carrier relationship and can relate to technical configuration, type, destination and amount of the use of the telecommunications service. BIAS providers are technically capable of configuring their networks to scan all parts of the data packet, including the payload, to detect security threats and block malicious packets.[178] The application payload can help identify the parties to the communication (e.g., the online streaming video distributor of a streaming video, or the homepage of a news website), and thus the communication's destination. The payload's size and substance can also indicate the amount of data the customer is using, the type of communication, and the duration of the use of the service. Another way to think of the application payload is as the "content of the communication." Because of the importance given to protecting content of communications in our legal system, we also discuss content separately as its own element of customer proprietary information.[179]

80. *Customer Premises Equipment (CPE) and other Customer Device Information*. Information pertaining to customer premises equipment (CPE) and other customer device information, such as that relating to mobile stations, is CPNI in the broadband context because it relates to the technical configuration, type, and destination of a telecommunications service.[180] The Act defines CPE as "equipment employed on the premises of a person (other than a carrier) to originate, route, or terminate telecommunications."[181] The Commission has long-understood CPE to include customers' mobile devices, such as cell phones.[182] Given this precedent, we believe that other consumer devices capable of being connected to broadband services, such as smartphones and tablets, also fall under the rubric of CPE, along with more traditional CPE such as a customer's computer, modem, router, videophone, or IP caption phone. However, we also observe that such devices would be considered "mobile stations," which the Act defines as "a radio-communication station capable of being moved and which ordinarily does move."[183] We disagree with commenters that argue that only devices furnished by the BIAS provider can qualify as CPE;[184] there is no such limitation in the statutory language.

81. We find that the traits of CPE and other customer devices (e.g., model, operating system, software, and/or settings) a customer uses relates to the technical configuration and communications

[175] *See 2013 CPNI Declaratory Ruling*, 28 FCC Rcd at 9615-16, para. 21-23.

[176] *See* NTCA Comments at 22-23; *see supra* para. 48.

[177] *See supra* Part III.B.3.a(i)(a); *see also* Public Knowledge White Paper at 48; CDT Comments at 17.

[178] *See* Sandvine Comments at 2-3; CDT Reply at 14 (BIAS providers scan payloads to "searc[h] for protocol non-compliance . . . viruses and spam, interference, and for collecting network statistics."). BIAS providers also use various network management techniques to minimize network congestion while transmitting application payloads.

[179] *See infra* Part III.B.3.d.

[180] *See* 47 U.S.C. § 222(h)(1)(A).

[181] 47 U.S.C. § 153(16); 47 CFR § 64.2003(h).

[182] *See generally Bundling of Cellular Customer Premises Equipment and Cellular Service*, Report and Order, 7 FCC Rcd 4028 (1992).

[183] 47 U.S.C. § 153(34).

[184] *See* NTCA Comments at 25.

protocols the BIAS provider uses to interface that device with its network, as well as the type of service to which the customer subscribes (e.g., fixed or mobile, cable or fiber). CPE and mobile station information relates to the destination of the use of BIAS because it can identify the endpoint for inbound communications.

82. We disagree with commenters who argue that we should not consider CPE and by extension other customer device information to be CPNI because CPE and other customer devices are also used for purposes other than BIAS, or because such information may be available to other parties.[185] As discussed above,[186] what matters is the nature of the information made available to the BIAS provider through its provision of service.

83. We disagree with NTCA, which misinterprets the Bureau-level *1998 CPNI Clarification Order* to argue that the Commission has previously found that CPE is not covered by Section 222.[187] In the *1998 CPNI Clarification Order*, the Bureau addressed the issue of "customer information independently derived from the carrier's prior sale of CPE to the customer or the customer's subscription to a particular information service offered by the carrier in its marketing of new CPE[.]"[188] By contrast, here we are addressing information about the CPE itself that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship, i.e., information derived in the course of providing BIAS or another telecommunications service.

84. *Other Types of CPNI.* We reiterate that the examples of CPNI discussed above are illustrative, not exhaustive. To the extent that other types of information satisfy the statutory definition of CPNI, those data may also be CPNI, either in the BIAS context or in the context of other telecommunications services.

#### b. Customer Proprietary Information (Customer PI)

85. Section 222(a) imposes a general duty on all telecommunications carriers "to protect the confidentiality of proprietary information of, and relating to, . . . customers."[189] "[P]roprietary information of, and relating to, . . . customers" is information that BIAS providers and other telecommunications carriers acquire in connection with their provision of service, which customers have an interest in protecting from disclosure.[190] We call this information "customer proprietary information" or "customer PI." Customer PI consists of three non-mutually-exclusive categories: (1) individually identifiable customer proprietary network information (CPNI), (2) personally identifiable information (PII), and (3) content of communications.[191] This interpretation of Section 222(a) is consistent with other provisions of the Communications Act that use the term "proprietary information,"[192] and with the

[185] *See id.* at 23-25.

[186] *See supra* para. 49

[187] *See* NTCA Comments at 25; *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Order, 13 FCC Rcd 12390, 12392-93, paras. 2-4 (CC Bur. 1998) (*1998 CPNI Clarification Order*).

[188] *1998 CPNI Clarification Order*, 13 FCC Rcd at 12393, para. 4.

[189] 47 U.S.C. § 222(a).

[190] *See TerraCom NAL*, 29 FCC Rcd at 13330-32, paras. 14-20 (defining the scope of the term "proprietary information").

[191] *See infra* Parts III.B.3.c, III.B.3.d.

[192] *See TerraCom NAL*, 29 FCC Rcd at 13330-31, para. 15 ("In the context of public broadcasting, for example, the Corporation for Public Broadcasting (CPB) must maintain for public inspection certain financial information about programming grants. But Congress also recognized that 'proprietary, confidential, or privileged information' should not be made public, and Congress thus expressly excluded such information from public disclosure. Similarly, . . . [r]ecognizing that [entities that review interoperability of telephone equipment] necessarily gain access to extremely (continued….)

Commission's use of that term before enactment of Section 222.[193] As we discuss in more detail below, protecting PII and content is at the heart of most privacy regimes[194] and we recognized in *TerraCom* that the Communications Act protects them as customer PI because it "clearly encompasses private information that customers have an interest in protecting from public exposure."[195]

86. As we previously explained, "[i]n the context of Section 222, it 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.[196] We reaffirm our conclusion that 'proprietary information' in Section 222(a), as applied to customers . . . clearly encompass[es] private information that customers have an interest in protecting from public exposure."[197] As such, we disagree with commenters that argue that the word "proprietary" in Section 222(a) means the statute only protects information the customer keeps secret from any other party.[198] If only secret information qualified as private information, then not even Social Security numbers would be "proprietary" and subject to the protections of Section 222 and our implementing rules.[199] People regularly give their Social Security numbers to banks, doctors, utility companies, telecommunications carriers, employers, schools, and other parties in order to obtain various services – but this does not mean the information is not "proprietary" to them. To define "proprietary" as these commenters propose would render Section 222(a) at worst meaningless and at best leaving a gap whereby sensitive proprietary information like a Social Security number would be unprotected.[200]

87. We disagree with commenters that assert that defining the category of customer PI in this way would dramatically expand the scope of providers' duties to protect private customer

(Continued from previous page)
valuable trade secrets, Congress explicitly prohibited those review entities from 'releasing or otherwise using any proprietary information' belonging to the manufacturer without written authorization."); *see also* CDT Comments at 12.

[193] *See Furnishing of Customer Premises Equipment and Enhanced Services by American Telephone & Telegraph Co.*, Order, 102 F.C.C.2d 655, 692-93, para. 64 (1985) (discussing 47 C.F.R. § 64.702 (1984) and noting that "customer proprietary information … belongs to the customers, and many may not want it to be made public").

[194] *See infra* Part III.B.3.c. *See, e.g.*, 18 U.S.C. § 2710 (Video Privacy Protection Act); 18 U.S.C. §§ 2721-2725 (Driver's Privacy Protection Act); 45 CFR pt. 164 (HIPAA rules); 16 CFR pt. 313 (Gramm-Leach-Bliley Act rules); 16 CFR pt. 682 (Fair Credit Reporting Act rules); 12 CFR pt. 1022 (Fair and Accurate Credit Transaction Act disposal rule); 45 CFR pt. 5b (Privacy Act rules); 34 CFR pt. 99 (FERPA rules); 16 CFR pt. 312 (COPPA rules); 2015 Administration CPBR Discussion Draft § 4(a)(1). *See also* CDT Comments at 8-9; Electronic Privacy Information Center (EPIC) Comments at 14-15.

[195] *TerraCom NAL*, 29 FCC Rcd at 13330-31, paras. 14, 17.

[196] *Id.*, para. 14.

[197] *Id*.

[198] *See* CTIA Comment at 33-34 (arguing that information cannot be proprietary if it is available to others); NTCA Comments at 28-29 (many types of PII are publicly available). *But see* Free Press Reply at 8-10 ("That edge providers may have access to certain kinds of 'Proprietary Information' is immaterial to whether the FCC can protect the use of that information by broadband ISPs.").

[199] *See* Daniel J. Solove, Nothing to Hide 178 (2011) ("The problem with the secrecy paradigm is that we *do* expect some degree of privacy in public. We don't expect total secrecy, but we also don't expect somebody to be recording everything we do.") (emphasis in original). A panopticon limited to the public sphere can still infringe the dignity of the private individual. *See United States v. Jones*, 132 S.Ct. 945, 955 (2012) (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.").

[200] *See Corley v. United States*, 556 U.S. 303, 314 (2009) ("a statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant") (internal quotation marks, alterations, and citation omitted).

information.[201] Based on the record before us, we find that BIAS providers—like other telecommunications carriers—are already on notice that they have a duty to keep such information secure and confidential based on, among other things, FTC guidance that applied to them prior to the reclassification of broadband in the *2015 Open Internet Order*.[202] According to FTC staff, "[t]o date, the FTC has brought over 500 cases protecting the privacy and security of consumer information."[203] We have held providers responsible for protecting these private data under Section 222(a).[204] In *TerraCom*, we also found that the failure to protect customer's private information was an unjust and unreasonable practice under Section 201(b).[205] Likewise, providers have been required to protect the content of communications for decades.[206] Moreover, customers reasonably expect and want their providers to keep these data secure and confidential.[207] Surveys reflect that 74 percent of Americans believe it is "very important" to be in control over their own information; as a Pew study found, "[i]f the traditional American view of privacy is the 'right to be left alone,' the 21st-century refinement of that idea is the right to control their identity and information."[208] We agree with the Center for Democracy & Technology that "[e]xcluding PII from the proposed rules would be contrary to decades of U.S. privacy regulation and public policy."[209] We also observe that omitting PII from the scope of these rules would

[201] *See* Competitive Carriers Association (CCA) Comments at 4 (proposal is a "significant expansion" of coverage); CenturyLink Comments at 35-36 ("broad scope" of coverage could increase compliance costs); INCOMPAS Comments at 8 ("sweeping alterations to the current framework"); Internet Commerce Coalition (ICC) Comments at 13 (broader coverage than previous rules); USTelecom Comments at 7 ("massive expansion" of coverage under Section 222); WISPA Comments at 12-13 ("vast expansion of the universe of information that would be subject to protection").

[202] *See* 2012 FTC Privacy Report at v, vii-ix, 15-22; *see also* ACLU Comments at 2-3 ("The nation's mail, telephone, and telegraph infrastructures have long been subject to rules protecting [Americans'] privacy.").

[203] FTC Staff Comments at 4. *See, e.g.*, *FTC v. E.M.A. Nationwide, Inc.*, 767 F.3d 611 (6th Cir. 2014); *FTC v. Accusearch, Inc.*, 570 F.3d 1187 (10th Cir. 2009); *FTC v. INC21.com Corp.*, 688 F.Supp.2d 927 (N.D. Cal. 2010), *aff'd*, 475 Fed. Appx. 106 (9th Cir. 2012); *Snapchat, Inc.*, Decision & Order, FTC Docket No. C-4501 (Dec. 23, 2014), https://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter; *Accretive Health, Inc.*, Decision & Order, FTC Docket No. C-4432 (Feb. 5, 2014), https://www.ftc.gov/enforcement/cases-proceedings/122-3077/accretive-health-inc-matter; *Compete, Inc.*, Decision & Order, FTC Docket No. C-4384 (Feb. 20, 2013), https://www.ftc.gov/enforcement/cases-proceedings/102-3116/compete-inc.

[204] *See, e.g.*, *TerraCom NAL*, 29 FCC Rcd at 13325, para. 2; *Cox Commc'n Inc.*, Order, 30 FCC Rcd 12302, 12303, para. 4. (Enf. Bur. 2015) (*Cox Consent Decree*); *Verizon UIDH Consent Decree*, 31 FCC Rcd at 1843, para. 2.

[205] *See TerraCom NAL*, 29 FCC Rcd at 13325, para. 2.

[206] *See* 47 U.S.C. § 605; 18 U.S.C. § 2511 (ECPA); *see also infra* Part III.B.3.d.

[207] *See* Lee Rainie, The State of Privacy in post-Snowden America, Pew Research Center (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ (91 percent of Americans agree that consumers have lost control of how personal information is collected and used by companies and 68 percent support more protective privacy and data retention laws); Rafi Goldberg, NTIA, Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities (May 13, 2016), https://www.ntia.doc.gov/print/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities (consumers change their online behavior if they believe their privacy is compromised); Morrison & Foerster, Consumer Outlooks on Privacy, 7 (2016), www.mofo.com/~/media/Files/Resources/2016/MoFoInsightsConsumerOutlooksPrivacy.pdf (describing consumer privacy expectations).

[208] Lee Rainie, The State of Privacy in post-Snowden America, Pew Research Center (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

[209] CDT Comments at 8-9 (citing regulations issued under Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act (FCRA), Fair and Accurate Credit

(continued….)

result in a gap in protection for PII under the Act's primary privacy regime for telecommunications services.[210] Thus, were PII not included within the scope of customer PI, sensitive PII like Social Security numbers or private medical records would receive fewer protections than a broadband plan's monthly data allowance, a result we do not think intended by Congress. We discuss and define PII below.

### c. Personally Identifiable Information (PII)

88. Protecting personally identifiable information is at the heart of most privacy regimes.[211] Historically, legal definitions of PII have varied. Some incorporated checklists of specific types of information; others deferred to auditing controls. Privacy protections must evolve and improve as technology—and our understanding of its potential—evolves and improves.[212] Our definition incorporates this modern understanding of data privacy and tracks the FTC, the Administration's proposed CPBR, and National Institute of Standards and Technology (NIST) guidelines on PII.[213]

89. We define personally identifiable information, or PII, as any information that is linked or reasonably linkable to an individual or device.[214] Information is linked or reasonably linkable to an individual or device if it can reasonably be used on its own, in context, or in combination to identify an individual or device, or to logically associate with other information about a specific individual or device.[215] The "linked or reasonably linkable" standard for determining the metes and bounds of personally identifiable information is well established and finds strong support in the record.[216] In addition to NIST, CPBR, and the FTC, the Department of Education, the Securities and Exchange

(Continued from previous page)
Transactions Act (FACTA), Privacy Act, Family Educational Rights and Privacy Act (FERPA), the Communications Act, Telephone Consumer Protection Act (TCPA), Children's Online Privacy Protection Act (COPPA), and CAN-SPAM Act of 2003).

[210] The Act also protects the PII of cable and satellite subscribers. *See* 47 U.S.C. § 338(i); 47 U.S.C. § 551 (collectively, "Satellite and Cable Privacy Acts").

[211] *See, e.g.*, Satellite and Cable Privacy Acts; 18 U.S.C. § 2710 (Video Privacy Protection Act (VPPA)); 18 U.S.C. §§ 2721-2725 (Driver's Privacy Protection Act (DPPA)); 45 CFR pt. 164 (HIPAA rules); 16 CFR pt. 313 (GLBA rules); 16 CFR pt. 682 (FCRA rules); 12 CFR pt. 1022 (FACTA disposal rule); 45 CFR pt. 5b (Privacy Act rules); 34 CFR pt. 99 (FERPA rules); 16 CFR pt. 312 (COPPA rules); 2015 Administration CPBR Discussion Draft § 4(a)(1). *See also* CDT Comments at 8-9; EPIC Comments at 14-15.

[212] *Compare Olmstead v. United States*, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting) ("[O]ur contemplation cannot be only of what has been, but of what may be. The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."), *with Riley v. California*, 134 S.Ct. 2473, 2490 (2014) ("Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate.").

[213] In the *TerraCom NAL*, we found NIST guidelines to be "informative" for determining the scope of PII; similarly we use those guidelines to inform our rule here. *See TerraCom NAL*, 29 FCC Rcd at 13331, para. 17; NIST, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) at § 2.1 (2010), http://www.nist.gov/manuscript-publication-search.cfm?pub_id=904990 (NIST PII Guide); 2012 FTC Privacy Report at 18-22; 2015 Administration CPBR Discussion Draft at § 4(a)(1). *See also Cox Consent Decree*, 30 FCC Rcd at 12306-07, paras. 2(s), 4.

[214] *See infra* Appx. A, at § 64.2002.

[215] *See* NIST PII Guide § 2.1 (defining linked and linkable); CDT Comments at 9 ("'Identifiable' information is increasingly contextual; while one or two data points alone may not identify an individual, these data could be linked to that person if combined with other data.").

[216] *See, e.g.*, Access Now Comments at 5; CDT Comments at 9-10; EFF Comments at 5; EPIC Comments at 18-19; Front Porch Comments at 2; FTC Staff Comments at 9; Public Knowledge Comments at 28.

Commission, the Department of Defense, the Department of Homeland Security, the Department of Health and Human Services, and the Office of Management and Budget all use a version of this standard in their regulations and policies.[217]

90. We agree with the FTC staff that "[w]hile almost any piece of data *could* be linked to a consumer, it is appropriate to consider whether such a link is practical or likely in light of current technology."[218] While we recognize that "'[i]dentifiable' information is increasingly contextual"[219]—especially when a provider can cross-reference multiple types and sources of information—anchoring the standard to a mere "possibility of logical association"[220] could result in "an overly-expansive definition."[221] Thus, we adopt the recommendation of the FTC staff and others to add the term "reasonably" to our proposed "linked or linkable" definition of PII.[222] This conclusion has broad support in the record.[223]

91. We also adopt the FTC staff recommendation that PII should include information that is linked or reasonably linkable to a customer device.[224] We agree with the FTC staff that "[a]s consumer devices become more personal and associated with individual users, the distinction between a device and its user continues to blur."[225] The Digital Advertising Alliance likewise recognizes the connection between individuals and devices, stating in its guidance that information "connected to or associated with a particular computer or device" is identifiable.[226] While some commenters argue that we should not include information linkable to a device in the definition of PII,[227] we find that such identifiers are often and easily linkable to an individual, as we discussed above.[228]

---

[217] *See* NIST PII Guide §§ 2.1-2.2; 2012 FTC Privacy Report at 18-22; 2015 Administration CPBR Discussion Draft at § 4(a)(1); 34 CFR §§ 99.3, 303.29; 17 CFR § 227.305(b); 32 CFR §§ 310.4, 311.3(g), 329.3; 6 CFR § 37.3; 45 CFR § 75.2; 2 CFR § 200.79. *See also* Clay Johnson III, Deputy Director for Management, Office of Management and Budget, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, at 1 n.1 (2007), https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.

[218] FTC Staff Comments at 9 (emphasis in original).

[219] CDT Comments at 10.

[220] NIST PII Guide § 2.1.

[221] Software & Information Industry Association (SIIA) Comments at 11-12.

[222] FTC Staff Comments at 9.

[223] *See* AT&T Reply at 39-40 (supporting reasonableness qualifier); T-Mobile Comments at 20 (linkability standard overbroad without a reasonableness qualifier like the FTC); CompTIA Comments at 2-3 (same); CTIA Comments at 38 (same); NCTA Reply at 40 (same); SIIA Reply at 3 (same); WISPA Reply at 16-17; Cincinnati Bell Comments at 5 ("[T]he Commission's PII regime should mirror the existing FTC definitions.").

[224] FTC Staff Comments at 10. As discussed above, devices in the BIAS context include a customer's smartphone, tablet, computer, modem, router, videophone, IP caption phone, and other consumer devices capable of connecting to broadband services. *See supra* para. 80.

[225] FTC Staff Comments at 10. *Accord* EPIC Comments at 18 (discussing how persistent identifiers like device information can be used to map out an individual's interactions); SIIA Comments at 12 (supporting the FTC's test for linkability to a "consumer, computer, or device").

[226] Digital Advertising Alliance, Application of Self-Regulatory Principles to the Mobile Environment, 6 (July 2013), http://www.aboutads.info/DAA_Mobile_Guidance.pdf (DAA Mobile Guidance) (defining "De-Identification Process").

[227] *See* Audience Partners Comments at 9-17; Future of Privacy Forum Comments at 5.

[228] *See supra* paras. 67-71.

92. We disagree with commenters that argue that PII should only include information that is sensitive or capable of causing harm if disclosed.[229] The ability of information to identify an individual defines the scope of PII. Whether or not any particular PII is sensitive or capable of causing harm if disclosed is a separate question from the definitional question of identifiability.[230] We address the treatment of sensitive versus non-sensitive information below.[231]

93. We agree with commenters that we should offer illustrative, non-exhaustive examples of PII.[232] We have analyzed descriptions of PII in the record, our prior orders,[233] NIST,[234] the FTC,[235] the Administration's proposed CPBR,[236] and other federal and state statutes and regulations.[237] We find that examples of PII include, but are not limited to: name; Social Security number; date of birth; mother's maiden name; government-issued identifiers (e.g., driver's license number); physical address; email address or other online contact information;[238] phone numbers; MAC addresses or other unique device identifiers; IP addresses; and persistent online or unique advertising identifiers. Several of these data elements may also be CPNI.

94. We disagree with commenters that argue that we should not consider MAC addresses, IP addresses, or device identifiers to be PII.[239] First, as discussed above,[240] a customer's IP address and

[229] *See* CenturyLink Comments at 16; Cincinnati Bell Comments at 7.

[230] "I find little comfort in the Court's notion that no invasion of privacy occurs until a listener obtains some significant information by use of the device. . . . A bathtub is a less private area when the plumber is present even if his back is turned." *Kyllo v. United States*, 533 U.S. 27, 39 (2001) (quoting *U.S. v. Karo*, 468 U.S. 705, 735 (1984) (Stevens, J., concurring in part and dissenting in part)). *See also* EPIC Comments at 18.

[231] *See infra* Part III.D.1.

[232] *See, e.g.*, Access Now Comments at 5; CDT Comments at 8-10; Consumer Watchdog Comments at 5; EFF Comments at 5; EPIC Comments at 18-19; OTI Comments at 22; Return Path Comments at 5.

[233] *See, e.g.*, *TerraCom NAL*, 29 FCC Rcd at 13331-32, paras. 17-18; *see also AT&T Services, Inc.*, Order and Consent Decree, 30 FCC Rcd 2808, 2811, para. 2(s) (Enf. Bur. 2015) (*AT&T Consent Decree*).

[234] *See* NIST PII Guide §§ 2.1-2.2.

[235] *See, e.g.*, *FTC v. Accusearch, Inc.*, 570 F.3d 1187 (10th Cir. 2009); *Snapchat, Inc.*, Decision and Order, F.T.C. Docket No. C-4501 (Dec. 23, 2014), https://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter; *Accretive Health, Inc.*, Decision and Order, F.T.C. Docket No. C-4432 (Feb. 5, 2014), https://www.ftc.gov/enforcement/cases-proceedings/122-3077/accretive-health-inc-matter; *Compete, Inc.*, Decision and Order, F.T.C. Docket No. C-4384 (Feb. 20, 2013), https://www.ftc.gov/enforcement/cases-proceedings/102-3116/compete-inc; *Craig Brittain,* Decision and Order, F.T.C. Docket No. C-4564 (Dec. 28, 2015), https://www.ftc.gov/enforcement/cases-proceedings/132-3120/craig-brittain-matter.

[236] 2015 Administration CPBR Discussion Draft § 4(a)(1).

[237] *See, e.g.*, DPPA, 18 U.S.C. § 2725(3)-(4); COPPA, 15 U.S.C. § 6501(8); COPPA Rule, 16 CFR § 312.2; GLBA, 15 U.S.C. § 6809(4); 12 CFR § 1022.3(g) (FCRA regulations); California Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code § 22577(a); California Consumer Protection Against Computer Spyware Act, Cal. Bus. & Prof. Code § 22947.1(k); Cal. Civ. Code § 1798.82(h); Conn. Gen. Stat. Ann. § 36a-701b(a); N.Y. Gen. Bus. Law §§ 899-aa(1)(a), (b); La. Stat. Ann. § 51:3073(4); Fla. Stat. § 501.171(1)(g).

[238] OTI asks us to clarify the meaning of "other online contact information." OTI Comments at 22. The term is meant to be technology neutral and encompass other methods of BIAS-enabled direct messaging. *See also* 16 CFR § 312.2 (defining "online contact information" for the COPPA Rule).

[239] *See* Audience Partners Comment at 11-13 ("IP addresses are incapable of identifying an individual without being linked to additional information"); Direct Marketing Association (DMA) Comments at 17 (information "that does not, on its own, identify a specific individual" should not qualify as PII); IAB Comments at 10 (an "anonymous identifier" should not qualify as PII); NCTA Comments at 22 (MAC addresses and IP addresses cannot identify an individual on their own); Front Porch Comments at 2-3 (IP addresses should not qualify as PII because while they

(continued….)

MAC address each identify a discrete customer and/or customer device by routing communications to a specific endpoint linked to the customer. Information does not need to reveal an individual's name to be linked or reasonably linkable to that person. A unique number designating a discrete individual—such as a Social Security number or persistent identifier—is at least as specific as a name.[241] Second, MAC addresses, IP addresses, and other examples of PII do not need to be able to identify an individual in a vacuum to be linked or reasonably linkable. BIAS providers can combine this information with other information to identify an individual (e.g., the BIAS provider's records of which IP addresses were assigned to which customers, or traffic statistics linking MAC addresses with other data).[242] As the Supreme Court has observed, "[w]hat may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context."[243]

95. *Customer Contact Information — Names, Addresses, and Phone Numbers of Individuals.* Names, addresses, telephone numbers, and other information that is used to contact an individual are classic PII because they are linked or reasonably linkable to an individual or device.[244] Some commenters argue that contact information is not protected under Section 222 because "Subscriber list information" is exempt from the choice requirements for CPNI under Section 222(e). However, subscriber list information, a relatively small subset of customer contact information, was subject to other considerations at the time of enactment.

96. Subscriber list information is defined in the statute as "any information (A) identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and (B) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format."[245] Through this definition, Congress recognized that a dispositive factor is whether the information has been published or accepted for publication in a directory format.

(Continued from previous page)
"might be issued to a subscriber for a period of time, a personal IP address can also change at any time, and therefore, is not reliable.").

[240] *See supra* paras. 67-71.

[241] In many cases, a unique numerical identifier will be *more* specific than the person's actual name. *See, e.g.*, Mona Chalabi and Andrew Flowers, *Dear Mona, What's the Most Common Name in America?*, FiveThirtyEight (Nov. 20, 2014), http://fivethirtyeight.com/features/whats-the-most-common-name-in-america/ (discussing the large number of people with common names such as James Smith or Maria Garcia).

[242] *See* CDT Comments at 13-14, 16 (discussing how MAC addresses and IP addresses in protocol headers, as well as other traffic statistics, can be shared with BIAS providers, allowing the provider to link them to the subscriber); Feamster Edge Provider Comments at 2 (BIAS providers can "link information about IP addresses seen in network traffic traces to CPNI from its subscribers"). In situations where the BIAS provider sold or leased a device to a customer—such as a smartphone, modem, or router—the provider could associate device identifiers with the customer from its records. *See* Sandvine Comments at 22 ("In some domains a device is fairly synonymous with a person (e.g., mobile phone).").

[243] *CIA v. Sims*, 471 U.S. 159, 178 (1985) (internal quotation marks, alterations, and citation omitted); *see also U.S. v. Maynard*, 615 F.3d 544, 561-63 (D.C. Cir. 2010), *aff'd on other grounds sub nom.*, *United States v. Jones*, 132 S.Ct. 945 (2012) ("Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what person does repeatedly, what he does not do, and what he does ensemble."); 2016 FTC Big Data Report at 3-5 (discussing the "Life Cycle of Big Data"). *See also* Access Now Comments at 5 ("[S]eemingly anonymous information can often—and easily—be re-associated with identified individuals.").

[244] FTC Staff Comments at 11.

[245] 47 U.S.C. § 222(h)(3).

97. The legislative history shows that Congress created a narrow carve out from the definition of CPNI for subscriber list information in order to protect the longstanding practice of publishing telephone books and to promote competition in telephone book publishing.[246] The legislative history is clear that Congress did not intend for subscriber list information "to include any information identifying subscribers that is prepared or distributed within a company or between affiliates or that is provided to any person in a non-public manner."[247] Instead, Congress intended subscriber list information to be "data that local exchange carriers traditionally and routinely make public. Subscribers have little expectation of privacy in this information because, by agreeing to be listed, they have declined the opportunity to limit its disclosure."[248] Based on this legislative history, we find that the phrase "published, caused to be published, or accepted for publication in any directory format" is best read as limited to publicly available telephone books of the type that were published when Congress enacted the statute, or their direct equivalent in another medium, such as a website republishing the contents of a publicly available telephone book.

98. Unlike landline voice carriers, neither mobile voice carriers nor broadband providers publish publicly-available directories of customer information.[249] Nor does the record reflect more than speculation about any future interest in publishing directories.[250] Because publishing of broadband customer directories is neither a common nor a long-standing practice, we find that broadband customers have no expectation that that they are consenting to the public release of their name, postal address, or telephone number when they subscribe to BIAS.[251] We therefore conclude that a directory of BIAS customers' names, addresses, and phone numbers would not constitute information published in a "directory format" within the meaning of the statute, and therefore there is no "subscriber list information" in the broadband context.[252] As such, we disagree with commenters who ask us to ignore

[246] S. CONF. REP. NO. 104-230 at 205 (1996) ("The subscriber list information provision guarantees independent publishers access to subscriber list information at reasonable and nondiscriminatory rates, terms and conditions from any provider of local telephone service."). In an earlier report, the Senate stated, "This provision is intended to assure that persons who utilize subscriber information, including publishers of telephone directories unaffiliated with local exchange carriers, are able to purchase published or to-be-published subscriber listings and updates from carriers on reasonable terms and conditions." S. REP. NO. 103-367 at 97 (1994). *See also* 47 U.S.C. § 222(e) (requiring carriers providing telephone exchange service to make subscriber list information available to directory publishers on nondiscriminatory and reasonable terms).

[247] H.R. REP. NO. 104-204 at 91 (1995).

[248] S. REP. NO. 103-367 at 97 (1994).

[249] *See* T-Mobile Comments at 21-22 ("[B]roadband providers do not publish directories of customer information today."). Section 222(e) likewise recognizes that subscriber list information is the publication of directories in the context of telephone exchange service. *See* 47 U.S.C. § 222(e) ("Notwithstanding subsections (b), (c), and (d) of this section, a telecommunications carrier that provides telephone exchange service shall provide subscriber list information gathered in its capacity as a provider of such service on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions, to any person upon request for the purpose of publishing directories in any format.").

[250] *See, e.g.*, T-Mobile Comments at 22 (stating that providers "may" publish directories in the future, but not identifying any concrete plans to do so).

[251] *Cf.* S. REP. NO. 103-367 at 97 (1994) (when subscribers "declin[e] the opportunity to limit [subscriber list information's] disclosure" they "have little expectation of privacy" in it). *See also* Greenlining Institute Comments at 50 ("the 'subscriber list' exception to CPNI applies narrowly, relates only to listing information exchanged between those actually in the business of publishing directories and actually used for that purpose").

[252] *See, e.g.*, Greenlining Institute Comments at 45-46 (supporting this conclusion); $S^2$ERC Comments at 8 (same).

the publication requirement in order to exempt names, addresses, telephone numbers, and IP addresses from these rules.[253]

99. We recognize that the Commission has previously found that names, addresses, and telephone numbers are not CPNI, even when not published as subscriber list information.[254] However, the Commission has not analyzed whether such customer contact information is PII, and therefore subject to protections under Section 222(a). As discussed above, we make clear today that it is PII.[255]

100. *Harmonization.* We agree with the American Cable Association and various small providers who urge us to harmonize our BIAS and voice definitions under Section 222.[256] Having one uniform set of definitions will simplify compliance and reduce consumer confusion. This is especially true for small providers who collect less customer information, use it for narrower purposes, and do not have the resources to maintain a bifurcated system. Consequently, we extend this definition of PII to all Section 222 contexts.

### d. Content of Communications

101. We find that the Act protects the content of communications as customer PI. Content is a quintessential example of a type of "information that should not be exposed widely to the public . . . [and] that customers expect their carriers to keep private."[257] Content is highly individualistic, private, and sensitive.[258] Except in limited circumstances where savvy customers deploy protective tools, BIAS providers often have access to at least some, if not most, content through their provision of service.[259] We agree with FTC staff that "[c]ontent data can be highly personalized and granular, allowing analyses that

[253] *See* T-Mobile Comments at 21-22; ICC Comments at 13-14 (arguing that IP addresses are analogous to subscriber list information and that names and addresses are "widely available"); DMA Comments at 13-14 (seeking "exemptions based on comparisons of" subscriber list information and certain types of information in the BIAS context); NTCA Comments at 29-30 (arguing that customer names, addresses, and telephone numbers should not be protected by these rules).

[254] *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, 14487, para. 146-47 (1999) (*1999 CPNI Reconsideration Order*) (adopting the conclusions of the Common Carrier Bureau in the *1998 CPNI Clarification Order*); *1998 CPNI Clarification Order*, 13 FCC Rcd at 12395-96, paras. 8-9 (finding that names, addresses, and telephone numbers are not CPNI).

[255] As PII, this information is subject to our customer choice rules, discussed in detail below. *See infra* Part III.D. Our customer choice rules will continue to allow this information to be used to publish publicly available telephone directories, consistent with the current practice of allowing customers to keep their information unlisted.

[256] *See* ACA Comments at 57-58; WTA & Nex-Tech Apr. 25 *Ex Parte* at 1 (urging Commission to "harmonize definitions, procedures and requirements in order to reduce the complexity of regulation of privacy and minimize the burdens on small providers").

[257] *TerraCom NAL*, 29 FCC Rcd at 13330-31, paras. 14, 16.

[258] *See* 2012 FTC Privacy Report at 55-56 (expressing concern regarding the potential for ISPs to use content for purposes other than providing service); FTC Staff Comments at 20-21 (supporting privacy protection for content); *accord* ACLU Comments at 7-8; AAJ Comments at 9; EFF Comments at 5; EPIC Comments at 26; OTI Comments at 23; Public Knowledge White Paper at 59. *See also infra* Part III.D.1.a.(i).

[259] *See* Public Knowledge White Paper at 48 (arguing that BIAS providers can view unencrypted payloads); CDT Comments at 17 ("BIAS subscribers sending and receiving unencrypted transmissions are no less deserving of privacy protections than subscribers who only visit sites supporting HTTPS or who employ proxy or VPN services."). BIAS providers' inability to access encrypted content is irrelevant; what matters is the information the BIAS providers *can* access. Moreover, even when traffic is encrypted, some content may remain visible or inferable to the provider. *See infra* para. 180.

would not be possible with less rich data sets."[260] In recognition of its importance, Congress has repeatedly and emphatically protected the privacy of communications content in various legal contexts, expressly prohibiting service providers from disclosing the contents of communications they carry, subject to statutorily enumerated exceptions, since at least 1912.[261] We agree with commenters that "Americans do not expect their broadband providers to be reading their electronic communications any more than they expect them to be keeping a list of their correspondents."[262] The same rationale that supports the treatment of the content of BIAS communications as customer PI supports the treatment of the content carried through other telecommunications services as customer PI.

102. *Definition of Content*. At the outset, we define content as any part of the substance, purport, or meaning of a communication or any other part of a communication that is highly suggestive of the substance, purpose, or meaning of a communication. We sought comment on how to define content in the *NPRM*, but received no substantive recommendations; consequently we base our definition on the long-established terminology of ECPA and Section 705.[263] We recognize that sophisticated monitoring techniques have blurred the line between content and metadata, with metadata increasingly being used to make valuable determinations about users previously only possible with content.[264] This has complicated traditional notions of how to define and treat content. We intend our definition to be flexible enough to encompass any element of the BIAS communication that conveys or implies any part of its substance, purport, or meaning. As a definitional matter, content in an inbound communication is no different from content in an outbound communication. As discussed above, because the categories of customer PI are not mutually exclusive, some content may also satisfy the definitions of CPNI and/or PII.[265]

103. Multiple components of an IP data packet may constitute or contain BIAS content.[266] First and foremost, we agree with commenters that the application payload is always content.[267] As

[260] FTC Staff Comments at 20.

[261] *See, e.g.*, An Act to Regulate Radio Communications, ch. 287, § 4, Reg. 19, 37 Stat. 302, 307 (1912); Radio Act of 1927, ch. 169, § 27, 44 Stat. 1162, 1172; Communications Act of 1934, ch. 652, § 605, 48 Stat. 1064, 1103-04; 47 U.S.C. § 605; 18 U.S.C. §§ 2510-2522; 18 U.S.C. §§ 2701-2712; 18 U.S.C. §§ 3121-3127.

[262] ACLU Comments at 7; *see also* OTI Comments at 23 ("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.").

[263] *See* 18 U.S.C. § 2510(8) ("'[C]ontents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication."); 47 U.S.C. § 605(a) (restricting the disclosure of "the existence, contents, substance, purport, effect, or meaning" of a communication by wire or radio). *See also* OTI Comments at 23 (quoting Section 705 and supporting content protections).

[264] *See* Mozilla Comments at 4 ("Usage patterns and metadata can be as revealing, or in some ways even more revealing, than content."); CDT Comments at 16 ("Such detailed information about a customer's communications may reveal more than just patterns of broadband usage; but also clues as to the content of those communications and the behaviors and interests of that customer."). *See also, e.g.*, *Riley v. California*, 134 S.Ct. 2473, 2490 (2014) (Cell phones carry "a digital record of nearly every aspect of [people's] lives—from the mundane to the intimate."); *United States v. Maynard*, 615 F.3d 544, 561-63 (D.C. Cir. 2010), *aff'd on other grounds sub nom.*, *United States v. Jones*, 132 S.Ct. 945 (2012) ("Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble.").

[265] *See supra* Part III.B.3.b. Because we conclude that Section 222(a) protects content as its own category of customer PI, we need not determine which types of content are also CPNI or PII.

[266] *See supra* Part III.B.3.a(i)(a).

[267] *See* EPIC Comments at 26 (quoting Tim Berners-Lee) ("The access by an ISP of information within an internet packet, other than that information used for routing, is equivalent to wiretapping a phone or opening sealed postal mail."); OTI Comments at 23 ("Recognizing packet contents as communications contents, and establishing an opt-in (continued….)

discussed above,[268] the application payload is the part of the IP packet containing the substance of the communication between the customer and the entity with which she is communicating.[269] Examples of application payloads include the body of a webpage, the text of an email or instant message, the video served by a streaming service, the audiovisual stream in a video chat, or the maps served by a ride-sharing app.[270] However, other portions of the packet also may contain content.[271] For example, as discussed above, the application header may reveal aspects of the application payload from which the content may be easily inferred—such as source and destination email addresses or website URLs.[272] Application usage information may also reveal content by disclosing the applications customers use or the substance of how they use them.[273] We agree with FTC Staff that BIAS content includes, but is not limited to, the "contents of emails; communications on social media; search terms; web site comments; items in shopping carts; inputs on web-based forms; and consumers' documents, photos, videos, books read, [and] movies watched[.]"[274] We emphasize that our examples of BIAS content are not exhaustive and others may manifest over time as analytical techniques improve.

104. We reject arguments that protecting BIAS content under Section 222 is unnecessary or unlawful because Section 705 of the Act,[275] and the Electronic Communications Privacy Act (ECPA)[276] or the Communications Assistance for Law Enforcement Act (CALEA),[277] already protect content.[278] Commenters do not claim that these various other laws are mutually exclusive with each other, belying the notion that the existence of multiple sources of authority in this area is inherently a problem. Instead, we find that Section 222 complements these other laws in establishing a framework for protecting the

(Continued from previous page)
standard for content, would honor BIAS customers' reasonable expectation that their provider is not inspecting their traffic for purposes other than to provide service.").

[268] *See supra* Part III.B.3.a(i)(a).

[269] *See* Public Knowledge White Paper at 48 ("As revealing as the packet headers may be, the payloads potentially reveal far more information.").

[270] BIAS providers' use of application payloads for network management is also one reason why BIAS content is not wholly equivalent to telephone conversations. Voice carriers do not scan a phone conversation to secure the network or reduce congestion. Application payloads in the broadband Internet context are far more sophisticated and complex than mere audio transmissions over a telephone line. *See* Public Knowledge White Paper at 59.

[271] *See* Free Press Reply at 12 (arguing that BIAS providers can infer a significant amount about content by examining other elements of the packet).

[272] *See supra* para. 76; *see also* EPIC Comments at 26 (quoting Tim Berners-Lee) ("The URLs which people use reveal a huge amount about their lives, loves, hates, and fears. This is extremely sensitive material."); Andrew G. West & Adam J. Aviv, On the Privacy Concerns of URL Query Strings, 2014 Proc. of the 8th Workshop on Web 2.0 Sec. and Privacy, available at http://w2spconf.com/2014/papers/privacy_query_strings.pdf; (Reisman and Narayanan June 17, 2016 *Ex Parte* at 22-24 (observing that customer names and other PII are included in some URLs).

[273] *See supra* para. 78; *Riley v. California*, 134 S.Ct. at 2490 (The applications a person uses "can form a revealing montage of the user's life.").

[274] FTC Staff Comments at 20. *See also Riley v. California*, 134 S.Ct. at 2490 ("An Internet search and browsing history . . . could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.").

[275] 47 U.S.C. § 605(a).

[276] 18 U.S.C. §§ 2510-2522.

[277] 47 U.S.C. §§ 1001-1010.

[278] *See, e.g.*, Electronic Transactions Association Comments at 11; USTelecom Comments at 34; NCTA Comments at 96.

content carried by telecommunications carriers.[279] Given the importance of protecting content, it is reasonable to interpret Section 222 as creating additional, complementary protection.[280]

105. We also disagree with the argument that because the data protected by Section 705 "bear scant resemblance" to content or other forms of customer PI, our interpretation of Section 222 is erroneous.[281] Congress can enact two statutory provisions that contain different scopes, and it is a cardinal principle of statutory construction that we should attempt to give meaning to both. Any incongruity between the scope of Sections 222 and 705 only demonstrates that the statutes are complementary and part of Congress's broad scheme to protect customer privacy. Sections 222 and 705 independently require telecommunications carriers to protect communications content.

#### 4. De-identified Data

106. In this section we describe a corollary regarding the circumstances in which information that constituted customer PI (*i.e.*, PII, content, or individually identifiable CPNI) can comfortably be said to have been de-identified. As discussed below, based on the record we are concerned that carriers not be allowed to skirt the protections of our rules by making unsupported assertions that customer PI has been "de-identified" and thus is not subject to our consent regime, when in fact the information remains reasonably linkable to an individual or device. As 38 public interest organizations pointed out in a joint letter, "[i]t is often trivial to re-identify data that has supposedly been de-identified."[282] We accordingly adopt a strong, multi-part approach regarding the circumstances under which carriers can properly consider data to be de-identified, using the three part test for de-identification articulated by the FTC in 2012.[283] The Administration's CPBR also uses this standard.[284] Specifically, we find that customer proprietary information is de-identified if the carrier (1) determines that the information is not reasonably linkable to an individual or device; (2) publicly commits to maintain and use the data in a non-individually identifiable fashion and to not attempt to re-identify the data; and (3) contractually prohibits any entity to which it discloses or permits access to the de-identified data from attempting to re-identify the data.[285] We apply these requirements to both BIAS and other telecommunications services.[286]

---

[279] *See* ACLU Comments at 7-8 ("All of the reasons why Congress charged the Commission with protecting customer information 'that relates to the quantity . . . type, destination, location, and amount of use of a telecommunications service' without doubt apply to content as well. The Commission should make this clear despite existing laws that have some bearing on the legality of content monitoring by BIAS providers."); *see also* EFF Comments at 2-3.

[280] Similarly, for example, both the Children's Online Privacy Protection Act and the Video Privacy Protection Act may protect videos that young children watch online. *See* 18 U.S.C. § 2710; 15 U.S.C. § 6502.

[281] CTIA Comments at 64 ("Additionally, the *data types* protected by Section 705—the 'existence, contents, substance, purport, effect, or meaning' of a communication—bear scant resemblance to many of the elements of 'customer proprietary information' that the Proposed Rules seek to cover—*e.g.*, device identifiers, IP addresses, and so forth. These incongruities demonstrate that Section 705 does not provide authority for the Proposed Rules.") (emphasis in original).

[282] Letter from 38 Public Interest Organizations to the Honorable Tom Wheeler, Chairman, FCC at 2 (Sept. 7, 2016) (https://www.fcc.gov/ecfs/filing/10907040663545). *See also* CDD Comments at 17; EPIC Comments at 21-23; OTI Comments at 21-22; Privacy Rights Clearinghouse Comments at 5.

[283] The FTC approach has broad support in the record. *See, e.g.*, AT&T Reply at 36; Access Now Comments at 11; Audience Partners Comments at 17; CTIA Comments at 38; Email Sender & Provider Coalition Comments at 7-8; ICC Comments at 12; ITIF Comments at 19; Sprint Reply at 3-4; T-Mobile Comments at 35.

[284] 2015 Administration CPBR Discussion Draft at § 4(a)(2)(A).

[285] As discussed in greater detail below, this third part of the test applies to entities with which the provider contracts to share de-identified customer information. It does not apply to the general disclosure or publication of highly aggregated summary statistics that cannot be disaggregated—for example, the use of statistics in advertisements

(continued….)

### a. Adoption of the FTC's Multi-Part Test

107. The record reflects that advances in technology and data analytics make it increasingly difficult to de-identify information such that it is not re-identifiable.[287] The Administration's 2014 Big Data Report observed that "[m]any technologists are of the view that de-identification of data as a means of protecting individual privacy is, at best, a limited proposition."[288] As the Electronic Privacy Information Center notes, "[w]idely-publicized anonymization failures have shown that even relatively sophisticated techniques have still permitted researchers to identify particular individuals in large data sets."[289] We also agree with the FTC's conclusion in its 2012 Privacy Report that "not only is it possible to re-identify non-PII data through various means, businesses have strong incentives to actually do so."[290]

108. For these reasons, our approach to de-identification establishes a strong, technology-neutral standard as well as safeguards to mitigate the incentives to re-identify customers' proprietary information. Furthermore, because companies, including BIAS providers, have incentives to re-identify customer information so that it can be further monetized,[291] we agree with Privacy Rights Clearinghouse that the burden of proving that individual customer identities and characteristics have been removed from the data must rest with the provider.[292] Taking this burden assignment into account, we find that our multi-part approach, grounded in FTC guidance, will ensure that as technology changes, customer information is protected, while at the same time minimizing burdens and maintaining the utility of de-identified customer information.

(Continued from previous page)
(e.g., "We offer great coverage in rural areas, because that is where 70% of our customers live."); *see also* AT&T Comments at 70-71. *See infra* Part III.B.4.a(iii).

[286] The record does not demonstrate a need to treat de-identified information differently in the voice context versus the BIAS context. We agree with the Greenlining Institute and other commenters that a uniform regime, "is easier for the carriers, easier [for] enforcement, and easier for customers to understand[.]" Greenlining Institute Comments at 16. *See also* ACA Comments at 57-58 (supporting harmonization of Section 222 rules).

[287] *See* Privacy Rights Clearinghouse Comments at 5; OTI Comments at 6, 21-22 (stating that a recent study found that supposedly de-identified datasets from medical records, search queries, social network data, genetic information, geo-location data, and taxi-cab history could all be used to specifically identify individuals); *accord* CDD Comments at 17; EFF Comments 14; EPIC Comments at 22; OTI Reply at 12-13; Public Knowledge White Paper at 49-50. *See also, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010); U.S. Public Policy Council of the Association for Computing Machinery, *Response to Request for Information, Big Data Review*, 79 FR 12251 at 2, https://usacm.acm.org/images/documents/BigDataOSTPfinal.pdf. In 2000, Latanya Sweeney, now the Director of the Data Privacy Lab in the Institute for Quantitative Social Science at Harvard University, demonstrated that 87 percent of the population in the United States had reported characteristics that likely made them unique based only on 5-digit ZIP, gender, and date of birth. Latanya Sweeney, Abstract, *Uniqueness of Simple Demographics in the U.S. Population* (Carnegie Mellon Univ., Lab. For Int'l Data Privacy 2000), https://dataprivacylab.org/projects/identifiability/index.html. In 2008, researchers at the University of Texas at Austin succeeded in using publicly available information to identify Netflix subscribers in a dataset of movie ratings from which personal identifiers had been removed, explaining that "[r]emoving identifying information is not sufficient for anonymity." Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets, in Proceedings of the 2008 IEEE Symposium on Security and Privacy*, 111, 118 (2008), https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf.

[288] 2014 Administration Big Data Report at 8.

[289] EPIC Comments at 22.

[290] 2012 FTC Privacy Report at 20.

[291] *See id.*; CDD Comments at 20; EPIC Comments at 22-23.

[292] *See* Privacy Rights Clearinghouse Comments at 5.

109. As such, we disagree with those commenters who urge us to use a different de-identification framework, such as that used in the HIPAA safe harbor context.[293] We find that the framework we adopt enables flexibility to accommodate evolving technology and statistical methods. In contrast, we find that developing a list of identifiers that must be removed from data to render such data de-identified is not feasible given the breadth of data to which BIAS providers have access, and would also rapidly become obsolete in the evolving broadband context.

110. The three-part test we adopt today for de-identification also contemplates the statutory exception for "aggregate customer information," as it defines the circumstances in which the Commission will find that "individual customer identities and characteristics have been removed" from collective data.[294] Likewise, our approach addresses arguments in the record that the Commission must give meaning to the fact that the customer approval requirement of Section 222(c)(1) applies to "individually identifiable" CPNI,[295] as our test for de-identification addresses whether an individual's CPNI or PII will not be deemed to be individually identifiable in practice due to steps taken by the carrier prior to using or sharing the data.

#### (i) Part One – Not Reasonably Linkable

111. First, for information to be de-identified under our rules, we require providers to determine that the information is not linked or reasonably linkable to an individual or device.[296] Because we are describing the scope of what is identifiable, we think it is appropriate to use the same standard that we use to define personally identifiable information (PII).[297] Above we define PII as information that is linked or reasonably linkable to an individual or device, and conversely we find it appropriate to limit de-identified information to information that is *not* linked or reasonably linkable to an individual or device. As we discussed above in our definition of PII, we agree with commenters that the "linked or reasonably linkable" standard—used by the FTC in its Privacy Report—provides useful guidance on what it means for information to be individually identifiable without being either overly rigid or vague.[298] As we discussed above, information is linked or reasonably linkable to an individual or device if it can reasonably be used on its own, in context, or in combination (1) to identify an individual or device, or (2) to logically associate with other information about a specific individual or device.[299] New methods are increasingly capable of re-identifying information previously thought to be sufficiently anonymized.[300] For these reasons, we will not specify an exhaustive list of identifiers, nor will we declare certain

[293] *See, e.g.*, IMS Health Comments at 15.

[294] 47 U.S.C. § 222(h)(2) ("The term 'aggregate customer information' means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.").

[295] *See, e.g.*, AT&T Reply at 36-39; CTIA Comments at 36-37; CenturyLink Comments at 17; Comcast Reply at 47-48; Sprint Reply at 3-4; T-Mobile Comments at 34-35; Verizon Comments at 44.

[296] *See* 2012 FTC Privacy Report at 21; *see also* 2015 Administration CPBR Discussion Draft at Sec. 4(a)(2)(A); Access Now Comments at 11; CDT Comments at 9-10; EFF Comments at 14; EPIC Comments at 21-23; FTC Staff Comments at 9; Public Knowledge Comments at 28.

[297] *See supra* Part III.B.3.c.

[298] *See* 2012 FTC Privacy Report at 21-22; NTCA Comments at 57; *see also supra* note 283. *See also* 2015 Administration CPBR Discussion Draft at Sec. (4)(a)(2)(A) (defining "de-identified data" and requiring that it be "alter[ed] such that there is a reasonable basis for expecting that the data could not be linked as a practical matter to a specific individual or device"). *See also supra* para. 89.

[299] *See supra* Part III.B.3.c.

[300] *See supra* note 287.

techniques to be *per se* sufficient or insufficient to achieve de-identification.[301] The test instead focuses on the outcome required, that is, that to be de-identified, the data must no longer be linked or reasonably linkable to an individual or device. We also agree with AT&T that we should not "dictate specific approaches to de-identifying data" because "[a]ny Commission-mandated approach would quickly become obsolete as new de-identification techniques are developed."[302]

112. We make clear that reasonableness depends on ease of *re*-identification, not the cost of *de*-identification.[303] As discussed above, customers' privacy interests include many noncommercial values, such as avoidance of embarrassment, concern for one's reputation, and control over the context of disclosure of one's information.[304] The decisive question here is not how difficult it is to de-identify the information, but rather the ease with which the information could be re-identified.[305] The FTC's linkability standard aligns with our approach: "[W]hat qualifies as a reasonable level of [de-identification] depends upon the particular circumstances, including the available methods and technologies. In addition, the nature of the data at issue and the purposes for which it will be used are also relevant."[306]

113. Consistent with the FTC's guidance and the carrier's burden to prove that information is in fact de-identified, if carriers choose to maintain customer PI in both identifiable and de-identified formats, they must silo the data so that one dataset is not reasonably linkable to the other.[307] Cross-referencing the datasets links the de-identified information with an identified customer, thus rendering the de-identified information linked or reasonably linkable.[308] We agree with Verizon that "providers should not be allowed to use de-identification and re-identification to circumvent consumers' privacy choices."[309]

114. We disagree with commenters who argue that the linkability standard should apply only to individuals and should not extend to devices.[310] As explained above, we agree with the FTC staff that "[a]s consumer devices become more personal and associated with individual users, the distinction between a device and its user continues to blur."[311] This is not an uncommon conclusion in the Internet

[301] *See, e.g.*, AT&T Reply at 38 n.102; EFF Comments at 14 ("the field of reidentification is constantly advancing, and any [pre-set list of identifiers] would quickly become obsolete"); NTCA Comments at 57; $S^2$ERC Comments at 14 (agreeing that "the categories of what can potentially be reasonably linkable information will continue to evolve").

[302] AT&T Reply at 38.

[303] *Cf. id.* at 36 (claiming that the FTC framework adopted a commercial reasonableness standard); CTIA Comments at 43 (CPNI is de-identified if the provider uses "commercially reasonable techniques").

[304] *See supra* para. 1.

[305] *See* EPIC Comments at 21-22 ("Because not all de-identification techniques adequately anonymize data, it is important that the process employed is robust, scalable, transparent, and shown to provably prevent the identification of consumer information."); *see also supra* note 287.

[306] 2012 FTC Privacy Report at 21.

[307] *See* 2012 FTC Privacy Report at 22 n.113. *See, e.g.*, WTA & Nex-Tech Apr. 25, 2016 *Ex Parte* at 1-2 (data retention mandates are burdensome for small providers).

[308] *See* Verizon Reply at 23-24 ("[P]roviders should be allowed to use and disclose de-identified data as long as the provider—and anyone it shares the data with—honors a consumer's choices prior to using that data in a way that would target the customer.").

[309] Verizon Comments at 44; *see also id.* at 44-45.

[310] *See* AT&T Comments at 69; Audience Partners Comments at 10-11, 14-17; NCTA Comments at 67; NTCA Comments at 56.

[311] FTC Staff Comments at 10. *Accord* EFF Comments at 5; EPIC Comments at 18-19 (discussing how persistent identifiers like device information can be used to map out an individual's interactions); Software & Info. Indus. Ass'n Comments at 12 (supporting the FTC's test for linkability to a "consumer, computer, or device").

ecosystem; the Digital Advertising Alliance also recognizes the connection between individuals and devices in its definition of de-identification, stating that "[d]ata has been De-Identified when . . . the data cannot reasonably . . . be connected to or associated with a particular computer or device."[312]

115. Similarly, for the reasons discussed above,[313] we disagree with commenters who argue that IP addresses and MAC addresses should not be considered reasonably linkable to an individual or device on the theory that "[t]hey only identify Internet endpoints, each of which, in turn, may reach multiple people or devices."[314] The question in this test is whether the information in question is reasonably linkable to an individual or device. Consider, for example, a typical fixed residential customer. The BIAS provider assigns that customer an IP address, and associates that customer with that IP address in its records. It is difficult to portray that scenario as not involving PII. On the other hand, if the BIAS provider shares the IP address with a third party without other identifying information, it may well be the case that the provider has not shared information that is "reasonably linkable" to an individual or device. Again, when confronted with the question, the Commission will look at all facts available and make a pragmatic determination of whether the information in question is "reasonably linkable" to an individual or device.[315]

**(ii) Part Two – Public Commitments**

116. Second, for information to meet our definition of de-identified, carriers must publicly commit to maintain and use de-identified information in a de-identified fashion and to not attempt to re-identify the data. Such public commitments inform customers of their legal rights and the provider's practices, and "promot[e] accountability."[316] As we discussed above, this level of transparency is a cornerstone of privacy best practices generally and these rules specifically.[317] As such, we disagree with commenters who argue that such public commitments are unnecessary.[318] This part of the test is consistent with FTC guidance[319]—which has broad support in the record[320]—and the CPBR.[321] We agree

[312] Digital Advertising Alliance, Application of Self-Regulatory Principles to the Mobile Environment at 6 (July 2013), http://www.aboutads.info/DAA_Mobile_Guidance.pdf (defining "De-Identification Process").

[313] *See supra* paras. 67-71.

[314] *See* NCTA Oct. 20, 2016 *Ex Parte* at 12.

[315] NCTA expresses concern that finding that IP addresses can constitute PII will undermine judicial precedent under the Video Privacy Protection Act. NCTA Oct. 20, 2016 *Ex Parte* at 11. As noted, we are not making categorical findings, but rather are looking to the "reasonably linkable" standard in finding whether information constitutes PII. We also observe that we are confronted with interpreting Section 222 of the Communications Act and its requirements concerning the protection of "proprietary information of, and relating to,. . . customers." This is distinct from the language of the VPPA, which more specifically defines PII as "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3). Accordingly, a Commission finding that certain information is or is not PII for purposes of Section 222 of the Communications Act does not answer the question of whether or not a court should consider that information to be PII under the VPPA or any other statutory provision.

[316] 2012 FTC Privacy Report at 22.

[317] *See supra* para. 8; *infra* Part III.C.

[318] *See* NTCA Comments at 57; IMS Health Comments at 16; $S^2$ERC Comments at 13-14; Paul Vixie Comments at 21 ("Public commitments are mere theater. Commission investigations with sanctions against violators would speak far more loudly and far more credibly than the most earnest of BIAS provider 'pinkie promises' to be good.").

[319] *See* 2012 FTC Privacy Report at 21-22.

[320] *See supra* note 283.

[321] *See* 2015 Administration CPBR Discussion Draft at Sec. 4(a)(2)(A)(ii). *See also* 2014 Administration Big Data Report at 8 ("In practice, data collected and de-identified is protected in this form by companies' commitments to not re-identify the data[.]").

that "[c]ompanies that can demonstrate that they live up to their privacy commitments have powerful means of maintaining and strengthening consumer trust."[322] Further, we find that this requirement will impose a minimal burden on providers, as a carrier can satisfy this requirement with a statement in its privacy policy.[323]

**(iii) Part Three – Contractual Limits on Other Entities**

117. Third, for information to meet our definition of de-identified, we require telecommunications carriers to contractually prohibit recipients of de-identified information from attempting to re-identify it. This requirement is consistent with the FTC's de-identification guidelines and the Administration's CPBR, as well as industry best practices.[324]

118. Businesses are often in the best position to control each other's practices. For example, AT&T's Privacy FAQ explains, "When we provide individual anonymous information to businesses, we require that they only use it to compile aggregate reports, and for no other purpose. We also require businesses to agree they will not attempt to identify any person using this information . . . ."[325] The record demonstrates that such contractual prohibitions are an important part of protecting consumer privacy because re-identification science is rapidly evolving.[326] We agree with Verizon and other commenters that "anyone with whom the provider shares such de-identified data should be prohibited from trying to re-identify it."[327] It is our expectation that carriers will need to monitor their contracts to maintain the carriers' continued adherence to these requirements.[328] Consequently, we need not adopt a separate part of the test to delineate monitoring requirements.[329] Further, we observe that third parties will have every incentive to comply with their contractual obligations to avoid both civil liability and enforcement actions by the FTC or the Commission (depending on the agency with authority over the third party). If

[322] Executive Office of the President, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy at 22 (2012) (2012 White House Privacy Blueprint), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[323] *See* Audience Partners Comments at 17-18 (arguing that providers should be able to satisfy this part of the test with a statement in their privacy policies); WTA Comments at 24-25 (supporting a privacy policy statement and observing that such a requirement would align with the FTC's unfair and deceptive practices guidance).

[324] Digital Advertising Alliance, Application of Self-Regulatory Principles to the Mobile Environment at 6 (July 2013), http://www.aboutads.info/DAA_Mobile_Guidance.pdf ("An entity should take reasonable steps to protect the non-identifiable nature of data if it is distributed to non-Affiliates and obtain satisfactory written assurance that such entities will not attempt to reconstruct the data in a way such that an individual may be re-identified and will use or disclose the de-identified data only for uses as specified by the entity."). The DAA guidance also requires that these commitments from recipients of the data be passed along to any further downstream recipients as well, which we support. *Id*.

[325] AT&T, Privacy FAQ, http://about.att.com/sites/privacy_policy/terms#aggregate (last visited Oct. 5, 2016) (under the heading "Do you provide companies with individual anonymous data as part of your External Marketing & Analytics Program?").

[326] *See supra* note 287; *see also* FTC Staff Comments at 9.

[327] Verizon Reply at 23-24. *See also* Audience Partners Comments at 18-19; IMS Health Comments at 16; NTCA Comments at 57.

[328] Verizon Comments at 44 ("Providers should exercise reasonable monitoring to ensure these contracts are not violated."); *see also* Sprint Reply at 4 (carriers should take "appropriate safeguards [to] mitigate privacy risks" associated with de-identified data); AT&T Reply at 38 ("ISPs should of course take reasonable safeguards to keep de-identified data from re-identification.").

[329] *See Broadband Privacy NPRM*, 31 FCC Rcd at 2556, para. 162. *See also* NTCA Comments at 57 (fourth prong is unnecessary); *accord* Audience Partners Comments at 18-19; IMS Health Comments at 17; Cincinnati Bell Comments at 14-15.

violations occur, we expect carriers to take steps to protect the confidentiality of customer's proprietary information.[330]

119. We agree with commenters who recommend a narrow clarification to the third part of the de-identification framework in situations involving disclosure of highly abstract statistical information. These situations include, for example, mass market advertisements or annual reports that reference the total number of subscribers or the percentage of customers at certain speed thresholds.[331] AT&T explains that these scenarios can involve customer information that is so "highly abstract[ed]" that it is, "in many circumstances, simply impossible" to re-identify the data.[332] Professor Narayanan concurs, noting that when statistical data is highly abstract, there is minimal risk of re-identification.[333] We agree. Consequently, we will not require contractual commitments when the de-identified customer information is so highly abstracted that a reasonable data science expert would not consider it possible to re-identify it.

120. A number of commenters also ask for a narrow exception to this part of the de-identification test for the purposes of various types of cybersecurity or de-identification research.[334] As explained below, we find that certain uses and disclosures of customer PI for the purpose of conducting research to improve and protect[335] networks and/or services are part of the telecommunications service or "necessary to, or used in" the provision of the telecommunications service for the purposes of these rules.[336]

**(iv) Case-by-case application**

121. In adopting a technology-neutral standard to determine whether otherwise personally identifiable customer PI has been de-identified, we have eschewed an approach that finds particular techniques to be *per se* acceptable or unacceptable.[337] That said, by adopting the three-part test, we have made clear that a carrier cannot "make an end-run around privacy rules simply by removing certain identifiers from data, while leaving vast swaths of customer details largely intact."[338] As Professor Ohm

[330] *See* 2012 FTC Privacy Report at 21 (arguing that companies sharing customer information should "exercise reasonable oversight to monitor compliance with these contractual provisions and take appropriate steps to address contractual violations"); Lehr et al. Comments at 6; CDT Reply at 13-14. *See also* 47 U.S.C. § 217 ("In construing and enforcing the provisions of this chapter, the act, omission, or failure of any officer, agent, or other person acting for or employed by any common carrier or user, acting within the scope of employment, shall in every case be also deemed to be the act, omission, or failure of such carrier or user as well as that person.").

[331] AT&T Comments at 70-71.

[332] *Id.* at 70; *see also* IMS Health Comments at 16-17.

[333] Reisman and Narayanan June 17, 2016 *Ex Parte* at 48, https://www.fcc.gov/ecfs/filing/60002158273/document/60002354966

[334] *See* EFF Comments at 15-16; Messaging Malware Mobile Anti-Abuse Working Group ($M^3$AAWG) Comments at 5; Feamster July 13, 2016 *Ex Parte*.

[335] Since telecommunications carriers must be able to provide secure networks to their customers, we include security research within the scope of research allowed under this limitation. Security research also falls under the exception covered in Part III.D.2.b, *infra*, regarding uses of customer PI to protect the rights and property of a carrier, or to protect users from fraud, abuse, or unlawful use of the networks.

[336] *See infra* Part III.D.2.a.

[337] We accordingly need not resolve the longstanding debate in the broader privacy literature concerning the circumstances under which data may be said to be reasonably de-identified, including the specific debate in the record concerning the appropriate role of aggregation. *See generally, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010); Future of Privacy Forum Comments.

[338] Letter from 38 Public Interest Organizations to the Honorable Tom Wheeler, Chairman, FCC at 1 (Sept. 7, 2016) (https://www.fcc.gov/ecfs/filing/10907040663545).

has stated, the FTC guidance on which we pattern our standard is "a very aggressive and appropriately strong form of de-identification"[339] and it is one that requires strong technological protections as well as business processes in its implementation. The Commission will carefully monitor carriers' practices in this area. We emphasize that carriers relying on de-identification for use and sharing of customer proprietary information should employ well-accepted, technological best practices in order to meet the three-part test described above – and employ practices that keep pace with evolving technology and privacy science.[340]

### C. Providing Meaningful Notice of Privacy Policies

122. In this section, we adopt privacy policy notice requirements for providers of broadband Internet access services and other telecommunications services. There is broad recognition of the importance of transparency as one of the core fair information practice principles (FIPPs),[341] and it is an essential component of many privacy laws and regulations, including the Satellite and Cable Privacy Acts.[342] Customer notification is also among the least intrusive and most effective measures at our disposal for giving consumers tools to make informed privacy decisions.[343] In fact, it is only possible for customers to give informed consent to the use of their confidential information if telecommunications carriers give their customers easy access to clear and conspicuous, comprehensible, and not misleading information about what customer data the carriers collect; how they use it; who it is shared with and for what purposes; and how customers can exercise their privacy choices.[344] Therefore, we adopt rules to ensure that BIAS providers' and other telecommunications carriers' privacy notices meet these essential criteria, which provide transparency and enable the exercise of choice.

123. In adopting these transparency requirements, we build on and harmonize our existing Section 222 rules for voice providers[345] with BIAS providers' existing requirement to disclose their

[339] Letter from Paul Ohm, Professor of Law, Georgetown University Law Center, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 3 (filed July 28, 2016) (Paul Ohm July 28, 2016 *Ex Parte*).

[340] Latanya Sweeney, *Only You, Your Doctor, and Many Others May Know*, JOTS – Technology Science (Sept. 29, 2015), http://techscience.org/a/2015092903/ ("Policy should adopt best practices, which improve over time as privacy technology and the science of data privacy advances. Society can learn from cycles of published re-identifications, because the knowledge of vulnerabilities will rapidly lead to improved techno-policy protections. It is an evolutionary cycle. First, a re-identification vulnerability becomes known, which leads to improved practices and technical solutions, which in turn leads to other re-identifications, and so on, until eventually we achieve robust technical, policy, or administrative solutions.").

[341] *See Broadband Privacy NPRM*, 31 FCC Rcd at 2527, para. 82; *see also* 2012 FTC Privacy Report at 61-64; Letter from Matthew M. Polka, President & CEO, American Cable Association, et al., to the Honorable Tom Wheeler, Chairman, FCC (March 1, 2016) (on file with WCB) (Industry Framework); New America's Open Technology Institute, The FCC's Role in Protecting Online Privacy 7 (2016) (OTI White Paper); Letter from Marc Rotenberg, Executive Director, EPIC, et al., to Tom Wheeler, Chairman, FCC, at 3 (Jan. 20, 2016); Letter from Jason Kint, Digital Content Next, to Tom Wheeler, Chairman, FCC, at 3-4 (Feb. 26, 2016).

[342] *See* 47 U.S.C. §§ 551(a), 338(i)(1) (directing cable providers and satellite carriers, respectively, to "clearly and conspicuously" notify their subscribers of data collection and disclosure practices).

[343] *See 2015 Open Internet Order*, 30 FCC Rcd at 5669, para. 154 (citing Howard Beales, Richard Craswell & Steven C. Salop, *The Efficient Regulation of Consumer Information*, 24 J. L. & Econ. 491 at 513 (1981); Howard Beales, Richard Craswell & Steven C. Salop, *Information Remedies for Consumer Protection*, 71 Am. Econ. Rev. 410 at 411 (Papers & Proceedings, May 1981); Alissa Cooper, *How Regulation and Competition Influence Discrimination in Broadband Traffic Management: A Comparative Study of Net Neutrality in the United States and United Kingdom*, at Section 2.4.3 (Sept. 2013)).

[344] *See infra* note 354.

[345] 47 CFR §§ 64.2001-64.2011.

privacy policy under the 2010 and 2015 *Open Internet Orders*.[346] For today's rules, we look to the record in this proceeding, which includes submissions from providers, consumer advocates, other government agencies,[347] and others about what does and does not work with respect to privacy policies.[348] Based on that record, we adopt rules that require providers to disclose their privacy practices, but decline 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 this requirement.[349] In the interest of further minimizing the burden of transparency, particularly for small providers, we also direct the Consumer Advisory Committee to convene a multi-stakeholder process to develop a model privacy policy notice that will serve as a safe harbor for our notice requirements.

124. We recognize that some commenters have criticized privacy notice requirements as providing incomplete protections for consumers. Notices by themselves do not give consumers the power to control their information; notices are not always read or understood, and newer developments in tracking and analytics can reveal more about consumers than most people realize.[350] However, none of these criticisms eliminates the fundamental need for and benefit of privacy notices.[351] If consumers do not have access to the information they need to understand what personal data is being collected and how their data is being used and shared, they cannot make choices about those practices. The fact that poorly written or poorly distributed notices can confound consumer understanding does not make well-formed notices useless, and while one consumer may ignore a notice, another who has a compelling desire to protect her privacy will benefit substantially from it. Notice also remains an essential part of today's privacy frameworks, even as big data analysis creates new privacy challenges. As the recent

[346] *See 2010 Open Internet Order*, 25 FCC Rcd at 17939, para. 56; *2015 Open Internet Order*, 30 FCC Rcd at 5673, para. 164.

[347] We observe in particular that notice is fundamental to the FTC's privacy regime, acting as a basis for its implementation of FIPPs and forming required components of their enforcement proceedings. *See* 2012 FTC Privacy Report; Facebook, Inc., Decision and Order, F.T.C. File No. 092-3184 (2012), https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc (Facebook Consent Order); Google, Inc., Decision and Order, F.T.C. File No. 102-3136 (2011), https://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter (Google Consent Order).

[348] *See, e.g.*, Comcast Comments at 16-17, 22 ("[C]ompanies must provide consumers with understandable privacy notices . . . [and] should make an effort to educate consumers about their data privacy practices."); CTIA Comments at 103; Hughes Network Systems (Hughes) Comments at 3; Industry Framework at 5 (arguing that carriers should provide notices "describing the CPNI that it collects, how it will use the CPNI, and whether and for what purposes it may share that CPNI with third parties"); INCOMPAS Comments at 9 (supporting FIPPs of transparency, choice, and security); Consumer Action Comments at 2 ("Consumers deserve to know what information is being collected about them, how it's being used and why it will be shared with other entities."); EPIC Reply at 3 (asserting that FCC should ensure fair information practices); CDT Comments at 6-7; Mozilla Comments at 6 ("Our users and our community have told us – through surveys, comments and emails – that transparency and control matter to them. They want to know what is happening with their data; they want to control what data is shared, understand how their data is used and what they get for that exchange."); Aleecia M. McDonald (McDonald) Reply at 1 ("Even the most minimal set of FIPPs include notice, choice, access, integrity, and enforcement.").

[349] Moreover, the record reflects that many BIAS providers and other telecommunications carriers already provide thorough notice of their privacy practices. *See infra* note 360.

[350] *See* EPIC Comments at 6; CDD Comments at 17; Behavioral Economics Consulting Group Comments at 3 ("In many cases, disclosure has no effect on behavior. . . Research has shown that transparency is only effective in preventing deception when the information shared is *meaningful* and *comprehensible to the recipient*.").

[351] 2014 Administration Big Data Report at 55 ("For the vast majority of today's ordinary interactions between consumers and first parties, the notice and consent framework adequately safeguards privacy protections."); *id.* at 61 ("While notice and consent remains fundamental in many contexts, it is now necessary to examine whether a greater focus on how data is used and reused would be a more productive basis for managing privacy rights in a big data environment.").

Administration Big Data Report explains, notice and choice structures may not be sufficient to account for all privacy effects of "big data,"[352] but such frameworks are necessary to protect consumers from a range of active privacy threats.

125. Below we lay out the specific transparency requirements we adopt today. First, we require that those privacy notices inform customers about what confidential information the providers collect, how they use it, and under what circumstances they share it. We also require that providers inform their customers about customers' rights to opt in to or out of (as the case may be) the use or sharing of their confidential information. This information must be presented in a way that is clear and conspicuous, in language that is comprehensible and not misleading.[353] Second, we require that providers present their privacy notice to customers at the point of sale prior to the purchase of service, and that they make their privacy policies persistently available and easily accessible on their websites, apps, and the functional equivalents thereof. Finally, we require providers to give their customers advance notice of material changes to their privacy policies. In adopting these transparency rules, we are implementing, in part, Sections 222(a) and 222(c)(1), under which we find that supplying customers with the information they need to make informed decisions about the use and sharing of their personal information is an element of "informed" approval within the meaning of Section 222, as well as necessary to protecting the confidentiality of customer proprietary information.[354]

### 1. Required Privacy Disclosures

126. Customers must have access to information about the personal data that a BIAS provider or other telecommunications carrier collects, uses, and shares, in order to make decisions about whether to do business with that provider, and in order to exercise their own privacy decisions. Absent such notice, the broad range of data that a provider is capable of gathering by virtue of providing service could leave customers with only a vague concept of how their privacy is affected by their service provider.[355] We also agree with the FTC that disclosing this information "provides an important accountability function,"[356] as disclosure of this information "constitute[s] public commitments regarding companies' data practices."[357]

[352] 2014 Administration Big Data Report at 54 ("[F]ocusing on controlling the collection and retention of personal data, while important, may no longer be sufficient to protect personal privacy."); *see also* Technology Policy Institute (TPI) Comments, Attach., Thomas Lenard and Scott Wallsten White Paper, An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking at 24 (Lenard and Wallsten White Paper) (citing 2014 Administration Big Data report in criticizing notice and consent); SIIA Comments at 8-9 (same).

[353] We will consider information to be misleading if it includes material misrepresentations or omissions.

[354] *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8117-18, para. 73 (1998) (*1998 CPNI Order*); *see also, e.g.*, ViaSat Comments at 3 (stating that "transparency is critical for 'consumers to make informed choices' regarding the collection and use of customer information"); California Attorney Gen. (California AG) Reply at 4 ("Consumers can only exercise privacy choices when they are aware of them and understand their implications."); U.S. Dep't of Health, Educ. And Welfare, Sec'y's Advisory Comm. on Automated Data Systems., Records, Computers, and the Rights of Citizens 41 (1973) (HEW Report) ("There must be a way for an individual, to find out what information about him is in a record and how it is used."); FTC, Privacy Online: A Report to Congress (1998) ("[D]ata collectors must disclose their information practices before collecting personal information from consumers").

[355] *See, e.g.*, Privacy Rights Clearinghouse Comments at 3 ("BIAS providers' data practices are largely invisible to customers and data is becoming increasingly valuable and easy to collect, store, and share. This highlights the need for clear, conspicuous, and easy-to-understand privacy notices.").

[356] FTC Staff Comments at 12.

[357] *Id.* (explaining that privacy advocates, regulators, the press, consumers, and others will have access to information about how companies collect, use, and share data).

To enable customers to exercise informed choice, and to reduce the potential for confusion, misunderstanding, and carrier abuse,[358] we find that a carrier's privacy notices must accurately describe the carrier's privacy policies with regard to its collection, use, and sharing of its customers' data. Therefore, we adopt rules that require each telecommunications carrier's notice of privacy policies to accurately specify and describe:

- The types of customer PI that the carrier collects by virtue of its provision of service, and how the carrier uses that information;
- Under what circumstances a carrier discloses or permits access to each type of customer PI that it collects, including the categories of entities to which the carrier discloses or permits access to customer PI and the purposes for which the customer PI will be used by each category of entities; and
- How customers can exercise their privacy choices.

We address each of these requirements in turn.

127. *Types of Customer PI Collected, and How It Is Used.* In order to make informed decisions about their privacy, customers must first know *what types* of their information their provider collects through the customers' use of the service. Therefore, we require BIAS providers and other telecommunications carriers to specify the types of customer PI that they collect by virtue of provision of the telecommunications service, and how they use that information.[359] Pursuant to the voice rules and the *2010 Open Internet Order*, all BIAS providers already provide customers with information about their privacy policies.[360] As such, we find that this requirement will not impose a significant burden on providers, and in some cases will decrease existing burdens.[361]

128. Likewise, customers have a right to know *how* their information is being used and under what circumstances it is being disclosed in order to make informed privacy choices.[362] Notices that omit these explanations fail to provide the context that customers need to exercise their choices. We emphasize that the notice must be sufficiently detailed to enable a reasonable consumer to make an informed choice

129. We do not require providers to divulge the inner workings of their data use programs. Instead, we find that to the extent that the notice requires providers to divulge the existence of such programs, the benefits to the market of more complete information, as well as the benefits to customers in knowing how their information is used, outweighs any individual advantage gained by any one competitor in keeping the existence of the programs secret. We therefore disagree with commenters that

[358] *See 1998 CPNI Order*, 13 FCC Rcd at 8161, para. 135.

[359] Comcast Comments at 22 ("Each ISP should provide notice to its customers that describes the CPNI that it collects."); EPIC Comments at 9-10 (asserting that notices "must include . . . the type of data collected about consumers").

[360] *See* CTIA Comments at 98 ("ISPs already publish privacy policies, providing their customers with significant information about their data practices, including a description of the type of information they collect, how they use it, with whom (and under what circumstances) they share it, and so forth."); T-Mobile Comments at 39; Hughes Comments at 3; AT&T Comments at 48-49 ("ISP privacy policies clearly set forth what information ISPs collect and how it is used."); Verizon Comments at 6 ("Verizon informs customers about what information it collects and gives consumers choices about how their data may be used.").

[361] In particular, we eliminate a number of specific requirements for voice providers' notices regarding customers' CPNI. *See infra* Part III.C.5.

[362] *See* CDD Comments at 20; OTI Comments at 33; T-Mobile Comments at 39; CTIA Comments at 98; AT&T Comments at 48-49; Verizon Comments at 6.

argue that these descriptions of how consumers' information will be used unduly jeopardize their competitive efforts.[363]

130. *Sharing of Customer PI with Affiliates and Third Parties*. We also require that providers' privacy policies notify customers about the types of affiliates and third parties with which they share customer information, and the purposes for which the affiliates and third parties will use that information. A critical part of deciding whether to approve of the sharing of information is knowing *who* is receiving that information and for what purposes.[364] This information will allow customers to gauge their comfort with the privacy practices and incentives of those other entities, whether they are affiliates or third parties. It will also promote customer confidence in their telecommunications service by providing concrete information and reducing uncertainty as to how their information is being used by the various parties in the data-sharing and marketing ecosystems. While our existing CPNI rules are more specific in requiring that individual entities be disclosed,[365] we seek to minimize customer confusion and provider burden by adopting an approach used by the FTC by allowing disclosure of categories of entities. We also encourage carriers to make these categories of entities as useful and understandable to customers as possible. By way of example, the FTC's regulations implementing the GLBA privacy rules will find a covered institution in compliance with its rules if it lists particular categories of third party entities that it shares information with, distinguishing, for instance, between financial services providers, other companies, and other entities.[366] The FTC's rules further specify that institutions should provide examples of businesses in those categories.[367] In the context of communications customers' information, relevant categories might include providers of communications and communications-related services, customer-facing sellers of other goods and services, marketing and advertising companies, research and development, and nonprofit organizations.

131. We find that requiring providers to disclose categories of entities with which they share customer information and the purposes for which the customer PI will be used by each category of entities balances customers' rights to meaningful transparency with the reality of changing circumstances and the need to avoid overlong or over-frequent notifications.[368] We therefore reject calls to mandate disclosure of a list of the specific entities that receive customer PI.[369] While some customers may benefit from receiving such detailed information, we are persuaded by commenters who assert that requiring such granularity would be unduly burdensome on carriers and induce notice fatigue in many customers. For instance, carriers would be faced with the near-continuous need to provide new notices every time contracts with particular vendors change or if third parties alter their corporate structure—and customers,

[363] *See* CTIA Comments at 105-06.

[364] *See* EFF Comments at 12-13; EPIC Comments at 9-10; OTI Comments at 33; CTIA Comments at 98.

[365] 47 CFR § 64.2008(c)(2) (requiring telecommunications carriers to describe the "specific entities" to which CPNI will be disclosed).

[366] 16 CFR § 313.6(c)(3).

[367] *Id.* (listing "illustrative examples" of financial service providers as "mortgage bankers, securities broker-dealers, and insurance agents" and "non-financial companies" as "retailers, magazine publishers, airlines, and direct marketer.").

[368] *See, e.g.*, FTC Staff Comments at 11-12 (supporting disclosure of categories of entities); CTIA Comments at 103 ("ISPs should be able to report general categories of data-sharing partners, rather than listing each and every affiliate, vendor, or contractor with whom the ISP works."). Because we harmonize these rules across BIAS and other telecommunications services, we eliminate the requirement that telecommunications services specify the "specific entities" that receive customer information in their notices of privacy policies accompanying solicitations for customer approval. 47 CFR § 64.2008(c)(2) ("the notification must specify the. . . specific entities that will receive the CPNI. . .").

[369] *See, e.g.*, OTI Comments at 33; EFF Comments at 12-13; EPIC Comments at 9-10.

in turn, would be inconvenienced with an overabundance of notices.[370] Furthermore, a list of specific entities may not in itself aid the average consumer in making a privacy decision more than the requirement that we adopt, which ensures that consumers understand what third parties that receive their information do as a general matter. We therefore adopt the requirement that carriers need only provide categories of entities with whom customer PI is shared, minimizing the burden on telecommunications carriers. If a provider finds that providing notice of the specific entities with which it shares customer PI would increase customer confidence, nothing prevents a provider from doing so, and we would encourage notices to include as much useful information to customers as possible, while maintaining their clarity, concision, and comprehensibility, as discussed in Part III.C.3, below.[371] Doing so does not require bombarding customers with pages of dense legal language; providers may make use of layered privacy notices or other techniques to ease comprehension and readability as necessary.[372]

132. *Customers' Rights with Respect to Their PI.* We also adopt our *NPRM* proposal to require BIAS provider and other telecommunications carrier privacy notices to provide certain minimum information. Carriers need not, however, repeat any of these "rights" statements verbatim, and we encourage carriers to adapt these statements in manners that will be most effective based on their extensive experience with their customer base. Specifically, carriers' privacy notices must:

- Specify and describe customers' opt-in and opt-out rights with respect to their own PI. This includes explaining that:
  - a denial of approval to use, disclose, or permit access to customer PI for purposes other than providing telecommunications service will not affect the provision of the telecommunications services of which they are a customer.
  - any approval, denial, or withdrawal of approval for use of the customer PI for any purposes other than providing telecommunications service is valid until the customer affirmatively revokes such approval or denial, and that the customer has the right to deny or withdraw access to such PI at any time. However, the notice should also explain that the carrier may be compelled, or permitted, to disclose a customer's PI when such disclosure is provided for by other laws.
- Provide access to a simple, easy-to-use mechanism for customers to provide or withdraw their consent to use, disclose, or permit access to customer PI as required by these rules.[373]

133. These notice requirements are intended to ensure that providers inform their customers that they have the right to opt into or out of the use and sharing of their information, as well as how to make those choices known to the provider. We discuss the choice mechanism itself in Part III.D.4, *infra*. Requiring providers to describe in a single place how information is collected, used, and shared, as well as what the consumers' rights are to control that collection, use, and sharing, enhances the opportunity for

[370] *See* CTIA Comments at 105 ("ISPs may enter into agreements with third-party agents, independent contractors, and other entities for a variety of different purposes, ranging from one-off transactions to repeat interactions."); NTCA Comments at 39-40 ("[T]his would create an administrative nightmare and hamstring a provider's ability to create arrangements in 'real market time' with third parties. . . Moreover, this requirement could be triggered if a third party undergoes an internal corporate restructuring, and then foists upon the provider a liability whose cause of action rests solely within the domain of the restructured third-party.").

[371] *See* EFF Comments at 12-13 (disclosure of specific entities can encourage customers to opt in to sharing when they trust particular third parties); *see also* CDD Comments at 17 (stating that providers "should be able to be both candid and succinct" and should be able to "test layout and design factors to ensure their privacy policies are actually in view (as the industry is able to do with 'viewability' of digital ads").

[372] *See* CDD Comments at 19; T-Mobile Comments at 39 (describing existing layered approach to privacy notices); WISPA Comments at 16 (asserting that "a layered privacy policy notice . . . should be considered" as a voluntary safe harbor).

[373] This mechanism is described below in Part III.D.4.

customers to make informed decisions.[374] Likewise, requiring the notice to provide access to the choice mechanism ensures that the mechanism is easily available and accessible as soon as the customer receives the necessary privacy information. This is important, since studies have shown that "adding just a 15-second delay between the notice and the loading of [a] webpage where subjects choose whether to reveal their information eliminates the privacy-protective effect of the notice."[375] As discussed further below,[376] we decline to specify particular formats for carriers to provide access to their choice mechanisms, recognizing that different forms of access to the choice mechanism (e.g., a link to a website, a mobile dashboard, or a toll-free number) may be more appropriate depending on the context in which the notice may be given (e.g., on a provider's website, in a provider's app, or in a paper disclosure presented in a provider's store).[377]

134. Studies have shown that customers are often resigned to an inability to control their information, and may be under a mistaken impression that exercising their rights may result in degraded service.[378] Thus, we require providers' notice of privacy policies to also inform customers that denying a provider the ability to use or share customer PI will not affect their ability to receive service.[379] This parallels the existing Section 222 rules, which require carriers to "clearly state that a denial of approval will not affect the provision of any services to which the customer subscribes."[380] Since providers drafting their notices have clear incentives to encourage customers to permit the use and sharing of customer PI, it can be easy for customers to misconstrue exactly what is conditioned upon their permission.[381] These provisions are intended to make customers aware that the offer of choice is not merely *pro forma*.

135. We permit providers to make clear and neutral statements about potential consequences when customers decline to allow the use or sharing of their personal information. We require that any such statements be clear and neutral in order to prevent them from obscuring the basic fact of the customer's right to prevent the use of her information without loss of service. Allowing difficult-to-read or biased statements would run counter to our goal of ensuring that notices overall are clear and conspicuous, comprehensible, and not misleading.[382] NTCA recommends that we remove or modify from the *NPRM*'s proposal the requirement that the explanation be brief.[383] In the interest of allowing more

[374] *See, e.g.*, OTI Comments at 33-34, 36; Online Trust Alliance Comments at 2.

[375] *See* Lauren Willis (Willis) Reply at 7 (citing Idris Adjerid, et al., *Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency*, Symposium on Usable Privacy & Security (2013)).

[376] *See infra* Part III.D.4.

[377] *See, e.g.*, NTCA Comments at 36-38; CTIA Comments at 104-05.

[378] *See, e.g.*, Lee Rainie and Maeve Duggan, *Privacy and Information Sharing*, Pew Research Center, December 2015, http://www.pewinternet.org/files/2016/01/PI_2016.01.14_Privacy-and-Info-Sharing_FINAL.pdf; Joseph Turow, et al., *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation*, Univ. of Penn. Annenberg School of Comm'n (June 2015), available at https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf; Joseph Turow, et al., *Americans Reject Tailored Advertising and Three Activities that Enable it* (September 29, 2009); available at SSRN: http://ssrn.com/abstract=1478214; *see also* CDD Comments at 5 (citing consumer belief that they lack control over their data); Free Press Reply at 25-26; CDD Reply at 2.

[379] *See infra* Part III.G.1. As noted below, this provision does not mean that carriers categorically cannot engage in financial incentive practices. *See infra* Part III.G.2.

[380] 47 CFR § 64.2008(c)(3).

[381] *See, e.g.*, California AG Reply at 3 (asserting "the choices offered to individuals [are often] illusory, frequently amounting to 'take it or leave it' or 'all or nothing'").

[382] *See infra* Part III.C.3.

[383] NTCA Comments at 37-38 (footnote omitted).

flexibility, we remove this requirement, with the understanding that brevity is often, but not always, a component of clarity.

136. We require providers to inform customers that their privacy choices will remain in effect until the customers change them, and that customers have the right to change them at any time. We acknowledge that "[c]ustomers may make hasty decisions in the moment simply to obtain Internet access . . . [and] therefore appreciate the reminder that they have the opportunity to change their mind."[384] We expect carriers' privacy promises to customers and the privacy choices customers make to be honored, including, for example, in connection with a carrier's bankruptcy.[385]

### 2. Timing and Placement of Notices

137. There is broad agreement that, in order to be useful, privacy policy notices must be clearly, conspicuously, and persistently available, and not overly burdensome to the carrier or fatiguing to the customer.[386] We therefore require telecommunications carriers to provide notices of privacy policies at the point of sale prior to the purchase of service, and also to make them clearly, conspicuously, and persistently available on carriers' websites and via carriers' apps that are used to manage service, if any. We also eliminate periodic notice requirements from the voice CPNI rules.

138. *Point of Sale.* We agree with commenters that requiring notices at the point of sale ensures that notices are relevant in the context in which they are given,[387] since this is a time when a customer can still decide whether or not to acquire or commit to paying for service, and it also allows customers to exercise their privacy choices when the carrier begins to collect information from them. In this, we agree with the FTC, which finds that the most relevant time is when consumers sign up for service.[388] The proximity in time between sale and use of information means that a point-of-sale notice, in many if not most instances, serves the same function as a just-in-time notice—that of providing information at the most relevant point in time. Consumer groups such as the Center for Digital Democracy and providers such as Sprint also appear to agree on this point.[389] The point-of-sale requirement is also consistent with the transparency requirements of the *2010 Open Internet Order*, which

[384] OTI Comments at 40.

[385] As the FTC has done in its groundbreaking work in this area, the FCC will be vocal in support of customer privacy interests that a carrier's bankruptcy may raise. *See, e.g.*, Letter from Jessica L. Rich, Director, FTC's Bureau of Consumer Protection to Elise Frejka, Esq. (May 16, 2015), *available at* https://www.ftc.gov/public-statements/2015/05/letter-jessica-rich-director-bureau-consumer-protection-bankruptcy-court (letter to bankruptcy court-appointed Consumer Privacy Ombudsperson expressing concern about possible sale of certain PII and suggesting conditions to protect customer privacy); *FTC v. Toysmart*, No. 00-11341-RGS (D. Mass. 2000), *available at* https://www.ftc.gov/enforcement/cases-proceedings/x000075/toysmartcom-llc-toysmartcom-inc (consent order relating to sale in bankruptcy of children's information, including shopping preferences).

[386] *See* Comcast Comments at 44 (noting potential fatigue with repeated notices); CTIA Comments at 101-102 (recommending against periodic notices); NCTA Reply at 53 (arguing the most relevant time for notice is at point of sale).

[387] *See, e.g.*, FTC Staff Comments at 24-25 (stating that customers should receive choice solicitations at "most relevant time," which is when they "sign up for service"); CDD Comments at 20 ("[P]rivacy decisions should be at or near the point of sale."); Sprint Comments at 12 (stating that notices may be most effective at the outset of the provider-customer relationship); Comcast Reply at 12 (citing FTC Staff Comments at 24); *cf., e.g.*, Privacy Rights Clearinghouse Comments at 4 (citing Consumer Fin. Prot. Bureau, *CFPB Finalizes Rule to Promote More Effective Privacy Disclosures*, October 20, 2014, http://www.consumerfinance.gov/about-us/newsroom/cfpb-finalizes-rule-to-promote-more-effective-privacy-disclosures/) (stating that frequency of notice presentation irrelevant as long as other standards are met); USTelecom Comments at 12 (citations omitted) (approving of a single initial notice).

[388] FTC Staff Comments at 24-25.

[389] CDD Comments at 20; Sprint Comments at 12.

requires disclosure of privacy policies at the point of sale.[390] As such, we find that this requirement will impose a minimal incremental burden on BIAS providers. The record further indicates that providing notice at the point of sale can be less burdensome for a carrier, in part because it allows the provider to walk a customer through the terms of the agreement.[391] Providing notice at the point of sale, and not after a customer has committed to a subscription, can also allow carriers to compete on privacy.[392]

139. We clarify that a "point of sale" need not be a physical location. Where the point of sale is over voice communications, we require providers to give customers a means to access the notice, either by directing them to an easily-findable website, or, if the customer lacks Internet access, providing the text of the notice of privacy policies in print or some other way agreed upon by the customer. We find that this requirement adequately addresses record concerns about the burdens associated with communicating polices orally to customers.[393]

140. *Clear, Conspicuous, and Persistent Notice.* We also require telecommunications carriers to make their notices persistently available through a clear and conspicuous link on the carrier's homepage, through the provider's application (if it provides one for account management purposes), and any functional equivalents of the homepage or application.[394] This requirement also reflects the transparency requirements in the *2010 Open Internet Order*, which mandate "at a minimum, the prominent display of disclosures on a publicly available . . . website,"[395] and as such, should add a minimal burden for BIAS providers. Persistent and visible availability is critical; customers must be able to review the notice and understand the carrier's privacy practices at any time since they may wish to reevaluate their privacy choices as their use of services change, as their personal circumstances change, or as they evaluate and learn about the programs offered by the provider.[396] Persistent access to the notice of privacy policies also ensures that customers need not rely upon their memory of the notice that they viewed at the point of sale; so long as they have access to the provider's website, app, or equivalent, they can review the notice. As such, we require providers to at least provide a link to the web-hosted notice in

[390] *See 2010 Open Internet Order*, 25 FCC Rcd at 17939-40, paras. 56-57; *see also FCC Enforcement Bureau and Office of General Counsel Advisory Guidance for Compliance with Open Internet Transparency Rule*, Public Notice, 26 FCC Rcd 9411, 9413-14 (2011) (*2011 Open Internet Transparency Guidance*).

[391] CTIA Comments at 143; *see also* NTCA Comments at 52-53.

[392] *See* Cincinnati Bell Comments at 12-13; Lenard and Wallsten White Paper at 18; FTC Staff Comments at 13 (citing 2012 FTC Privacy Report at 61); *see also* INCOMPAS Comments at 6; NTCA Comments at 7 (citation omitted).

[393] ITTA Comments at 21 (noting potential difficulty in providing notice if point of sale is over the telephone); ViaSat Comments at 3-4 (asserting that "the Commission should permit BIAS providers at the point of sale to direct consumers to such online disclosures orally or in writing—rather than, for example, requiring BIAS providers to have employees read privacy notices aloud to potential customers when signing them up for service over the phone").

[394] *See, e.g.*, Hughes Comments at 3 ("Hughes provides all consumers with 24 hour access to our plain language privacy policy on our website . . . Accordingly, Hughes, an early adopter of consumer privacy protections, fully supports the FCC requiring all broadband providers to provide clear, transparent privacy disclosures on their website to prospective customers and current subscribers."); OTI Comments at 40 (supporting proposal); NTCA Comments at 36-38 (supports homepages links as persistent access to notice); ViaSat Comments at 3 ("[P]rivacy disclosures should be readily available to customers through the provider's website.").

[395] *2010 Open Internet Order*, 25 FCC Rcd at 17939-40, para. 57.

[396] OTI Comments at 40 ("[C]onsumers generally cannot adequately account for privacy harms that result from information disclosure far in the future . . . circumstances may have changed, particularly if customers can access the information BIAS providers have collected about them . . . . Customers may make hasty decisions in the moment simply to obtain Internet access [and] therefore appreciate the reminder that they have the opportunity to change their mind."); Hughes Comments at 5 (stating that persistent notice and choice mechanisms allow customers to re-evaluate their choices); Mozilla Comments at 7 (stating that customers should be able to easily change their minds).

a clear and conspicuous location on its homepage, to ensure that customers who visit the homepage may easily find it.[397]

141. We require the notice of privacy policies to be clearly and conspicuously present not only on the provider's website, but to be accessible via any application ("app") supplied to customers by the provider that serves as a means of managing their subscription to the telecommunications service. As more consumers rely upon mobile devices to access online information, a provider's website may become less of a central resource for information about the provider's policies and practices. Certain mobile apps serve much the same function as a mobile website interface, giving customers tools to manage their accounts with their providers.[398] As a significant point of contact with the customer, such apps are an ideal place for customers to be able to find the notice of privacy policies.[399] We do not, however, expect that every app supplied by a provider must carry the notice of privacy policies for the entire service—for instance, a mobile broadband provider that bundles a sports news app or a mobile game with its phones and services would not need to provide the privacy notice we require here with those apps.[400] Nor do we require providers who lack an app to develop one.[401] However, we require carriers that provide apps that manage a customer's billing or data usage, or otherwise serve as a functional equivalent to a provider's website, to ensure that those apps provide at least a link to a viewable notice of privacy policies.[402]

142. Providing the notice both via the app and on the provider's website increases customers' ability to access and find the policy regardless of their primary point of contact with the provider. We do, however, wish to ensure that customers can still reach notices even as providers may develop other channels of contact with their customers, and thus require that the notice be made available on any functional equivalents of the website or app that may be developed. While we anticipate that all BIAS providers and most other telecommunications providers have a website, those that do not may provide their notices to customers in paper form or some other format agreed upon by the customer.

143. *No Periodic Notice Requirement.* We decline to require periodic notice on an annual or bi-annual basis. While periodic notices might serve to remind customers of their ability to exercise privacy choices,[403] we remain mindful of the potential for notice fatigue and find that notices at the point of sale, supplemented by persistently available notices on providers' websites, and notices of material change to privacy policies,[404] is sufficient to keep customers informed.[405] Additionally, we believe that periodic notices might distract from notices of material changes, reducing the amount of customer

[397] NTCA Comments at 35-38; ViaSat Comments at 3-4 ("[T]he Commission should permit BIAS providers at the point of sale to direct consumers to such online disclosures orally or in writing—rather than, for example, requiring BIAS providers to have employees read privacy notices aloud to potential customers when signing them up for service over the phone.").

[398] *See* NTCA Comments at 36 (noting the existence of mobile apps that track data usage and consumption, or enable bill payment).

[399] *See* NTCA Comments at 35-36; Privacy Rights Clearinghouse Comments at 4. The notice may be provided either within the application itself or through a link in the application to a different location hosting the notice.

[400] *See, e.g.*, NTCA Comments at 35-36; $S^2$ERC Comments at 11.

[401] *See* $S^2$ERC Comments at 11.

[402] *See* NTCA Comments at 35-36 (approving of links to privacy policies on apps that serve as mobile web interfaces).

[403] *See* CDD Comments at 19 (suggesting marketing techniques can prevent customers from being overwhelmed by regular notices); OTI Comments at 34-35 (recommending annual reminders of choice options).

[404] *See infra* Part III.C.4.

[405] *See* Privacy Rights Clearinghouse Comments at 4; WTA Comments at 15; XO Comments at 15; Rural Wireless Association Comments at 7.

attention to such changes.[406] We find that annual or periodic notices are unnecessary or even counterproductive in this context, and we reduce burdens on all telecommunications carriers—including smaller carriers—by eliminating the pre-existing every-two-year notice requirement from our Section 222 rules.[407]

### 3. Form and Format of Privacy Notices

144. Recognizing the importance of flexibility in finding successful ways to communicate privacy policies to consumers, we decline to adopt any specific form or format for privacy notices. We agree with commenters that, in addition to running the risk of providing insufficient flexibility, mandated standardized requirements may unnecessarily increase burdens on providers, and prevent consumers from benefitting from notices tailored to a specific provider's practices. For example, the record reflects concerns that mandated standardized requirements can increase burdens on providers, and can also create a number of problems, including a lack of flexibility to account for the fact that different carriers may have different needs, such as creating comprehensive policies across different services.[408] This concern is especially prevalent for smaller carriers.[409] At the same time, we agree with commenters that whatever form of privacy notices a provider adopts, in order to adequately inform customers of their privacy rights, such privacy notices must clearly and conspicuously provide information in language that is comprehensible and not misleading, and be provided in the language used by the carrier to transact business with its customer.[410] We therefore require providers to implement these general principles in formatting their privacy policy notices.

145. These basic requirements for the form and format of privacy policies build on existing Commission precedent regarding notice requirements for voice providers and open Internet transparency requirements for BIAS providers, and incorporate FTC guidance on customer notice standards.[411] These basic principles are well suited to accommodating providers' and customers' changing needs as new business models develop or as providers develop and refine new ways to convey complex information to customers.[412] Within these basic guidelines, providers may use any format that conveys the required information, including layering and adopting alternative methods of structuring the notice or highlighting its provisions.[413] We encourage innovative approaches to educating customers about privacy practices and choices.

146. While we decline to mandate a standardized notice at this time, the record demonstrates that voluntary standardization can benefit both customers and providers.[414] As such, as described below,

---

[406] *See supra* note 403.

[407] *See* NTCA Comments at 41; WTA Reply at 7; *see also infra* Part III.C.5.

[408] *See, e.g.*, CTIA Comments at 102-03; Mobile Future Comments at 4 (citing 2012 FTC Privacy Report at 27); NCTA Comments at 85; WTA Comments at 14; ACA Reply at 14-15.

[409] *See, e.g.*, Rural Wireless Association Comments at 6-7 (expressing concern "about the financial burdens that the proposed privacy notice framework will impose on small providers"); NTCA Comments at 41-42; WTA Comments at 10.

[410] *See* FTC Staff Comments at 14 (citing 16 CFR § 437.3(a) ("business opportunity rule"); 16 CFR § 14.9 ("requirements concerning clear and conspicuous disclosures in foreign language advertising and sales materials")).

[411] *See* 47 CFR §§ 64.2001-2011; *2010 Open Internet Order*, 25 FCC Rcd at 17939, para. 56; *2015 Open Internet Order*, 30 FCC Rcd at 5673, para. 164; FTC Staff Comments at 11-15; 2012 FTC Privacy Report at 60-64.

[412] *See, e.g.*, T-Mobile Comments at 41-42; Future of Privacy Forum Reply at 6.

[413] T-Mobile Comments at 39 (noting T-Mobile's existing layered privacy notices); WISPA Comments at 16 (suggesting voluntary layered notices). We note that as standard business practices for conveying complex information improve, we expect notices of providers' privacy policies to keep pace.

[414] *See infra* note 427.

we adopt a voluntary safe harbor for a disclosure format that carriers may use in meeting the rules' standards for being clear and conspicuous, comprehensible, and not misleading.

147. *Clear, Conspicuous, Comprehensible and Not Misleading.* Consistent with existing best practices, we require providers' privacy notices to be readily available and written and formatted in ways that ensure the material information in them is comprehensible and easily understood. The record reflects broad agreement that providers' privacy practices "should be easily available [and] written in a clear way."[415] A number of commenters noted that certain practices frustrate the ability of customers to find and identify the important parts of privacy notices, observing, for example, that notices could be presented among or alongside distracting material, use unclear or obscure language, presented with significant delays in ability for consumers to act, or be placed only at the bottom of "endless scrolling" pages.[416] By mandating that notices be clear, conspicuous, comprehensible, and not misleading, we prohibit such practices and others that render notices unclear, illegible, inaccessible, or needlessly obtuse.[417]

148. The *NPRM* framed these requirements in several ways, including that notices be "clear and conspicuous," as well as "clearly legible, use sufficiently large type, and be displayed in an area so as to be readily apparent to the consumer."[418] In adopting these rules, we streamline these requirements by interpreting "conspicuous" to include requirements for prominent display, and eliminate the requirement for "sufficiently large type," based upon the understanding that insufficiently large type would not be "comprehensible" or "clear and conspicuous." Removing this specific requirement also preserves the ability for providers who may be able to convey the necessary information through images or other non-textual means.[419]

149. We agree with the FTC's observation that existing notices of privacy policies are frequently too long and unclear;[420] overlong notices are often inherently less comprehensible.[421] As T-Mobile states, "today's busy consumers often have limited ability to fully review the hundreds of privacy

[415] Consumer Action Comments at 2 ("The provider's privacy practices should be easily available, written in a clear way and linked to a user-friendly opt-out and preference page."); Comcast Comments at 42-43 ("Two of the key tenets of the FTC's regime and Administration's Consumer Privacy Bill of Rights are transparency and choice, including making privacy practices as simple and clear as possible so that consumers can make informed decisions."); FTC Staff Comments at 11 ("FTC staff supports the proposed requirement to clearly and conspicuously disclose privacy policies."); Privacy Rights Clearinghouse Comments at 3 ("BIAS providers' data practices are largely invisible to customers. . . . This highlights the need for clear, conspicuous, and easy-to-understand privacy notices."); EPIC Comments at 9-10 ("Internet-based services must provide individuals in concise and easily understandable language, accurate, clear, timely, and conspicuous information about the covered entity's privacy and security practices."); CCA Reply at 34 (asserting that policies should be easily findable by customers).

[416] Free Press Comments at 15 (criticizing notices presented among distractions); Greenlining Comments at 34-40 (noting examples of confusing or obscure language); Willis Reply at 7-8 (noting that firms can "sabotage" disclosures through, *inter alia*, distractions, delays between notice and ability to act, and placing disclosures at the end of lengthy processes to exhaust consumers); Willis Reply at 11-12 (detailing techniques that discourage customer action on privacy notices); OTI Comments at 34 (criticizing "endless scrolling" pages obscuring privacy notices).

[417] *See* Greenlining Institute Comments at 33 ("It is unlikely that a customer reads and digests any of this information."); CDD Comments at 4 n.6 (arguing that "oblique and disingenuous" policies provider little consumer notice but shield providers from liability); OTI Comments at 34 (calling for enforcement against inadequately readable notices).

[418] *Broadband Privacy NPRM*, 31 FCC Rcd at 2527-29, paras. 82, 83.

[419] *See* Willis Reply at 5.

[420] FTC Staff Comments at 12.

[421] FTC Staff Comments at 12-13; New York Attorney General Reply at 2.

policies that apply to the apps, websites, and services they use, and prefer simpler notices that provide meaningful information."[422] We recognize that providers must balance conveying the required information in a comprehensive and comprehensible manner,[423] and therefore encourage, but do not require, providers to make their notices as concise as possible while conveying the necessary information. Layered notices, lauded by a few commenters, may be one of several ways to achieve these parallel objectives.[424]

150. The record also reflects that transparency is only effective in preventing deception when the information shared is meaningful to the recipient.[425] We agree with the California Attorney General that companies should "alert consumers to potentially unexpected data practices," and as such require that providers' notices not be misleading in addition to being comprehensible.[426] This requirement is also consistent with FTC precedent.[427]

151. *Other Languages.* We agree with the FTC that providers should convey notices to their customers in a language that the customers can understand.[428] We therefore require providers to convey their entire notices of privacy policies to customers in another language, if the telecommunications carrier transacts business with the customer in that other language.[429] This requirement ensures that customers who are advertised to in a particular language may also understand their privacy rights in that same language.[430] We conclude that this obligation appropriately balances accommodating customers who primarily use languages other than English and reducing the burden on providers, especially small providers, to translate notices into languages that are unused by their particular customers.[431]

152. *Mobile-Specific Considerations*. We decline to mandate any additional requirements for notices displayed on mobile devices. The record indicates that providers desire flexibility to adapt notices to be usable in the mobile environment for their customers, while consumer advocates stress that the requirements for usability must be met in some way, regardless of the specific formatting.[432] So long as

[422] T-Mobile Comments at 39.

[423] ADTRAN Comments at 10-11.

[424] *See, e.g.*, T-Mobile Comments at 39; WISPA Comments at 16; Ghostery Apr. 29, 2016 *Ex Parte* at 18.

[425] Behavioral Economics Consulting Group Comments at 3; *see also* McDonald Reply at 3 (noting misleading characterizations of targeted advertising).

[426] California Attorney General Reply at 4-5; *see also* 2014 Administration Big Data Report at 56 (advocating a "no surprises" rule based upon respecting the context of a consumer's expectations of contextual use); INCOMPAS Comments at 12 (noting heightened privacy implications for provisions that would surprise customers); T-Mobile Comments at 29 (same); Mozilla Comments at 6 (advocating "no surprises" as a data principle).

[427] *See, e.g.*, Snapchat Consent Decree at 3 (prohibiting Snapchat from misrepresenting the extent which Snapchat or its products or services maintain and protect the privacy, security, or confidentiality of any covered information, including but not limited to: "(1) the extent to which a message is deleted after being viewed by the recipient; (2) the extent to which respondent or its products or services are capable of detecting or notifying the sender when a recipient has captured a screenshot of, or otherwise saved, a message; (3) the categories of covered information collected; or (4) the steps taken to protect against misuse or unauthorized disclosure of covered information").

[428] FTC Staff Comments at 14; Asian American and Pacific Islander Technology & Telecommunications Table (AAPI) Comments at 1.

[429] *Cf.* Requirements concerning clear and conspicuous disclosures in foreign language advertising and sales materials, 16 CFR § 14.9; Business Opportunity Rules, 16 CFR § 437.3(a).

[430] FTC Staff Comments at 14. We note that for the purposes of this rule, "language" also includes American Sign Language, meaning that if the customer transacts business with the carrier in American Sign Language, the notice would need to be made available in that language.

[431] AAPI Comments at 1.

[432] *See* CTIA Comments at 103-04; EFF Comments at 14; Lehr et al. Comments at 4.

notices on mobile devices meet the above guidelines and convey the necessary information, they will comply with the rules. Providers are free to experiment within those broad guidelines and the capabilities of mobile display technology to find the best solution for their customers.

153. *Safe Harbor for Standardized Privacy Notices.* To encourage adoption of standardized privacy notices without mandating a particular form, we direct the Consumer Advisory Committee, which is composed of both industry and consumer interests,[433] to formulate a proposed standardized notice format, based on input from a broad range of stakeholders, within six months of the time that its new membership is reconstituted, but, in any event, no later than June 1, 2017. There is strong support in the record for creation of standardized notice, and for use of multi-stakeholder processes.[434] Standardized notices can assist consumers in interpreting privacy policies, and allow them to better compare the privacy policies of different providers, allowing increased competition in privacy protections.[435] Standardized notices can also reduce compliance costs for providers, especially small providers, by ensuring they can easily adopt a compliant form and format for their notices.[436]

154. The CAC has significant expertise in developing standard broadband disclosures and other consumer disclosure issues.[437] We find that the Committee's experience makes it an ideal body to recommend a notice format that will be sufficiently clear and easy to read to allow consumers to easily understand and compare the privacy practices of different providers. To ensure that the notice will be clear and easy to read for all customers, it must also be accessible to persons with disabilities. We delegate authority to the Wireline Competition Bureau, Wireless Telecommunications Bureau, and Consumer & Governmental Affairs Bureau to work with the CAC on the draft standardized notice. If the CAC recommends a form or format that do not meet the Bureaus expectations, the Bureaus may ask the CAC to consider changes and submit a revised proposal for the Bureaus' review within 90 days of the Bureaus' request. The Bureaus may also seek public comment, as they deem appropriate, on any standardized notice the CAC recommends. We also delegate authority to the Bureaus to issue a Public Notice announcing any proposed format or formats that they conclude meet our expectations for the safe harbor for making consumer-facing disclosures.[438]

---

[433] FTC Staff Comments at 13-14; Hughes Comments at 3-4 (noting the CAC has a precedent for developing standard notices); WISPA Comments at 16 (approving of CAC process as a model for standardized notices); WISPA Reply at 31 (specifically recommending the CAC develop standardized privacy notices). The Committee's purpose is to make recommendations to the Commission regarding consumer issues within the Commission's jurisdiction and to facilitate the participation of consumers in proceedings before the Commission.

[434] ACA Reply at 14-15; NTCA Comments at 41-42 (supporting standardized safe harbor notice, but no mandated standard); Privacy Rights Clearinghouse Comments at 3 (recommending standardized notice); Rural Wireless Association Comments at 7; ViaSat Comments at 4; WISPA Comments at 16 (recommending standardized safe harbor if notice is required); WISPA Reply at 31; Letter from Jodi Goldberg, Associate Corporate Counsel, Hughes Network Systems, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, Attach. at 1 (filed Oct. 14, 2016) (Hughes Oct. 14, 2016 *Ex Parte*) (supporting standardized notices as a safe harbor). We note that the record is largely lacking on specific models for or details about how to format such notices.

[435] FTC Staff Comments at 13; Greenlining Institute Comments at 41-42; EFF Comments at 13-14; ViaSat Comments at 2 ("[P]rivacy practices often can be a point of competitive differentiation between service providers.").

[436] *See, e.g.*, ACA Comments at 49-51; CTIA Comments at 104; EFF Comments at 13-14.

[437] The Committee previously developed the Open Internet broadband consumer labels, as well as developed guidelines on consumer disclosures via its Consumer Information Disclosure Task Force. *Consumer and Governmental Affairs, Wireline Competition, and Wireless Telecommunication Bureaus Approve Open Internet Broadband Consumer Labels*, GN Docket No. 14-28, Public Notice, 31 FCC Rcd 3358; FCC Consumer Advisory Committee, Recommendations Regarding Pre-Sale Consumer Disclosures (Aug. 4, 2010), at https://apps.fcc.gov/edocs_public/attachmatch/DOC-300826A1.pdf.

[438] 47 CFR §§ 0.291, 0.331, 0.361.

155. Providers that voluntarily adopt a privacy notice format developed by the CAC and approved by the Bureaus will be deemed to be in compliance with the rules' requirements that notices be clear, conspicuous, comprehensible, and not misleading. As with the *Open Internet* BIAS transparency rules, use of the safe harbor notice is a safe harbor with respect to the format of the required disclosure to consumers. A provider meeting the safe harbor could still be found to be in violation of the rules, for example, if the content of that notice is misleading, otherwise inaccurate, or fails to include all mandated information.

#### 4. Advance Notice of Material Changes to Privacy Policies

156. We require telecommunications carriers to provide advance notice of material changes to their privacy policies to their existing customers, via email or other means of active communication agreed upon by the customer.[439] As with a provider's privacy policy notice, any advance notice of material changes to a privacy policy must be clear, conspicuous, comprehensible, and not misleading. The notice also must be completely translated into a language other than English if the telecommunications carrier transacts business with the customer in that language. This notice must inform customers of both (1) the changes being made; and (2) customers' rights with respect to the material change as it relates to their customer PI.[440] In doing so, we follow our own precedent and that of the FTC in recognizing the need for consumers to have up-to-date and relevant information upon which to base their choices.[441] This requirement to notify customers of material change finds strong support in the record.[442]

157. The record reflects strong justifications for requiring providers to give customers advance notice of material changes to their privacy policies.[443] In order to ensure that customer approval to use or share customer PI is "informed" consent, customers must have accurate and up-to-date information of what they are agreeing to in privacy policies.[444] The notice of material change requirement that we adopt is consistent with the transparency requirements of the *2015 Open Internet Order*, which require providers to disclose material changes in, among other things, "commercial terms,"[445] which includes privacy policies.[446] Notices of material change are essential to respecting customers' informed privacy choices; if a provider substantially changes its privacy practices after a customer has agreed to a different set of practices, the customer cannot be said to have given informed consent, consistent with Section 222. This is particularly important when providers are seeking a customer's opt-out consent, since the customer's privacy rights could change whether or not they had actual knowledge of the change in policy. We therefore disagree that such a requirement is outweighed by the risk of notice fatigue;[447] to the extent

[439] *See Broadband Privacy NPRM*, 31 FCC Rcd at 2533-34, para. 96. As with our requirements for the notice of privacy policy, if a carrier does not have a website, it may provide notices of material change notices to customers in paper form or some other format agreed upon by the customer.

[440] *See id.*

[441] *See 2015 Open Internet Order*, 30 FCC Rcd at 5671-73, paras. 161-164; Facebook Consent Order; Google Consent Order.

[442] *See, e.g.*, FTC Staff Comments at 14-15; EFF Comments at 13; Comcast Comments at 49; CTIA Comments at 122-23; T-Mobile Comments at 41; WISPA Comments at 14.

[443] *See* FTC Staff Comments at 14-15; EFF Comments at 13; Comcast Comments at 49; CTIA Comments at 122-23; T-Mobile Comments at 41; WISPA Comments at 14.

[444] *See, e.g.*, Online Trust Alliance Comments at 3; McDonald Reply at 3 ("Many ISPs provided limited information to users, at best informing users that terms and conditions had changed without explaining the scale and scope of privacy change. Some ISPs reportedly did not notify users at all.").

[445] *2015 Open Internet Order*, 30 FCC Rcd at 5671-72, para. 161.

[446] *Id.* at 5672-73, para. 164.

[447] *See* CTA Comments at 11 (arguing that material change notices will result in notice fatigue).

that providers are frequently changing their policies materially, they should alert their customers to that fact, or risk rendering their earlier efforts at transparency fruitless.

158. For the purposes of this rule, we consider a "material change" to be any change that a reasonable customer would consider important to her decisions on her privacy. This parallels the consumer interest-focused definition of "material change" used in the *2015 Open Internet Order*.[448] Such changes would primarily include any changes to the types of customer PI at issue, how each type of customer PI is used or shared and for what purpose, or the categories of entities with which the customer PI is shared. To provide guidance on the standard above, at minimum, if any of the required information in the initial privacy notification changes, then the carrier must provide the required update notice. We adopt this guidance because the initial notice contains the information on which customers are making their privacy decisions, and changes to that information may alter how consumers grant permissions to their carriers. We also limit carriers' requirements under this section to existing customers, since only existing customers (and not new applicants) would have a current privacy policy that could be materially changed.

159. *Delivering Notices of Material Changes*. For consumers to understand carriers' privacy practices, carriers must keep them up to date and persistently available, but must also ensure that customers' knowledge of them is up to date. It is not reasonable, for instance, to expect consumers to visit carriers' privacy policies on a daily basis to see if anything has changed. Therefore, we require telecommunications carriers to notify an affected customer of material changes to their privacy policies by contacting the customer with an email or some other form of active communication agreed upon by the customer.

160. We require active forms of communication with the customer because merely altering the text of a privacy policy on the carrier's website alone is insufficient. There is little chance that, absent some form of affirmative contact, a customer would periodically visit and review a provider's notices of privacy policies for any changes.[449] We also recommend, but do not require, providers to solicit customers' contact preferences to enable customers to choose their preferred method of active contact (such as email, text messaging, or some other form of alert), as not all customers have the same contact preferences. This is particularly true for voice services, where it may be less likely that customers will visit a provider's website, and providers may not have a customer's email address.[450] While this does require each provider to have some means of contacting the customer, it does not require gathering more customer information, since, by virtue of providing service, a provider will necessarily be able to contact a customer, whether by email, text message, voice message, or postal mail.[451] Some commenters have expressed concern that requiring carriers to send multiple notices in different formats for each material change would present "significant logistical challenges."[452] The rules do not require multiple formats for

[448] The definition differs from that in the *2015 Open Internet Order* in two respects: the customer's interest is defined by the customer's decisions on privacy, and not choice of provider, service, or application; and the reference to edge providers, which are not relevant to the material changes at issue, has been removed. *See* WISPA Comments at 14.

[449] *Cf.* NTCA Reply at 42-43 (submitting that push notices and billing statements, supplemented by a notice on the website, are sufficient); *contra* CenturyLink Comments at 21-22 (arguing that initial notice of privacy policies and disclosure on a website is sufficient).

[450] *See* NCTA Comments at 85 (suggesting text messages as one form of notice and solicitation).

[451] *But cf.* CenturyLink Comments at 21-22 (arguing that actively contacting customer required further data collection).

[452] *See, e.g.*, Letter from Rebecca Murphy Thompson, EVP & General Counsel, Competitive Carriers Association, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 3 (filed Oct. 13, 2016) (CCA Oct. 13, 2016 *Ex Parte*).

each notice of material change, but allow carriers to use one method, whether that is email or some other active method agreed upon by the customer.

161. The active notice requirements reflect the rationale behind the transparency requirements of the *2015 Open Internet Order*, which require directly notifying end users if the provider is about to engage in a network practice that will significantly affect a user's use of the service.[453] As explained in that *Order*, the purpose is to "provide the affected [] users with sufficient information. . . " to make choices that will affect their usage of the service.[454] Given these existing obligations, we disagree with commenters who suggest that providing more than one notice is overly burdensome.[455]

162. In addition to the active notice required above, we encourage providers to include notices of changes in customers' billing statements, whether a customer has selected electronic billing, paper bills, or some other billing format.[456] Providing notice via bills can help ensure that customers will receive the notice, and makes it more likely that they will correctly attribute the notice as coming from their provider.[457]

163. *Contents of Advance Notice of Material Changes*. As proposed in the *NPRM*, the advance notice of material change must specify and describe the changes made to the provider's privacy policies, including any changes to what customer PI the provider collects; how it uses, discloses, or permits access to such information; and the categories of entities with which it shares that information.[458] This explanation should also include whether any changes are retroactive (i.e., they will involve the use or sharing of past customer PI that the provider can access).[459] The entire notice must be clear and conspicuous, comprehensible, and not misleading. The notice of material change need not contain the entirety of the provider's privacy policies, so long as it accurately conveys the relevant changes and provides easy access to the full policies. Moreover, the notice of material change must not simply provide fully updated privacy policies without specifically identifying the changes—as stated above, the changes must be identified clearly, conspicuously, comprehensibly, and in a manner that is not misleading. For the same reasons that we impose this requirement with respect to the notice of privacy policies, we also require that the notice of material change be translated into a language other than English if the telecommunications carrier transacts business with the customer in that language. As with the initial notice of privacy policies, the notice of material change must also explain the customer's rights with regard to this information. We do not, however, require that carriers use any particular language in these explanations, and encourage carriers to adapt their notices in ways that best suit their customers. We decline to specify how much advance notification providers must give their customers before making material changes to their privacy policies, recognizing that the appropriate amount of time will vary, *inter*

[453] *2015 Open Internet Order*, 30 FCC Rcd at 5677, para. 171.

[454] *Id.*

[455] *See, e.g.*, CenturyLink Comments at 21-22.

[456] *See generally* NTCA Comments at 40-41 (noting that many customers do not receive printed billing statements).

[457] *Cf.* McDonald Reply at 3-4 (noting 11 percent of consumers in one survey who believed an opt-out notice was a scam).

[458] *See Broadband Privacy NPRM*, 31 FCC Rcd at 2533-35, paras. 96, 100; 31 FCC Rcd at 2605, Appendix A (proposed §64.7001(c)(1)).

[459] *See* FTC Staff Comments at 14-15; *see also* 2012 FTC Privacy Report at 57-58.; EFF Comments at 13; Comcast Comments at 49; CTIA Comments at 122-23; T-Mobile Comments at 41; WISPA Comments at 14. The Administration CPBR similarly notes that "previously collected personal data" calls for increased privacy controls over ongoing collection. 2015 Administration CPBR Discussion Draft, § 102(e)(2). As discussed in Part III.D.1.a(ii) below, if the material change affects previously collected information, then, consistent with FTC precedent and recommendations, the carrier must obtain opt-in consent for that new use of previously collected information.

*alia*, based on the scope of the change or the sensitivity of the information at issue. However, BIAS providers and other telecommunications carriers must give customers sufficient advance notice to allow the customers to exercise meaningful choice with respect to those changed policies.

#### 5. Harmonizing Voice Rules

164. As noted above, we apply these rules to all providers of telecommunications services. Harmonizing the rules for broadband and other telecommunications services will allow providers that offer multiple (and frequently bundled)[460] services within this category to operate under a more uniform set of privacy rules, reducing potential compliance costs.[461] For example, our rules will enable providers to provide the necessary notices for both voice and broadband services at the point of sale, allowing the information to be conveyed in one interaction for customers purchasing bundles, minimizing burdens on providers and customers alike.[462] Furthermore, this consistency also enhances the ability of customers purchasing BIAS and other telecommunications services from a single provider to make informed choices regarding the handling of their information.

165. In harmonizing our notice rules across BIAS and other telecommunications services, we are able to reduce burdens on providers by eliminating certain existing requirements that we find are no longer necessary. For instance, because we require that notice of privacy practices be readily available on providers' websites, an already common practice,[463] we eliminate the requirement that notices of privacy practices be re-sent to customers every 2 years.[464] Further, because the record evinces the growing need for flexibility in applying the principles of transparency, we eliminate requirements that notices provide that "the customer has a right, and the carrier has a duty, under federal law, to protect the confidentiality of CPNI" [465]—a requirement that has apparently been interpreted as requiring that language to appear verbatim in privacy policies.[466] Similarly, we eliminate requirements that emails containing notices of material changes contain specific subject lines, leaving to providers the means by which they can meet the general requirements that any communication must be clear and conspicuous, comprehensible, and not misleading. We find that in lieu of these more prescriptive requirements, the common-sense rules we adopt above better ensure that customers receive truly informative notices without unnecessary notice fatigue or unnecessary regulatory burdens on carriers.

### D. Customer Approval Requirements for the Use and Disclosure of Customer PI

166. In this section, we adopt rules that give customers of BIAS and other telecommunications services the tools they need to make choices about the use and sharing[467] of their personal information, and to easily adjust those choices over the course of time. Respecting the choice of the individual is

[460] *See* Charter Reply at 13-14; NTCA Comments at 47; INCOMPAS Comments at 4-5; WTA Comments at 12.

[461] *See, e.g.*, NTCA Comments at 38-39; RWA Comments at 6-7; WTA Comments at 9; Letter from Catherine M. Hilke, Assistant General Counsel, Verizon, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 (filed Aug. 17, 2016).

[462] *See* Letter from Catherine M. Hilke, Assistant General Counsel, Verizon, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 at 1 (filed Oct. 13, 2016) (Verizon Oct. 13, 2016 *Ex Parte*).

[463] *See supra* note 360.

[464] *See* Privacy Rights Clearinghouse Comments at 4; WTA Comments at 15; XO Comments at 15.

[465] *See* 47 CFR § 64.2008(c)(1).

[466] *See* Letter from William H. Johnson, Senior Vice President, Federal Regulatory & Legal Affairs, Verizon, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 (filed June 23, 2016).

[467] Section 222 addresses the conditions under which carriers may "use, disclose, or provide access to" customer information. 47 U.S.C. § 222(c)(1), (c)(3), (d), (f). For simplicity throughout this document we sometimes use the terms "disclose" or "share" in place of "disclose or provide access to."

central to any privacy regime,[468] and a fundamental component of FIPPs.[469] In adopting Section 222, Congress imposed a duty on telecommunications carriers to protect the confidentiality of their customers' information, and specifically required that carriers obtain customer approval for use and sharing of individually identifiable customer information. In adopting rules to implement these statutory requirements, we look to the record, which includes substantial discussion about customers' expectations in the context of the broader Internet ecosystem, as well as existing regulatory, enforcement, and best practices guidance. We are persuaded that sensitivity-based choice rules are the best way to implement the mandates of Section 222, honor customer expectations, and provide carriers the ability to engage their customers.

167. We therefore adopt rules that require express informed consent (opt-in approval) from the customer for the use and sharing of sensitive customer PI. As described in greater detail below, our rules treat the following information as sensitive: precise geo-location, health, financial, and children's information; Social Security numbers; content; and web browsing and application usage histories and their functional equivalents. For voice providers, our rules also treat call detail information as sensitive. With respect to non-sensitive customer PI, carriers must, at a minimum, provide their customers the ability to opt out of the carrier's use or sharing of that non-sensitive customer information. Carriers must also provide their customers with an easy-to-use, persistent mechanism to adjust their choice options.[470]

168. The sensitivity-based choice approach we adopt is not monolithic. We recognize certain congressionally-directed exceptions to customer approval rights. Most obviously, carriers can, and indeed must, use and share customer PI in order to provide the underlying telecommunications service, to bill and collect payment for that service, and for certain other limited purposes by virtue of delivering the service. Congress also recognized that there are other laws and regulations that allow or require carriers to use and share customer PI without consent. Therefore, we adopt exceptions to our choice framework that allow carriers to use and share information for the congressionally directed purposes outlined in the Communications Act, and as otherwise required or authorized by law.

169. In the first part of this section, we discuss our application of a sensitivity-based framework to the use and sharing of customer PI. We explain what we consider to be sensitive customer PI, and how our rules apply the sensitivity-based framework. In the second part of this section, we explain and implement the limitations and exceptions to that choice framework.

170. In the next parts of this section, we discuss the mechanisms for customer approval provided for in our rules. We explain how and when carriers must solicit and obtain customer approval to use and share the customer's PI under the framework we adopt today, and require carriers to provide customers with easy access to a choice mechanism that is simple, easy-to-use, clearly and conspicuously disclosed, persistently available, and made available at no additional cost to the customer. Finally, we eliminate the requirements that telecommunications providers keep particular records of their use of customer PI and periodically report compliance to the Commission.

171. These rules apply both to BIAS and other telecommunications services. The record reflects strong support for consistency between privacy regimes for all telecommunications services, both to reduce possible consumer confusion,[471] and to decrease compliance burdens for all affected

[468] *See, e.g.*, 47 U.S.C. §§ 551(c), 338(i)(4) (imposing on cable operators and satellite carriers, respectively, requirements to obtain subscriber consent prior to disclosing personally identifiable information).

[469] *See supra* note 341.

[470] As discussed below, we do not consider a carrier's sharing of customer PI with the carrier's own agents to constitute sharing with third parties that requires either opt-in or opt-out consent. *See infra* note 623.

[471] *See, e.g.*, Verizon Comments at 9 ("[H]aving to deal with different and even inconsistent privacy frameworks will inevitably lead to consumer confusion and frustration."); CTIA Comments at 96 ("The Commission likewise should use data sensitivity and flexibility as its touchstones so that its rules. . . will meet consumer expectations, avoid consumer confusion, and minimize other harms associated with disparate privacy regulation across the

(continued….)

telecommunications carriers, particularly small providers.[472] Therefore, within the scope of our authority over telecommunications carriers, we apply these rules to all BIAS providers and other telecommunications carriers.

### 1. Applying a Sensitivity-Based Customer Choice Framework

172. Except as otherwise provided by law and subject to the congressionally-directed exceptions discussed below, we adopt a customer choice framework that distinguishes between sensitive and non-sensitive customer information. We adopt rules that require BIAS providers and other telecommunications carriers to obtain a customer's opt-in consent before using or sharing sensitive customer PI.[473] We also adopt rules requiring carriers to, at a minimum, offer their customers the ability to opt out of the use and sharing of non-sensitive customer information. Carriers may also choose to obtain opt-in approval from their customers to use or share non-sensitive customer PI. To ensure that consumers have effective privacy choices, we require carriers to provide their customers with a persistent, easy-to-access mechanism to opt in to or opt out of their carriers' use or sharing of customer PI.

173. In adopting a sensitivity-based framework, we move away from the purpose-based framework—in which the purpose for which the information will be used or shared determines the type of customer approval required—in the current rules and in the rules we proposed in the *NPRM*.[474] Having sought comment on a sensitivity-based framework in the *NPRM*,[475] and having received substantial support for it in the record, we find that incorporating a sensitivity element into our framework allows our rules to be more properly calibrated to customer and business expectations. This approach is also consistent with the framework recommended by the FTC in its comments and its 2012 staff report, and

(Continued from previous page)
ecosystem."); CTIA Comments at 117 (agreeing "in principle that there may be significant advantages to harmonizing regulations to create the *right* regulatory framework for voice, broadband, and cable services—including both the delivery of an improved and simplified customer experience, and the realization of saved administrative costs."); LGBT Technology Partnership Comments at 4 ("In this regard, we encourage the Commission to adopt the FTC guidelines that protect date for all consumers and treats all companies equally thus avoiding consumer confusion and conflicting regulations."); Greenlining Institute Comments at 18 ("Commenters believe that a uniform regime is not only easier for the carriers, easier of enforcement, and easier for customers to understand, it is also consistent with the Open Internet Order in terms of law and policy."); WISPA Comments at 16 ("A combined privacy policy would provide more clarity and less confusion to customers.").

[472] WTA & Nex-Tech Apr. 25, 2016 *Ex Parte* at 1 (urging the Commission to "harmonize definitions, procedures and requirements in order to reduce the complexity of regulation of privacy and minimize the burdens on small providers"); Rural Wireless Association Comments at 7 ("RWA recommends that the Commission harmonize its proposals with existing regulations regarding CPNI."); WISPA Comments at 16-17 ("A combined privacy policy. . . would reduce the administrative burdens and costs of developing and maintaining separate policies, especially for small carriers that do not have sufficient resources."); WTA Comments at 3 ("[T]he Commission should make certain that its new broadband CPNI customer approval, security and notification rules correspond as much as practicable to its existing rules for voice and cable television service."); WTA Comments at 10 ("The Commission should also harmonize customer solicitation and approval requirements for voice and broadband services.").

[473] We also require carriers to obtain customer opt-in consent for material retroactive uses of customer PI, as discussed below. *See infra* para. 195.

[474] *Broadband Privacy NPRM*, 31 FCC Rcd at 2543-46, paras. 122-30 (proposing to require opt-out consent for uses of customer PI that were for the purpose of marketing communications-related services to customers, or for sharing information with affiliates offering communications-related services for the purpose of marketing those communications-related services to customers; and to require opt-in consent for all other purposes that require consent).

[475] *Broadband Privacy NPRM*, 31 FCC Rcd at 2548-49, para. 136 (seeking comment on a sensitivity-based framework); *see infra* note 477.

used by the FTC in its settlements.[476] We make this transition for both BIAS and other telecommunications services because the record demonstrates that a sensitivity-based framework better reflects customer expectations regarding how their privacy is handled by their communications carriers.[477]

174. Some commenters argue that all customer information is sensitive, and that subjecting only certain information to opt-in approval imposes an unnecessary burden on consumers who want to protect the privacy of their information to opt-out.[478] While we appreciate that consumers are not monolithic in their preferences, as discussed below, we think the rule we adopt today strikes the right balance and gives consumers control over the use and sharing of their information. We decline to conclude that all customer PI is sensitive by default, and instead identify specific types of sensitive information, consistent with the FTC.[479] Other commenters express concern that drawing a distinction between sensitive and non-sensitive information requires a broadband provider to analyze a customer's web browsing history and content to identify sensitive information, rendering the point of the distinction moot.[480] Some commenters argue that carriers can use a system of whitelists to determine sensitive versus non-sensitive web sites.[481] This argument mistakenly presumes that the sensitivity of a customer's traffic relies upon the type or contents of the sites visited, and not simply the fact of the customer having visited them. However, this dispute and the concerns underlying it are themselves mooted by our decision to treat content, browsing history, and application usage history as sensitive and subject to opt-in consent. Thus, recognizing customer expectations and the comments reflecting them in the record, we adopt rules that base the level of approval carriers must obtain from customers upon the sensitivity of the customer PI at issue.

175. Adopting this choice framework implements the requirement in Section 222(c)(1) that carriers, subject to certain exceptions, must obtain customer approval before using, sharing, or permitting access to individually identifiable CPNI. Further, we find that except where a limitation or exception discussed below applies, obtaining consent prior to using or sharing customer PI is a necessary component of protecting the confidentiality of customer PI pursuant to Section 222(a). We also observe that drawing distinctions that allow opt-out or opt-in approval is well-grounded in our Section 222

[476] *See* FTC Staff Comments at 21-22 (citing 2012 FTC Privacy Report at 40, n.189). The Administration's CPBR similarly proposes that individuals' control over the processing of their data be "in proportion to the privacy risk to the individual and consistent with context." 2015 Administration CPBR Discussion Draft §102(a).

[477] *See* FTC Staff Comments at 21-22; Future of Privacy Forum Comments at 26 (citing the NAI and DAA frameworks as drawing the sensitive/non-sensitive distinction); Future of Privacy Forum Reply at 8; Richard Bennett Comments at 5; ICLE Comments at 18; CompTIA Comments at 7; Internet Commerce Coalition Comments at 3; ACA Comments at 51-52; State Privacy & Security Coalition Comments at 5; CenturyLink Comments at 16, 28; Comcast Comments at 13; NCTA Comments at 3; WISPA Comments at 23; INCOMPAS Comments at 12; T-Mobile Comments at 8, 29; AT&T Comments at 1, 96-97; ANA Comments at 18; FTC Commissioner Maureen Ohlhausen (Ohlhausen) Comments at 1-2.

[478] *See* National Consumers League Comments at 7 ("NCL views all information held by BIAS providers to be sensitive and thus require the same, strict data security protections."); Letter from Dallas Harris, Policy Fellow, Public Knowledge, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed May 9, 2016) (Public Knowledge May 9, 2016 *Ex Parte*) ("[O]nly by treating all information as the most sensitive can the Commission ensure that highly sensitive information will not be compromised.").

[479] *See, e.g.*, OTI Oct. 13, 2016 *Ex Parte* at 3; Letter from Dallas Harris, Policy Fellow, Public Knowledge, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1 (filed Oct. 18, 2016).

[480] *See, e.g.*, Public Knowledge Comments at 24-26; Letter from Dallas Harris, Policy Fellow, Public Knowledge, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 3 (filed July 26, 2016) (Public Knowledge July 26, 2016 *Ex Parte*); Paul Ohm Reply at 10-12; National Consumers League Comments at 2.

[481] *See, e.g.*, Future of Privacy Forum Reply at 8; *see also* Letter from Austin C. Schlick, Director, Communications Law, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1 (filed Oct. 3, 2016) (Google Oct. 3, 2016 *Ex Parte*).

precedent and numerous other privacy statutes and regimes.[482] The Commission has long held that allowing a customer to grant partial use of CPNI is consistent with one of the underlying principles of Section 222: to ensure that customers maintain control over their own information.[483]

176. Below, we explain the framework and its application. First, we define the scope of sensitive customer PI and explain our reasons for requiring opt-in consent to use or share sensitive customer PI. Consistent with FTC enforcement work and best practices guidance, we also require telecommunications carriers that seek to make retroactive material changes to their privacy policies to obtain opt-in consent from customers. Next, we discuss our reasons for allowing carriers to use and share non-sensitive customer PI subject to opt-out approval.

#### a. Approval Requirements for the Use and Sharing of Sensitive Customer PI

##### (i) Defining Sensitive Customer PI

177. For purposes of the sensitivity-based customer choice framework we adopt today, we find that sensitive customer PI includes, at a minimum, financial information; health information; Social Security numbers; precise geo-location information; information pertaining to children; content of communications; call detail information; and a customer's web browsing history, application usage history, and their functional equivalents. Although a carrier can be in compliance with our rules by providing customers with the opportunity to opt in to the use and sharing of these specifically identified categories of information, we encourage each carrier to consider whether it collects, uses, and shares other types of information that would be considered sensitive by some or all of its customers, and subject the use or sharing of that information to opt-in consent.

178. In identifying these categories as sensitive and subject to opt-in approval, we draw on the record and consider the context, which is the customer's relationship with his broadband or other telecommunications provider. The record demonstrates strong support for designating these specific categories of information as sensitive: health information,[484] financial information,[485] precise geo-location information,[486] children's information,[487] and Social Security numbers. The FTC explicitly regards these

---

[482] *See, e.g.*, *NCTA v. FCC*, 555 F.3d 996 (D.C. Cir. 2009) (upholding the Commission's CPNI framework which required opt-in approval for certain uses and opt-out for others); 45 CFR §§ 164.508, 164.510 (HIPAA rule) (requiring opt-in approval for certain uses, and allowing opt-out approval (i.e., "opportunity for the individual to agree or to object") for others); COPPA, 15 U.S.C. § 6502 (requiring opt-in consent for most uses of children's information, but permitting certain uses with disclosures).

[483] *See 1998 CPNI Order*, 13 FCC Rcd at 8152, para. 118 (observing that "Section 222(c)(1) is silent on the issue of whether a customer may grant a carrier partial use or access to CPNI outside the scope of Section 222(c)(1)" and concluding that "[a] customer could grant approval for partial use, for example, by limiting the uses made of CPNI, the time period within which approval remains valid, and *the types of information that may be used*") (emphasis added).

[484] *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (HIPAA); *see also* FTC Staff Comments at 21.

[485] *See, e.g.*, Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (GLBA); *see also* FTC Staff Comments at 21. *See also infra* note 791.

[486] *See, e.g.*, FTC Staff Comments at 21.

[487] *See, e.g.*, Children's Online Privacy Protection Act, Pub. L. No. 105-277, 112 Stat. 2681-728 (1998) (COPPA); Common Sense Kids Action Comments at 2-3; Letter from Ariel Fox Johnson, Senior Policy Counsel, Privacy and Consumer Affairs, Common Sense Kids Action, to Tom Wheeler, Chairman, FCC, WC Docket No. 16-106, at 2 (filed Oct. 5, 2016) (Common Sense Kids Action Oct. 5, 2016 *Ex Parte*) ("Children's information, all of it, is sensitive. This is why the FTC's COPPA Rule protects a wide swathe of children's information—not just their social security numbers."); FTC Staff Comments at 21.

categories of information as sensitive, as well.[488] Despite some commenters' assertions to the contrary,[489] the FTC does not claim to define the outer bounds of sensitive information with this list.[490] For example, in its 2009 Staff Report on online behavioral advertising and in its comments to this proceeding, the FTC clearly indicated that its list was non-exhaustive.[491] Furthermore, Commission precedent and consumer expectations demonstrate strong support for certain additional categories of sensitive information. For instance, the Commission has also afforded enhanced protection to call detail information for voice services.[492] Consumer research also supports identifying several types of information as sensitive: the 2016 Pew study, noted by a number of commenters in the record, found that large majorities of Americans considered Social Security numbers, health information, communications content (including phone conversations, email, and texts), physical locations over time, phone numbers called or texted, and web history to be sensitive.[493] Each of these categories has a clear and well attested case in the record and in federal law for being considered sensitive.[494]

179. Consistent with the FTC and the record, we conclude that precise geo-location information is sensitive customer PI.[495] Congress specifically amended Section 222 to protect the privacy

[488] FTC Staff Comments at 19-20.

[489] *See, e.g.*, Letter from Michelle R. Rosenthal, Senior Corporate Counsel, T-Mobile, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1-2 (filed Oct. 14, 2016) (T-Mobile Oct. 14, 2016 *Ex Parte*) (asking the Commission to "consider narrowing the scope of sensitive CPNI to the five FTC categories"); Letter from James J.R. Talbot, Executive Director – Senior Legal Counsel, AT&T, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 3 (filed Oct. 17, 2016) (AT&T Oct. 17, 2016 *Ex Parte*) (claiming that the FTC considers information sensitive only if it is content or "falls within the traditional categories of sensitive data"); Advertisers Oct 10, 2016 *Ex Parte* at 3-4 (suggesting that FTC has "long held that 'sensitive data' encompasses a limited set of data types"); Letter from Sydney M. White, Counsel to Internet Commerce Coalition, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Oct. 18, 2016) (ICC Oct. 18, 2016 *Ex Parte*).

[490] FTC 2012 Privacy Report at 58-60 (observing general consensus that five categories were sensitive).

[491] *See* FTC, Self-Regulatory Principles for Online Behavioral Advertising: Behavioral Advertising Tracking, Targeting, & Technology (2009) 12 (setting out the principle that "companies should obtain affirmative express consent before they use sensitive data—*for example*, data about children, health, or finances—for behavioral advertising" (emphasis added)); FTC Staff Comments at 19-20 (supporting opt-in "for sensitive information that could be collected by BIAS providers, *including*: (1) content of communications and (2) Social Security numbers or health, financial, children's or precise geolocation data" (emphasis added)).

[492] *See 2007 CPNI Order*, 22 FCC Rcd at 6936, para. 13 (finding that "the release of call detail over the telephone presents an immediate risk to privacy" and imposing restrictions on its release); *id.* at 6936, n.45 (explaining that "'call detail' or 'call records' includes any information that pertain to the transmission of specific telephone calls including, for outbound calls, the number called, and the time, location, or duration of any call and, for in inbound calls, the number from which the call was placed, and the time, location, or duration of any call"; and finding that "a narrower definition that included only inbound or outbound telephone numbers would make it too easy for unauthorized persons with partial information to confirm and expand on that information").

[493] *See* Consumer Watchdog Comments at 2-3; Lee Rainie, The State of Privacy in post-Snowden America, Pew Research Center (Sept. 21, 2016) at http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/ft_16-01-20_ssnumbers-1/.

[494] *See* CTIA Comments at 96-97; Comcast Comments at 18; ANA Comments at 12; Electronic Transactions Association Comments at 13; Future of Privacy Forum Comments at 27; NCTA Comments at 44.

[495] *See* Letter from Maria L. Kirby, AVP Regulatory Affairs & Assoc. General Counsel, CTIA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Oct. 18, 2016); Letter from Michelle R. Rosenthal, Senior Corporate Counsel, Government Affairs, Federal Regulatory, T-Mobile, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1, n.1 (filed Oct. 19, 2016); *see also, e.g.*, 2012 FTC Report at 58-60; FTC Staff Comments at 19-20; CTIA Comments at 96-97; DMA Comments at 10-11; ANA Comments at 12; CCA Reply at 19-22; Verizon Reply at 21-22; Letter from Melissa Newman, Vice President-Federal Regulatory Affairs, CenturyLink, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 5 (filed Sept. 13, 2016); Letter from (continued….)

of wireless location information as the privacy impacts of it became clear.[496] Real-time and historical tracking of precise geo-location is both sensitive and valuable for marketing purposes due to the granular detail it can reveal about an individual. Such data can expose "a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[497] In some cases, a BIAS provider can even pinpoint in which part of a store a customer is browsing.[498] The FTC has found that precise geo-location data "includ[es] but [is] not limited to GPS-based, WiFi-based, or cell-based location information."[499]

180. The record also reflects the historical and widely-held tenet that the content of communications is particularly sensitive.[500] Like financial and health information, Congress recognized communications as being so critical that their content, information about them, and even the fact that they have occurred, are all worthy of privacy protections.[501] This finding is strongly supported by the record, and consistent with FTC guidance.[502] As the FTC explains, "content data can be highly personalized and granular, allowing analyses that would not be possible with less rich data sets."[503] We therefore concur with the large number of commenters who assert that content must be protected[504] and agree with Access Now in finding that "the use or sharing . . . of the content of user communications is a clear violation of the right to privacy."[505] As such, we consider communications contents to be sensitive information.[506]

181. We also add to the list of sensitive customer PI a customer's web browsing and application usage history, and their functional equivalents. A customer's web browsing and application

(Continued from previous page)
Francis M. Buono, Sr. Vice President, Legal Regulatory Affairs & Sr. Dep. General Counsel, Comcast Corp., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1 (filed Aug. 2, 2016); Future of Privacy Forum Comments at 22-23.

[496] *See* Wireless Communications and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286 (1999).

[497] *United States v. Jones*, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring). *Accord* CDT Comments at 14; EFF Comments at 3-4.

[498] *See Riley v. California*, 134 S.Ct. 2473, 2490 (2014) ("Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building."); CDD Comments at 14.

[499] *Goldenshores Technologies, LLC*, Decision and Order, F.T.C. Docket No. C-4446, at 3 (March 31, 2014). *Accord Snapchat, Inc.*, Decision and Order, F.T.C. Docket No. C-4501, at 2 (Dec. 31, 2014); *Designware, LLC*, Decision and Order, F.T.C. Docket No. C-4390, at 3 (April 11, 2013). As noted above in paragraph 66, we do not draw distinctions between technologies used to determine precise geo-location. We make clear, however, that we do not consider a customer's postal or billing address to be sensitive precise geo-location information, but rather to be non-sensitive customer PI when used in context as customer contact information.

[500] AAJ Comments at 8; ACLU Comments at 7-8; EFF Comments at 5; FTC Staff Comments at 21; OTI Comments at 23; Public Knowledge White Paper at 59; CCA Reply at 19.

[501] *See, e.g.*, 47 U.S.C. § 605; 18 U.S.C. § 2510 et seq.; 18 U.S.C. § 2701 et seq.; 18 U.S.C. § 3121 et seq.

[502] FTC Staff Comments at 20-21; *see also supra* note 500.

[503] FTC Staff Comments at 20.

[504] *See supra* note 500.

[505] Access Now Comments at 6.

[506] Designating content as sensitive customer PI will not, despite NCTA's concerns, require a carrier to obtain additional customer approval to accept or respond to communications with its customers. *See infra* para. 215; *see also* Letter from Loretta Polk, Vice President and Associate General Counsel, NCTA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Oct. 18, 2016).

usage history frequently reveal the contents of her communications,[507] but also constitute sensitive information on their own[508]—particularly considering the comprehensiveness of collection that a BIAS provider can enjoy and the particular context of the BIAS provider's relationship with the subscriber. The Commission has long considered call detail information sensitive, regardless of whether a customer called a restaurant, a family member, a bank, or a hospital. The confidentiality of that information, and its sensitivity, do not rely upon what category of entity the customer is calling. The same is true of a customer's web browsing and application usage histories.[509] We therefore decline to define a subset of non-sensitive web browsing and application usage history, as a number of commenters urge.[510]

182. Web browsing and application usage history, and their functional equivalents are also sensitive within the particular context of the relationship between the customer and the BIAS provider, in which 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. This is a different role than even the large online ad networks occupy—they may see many sites a subscriber visits, but rarely see all of them.[511] The notion is that before a BIAS provider tracks the websites or other destinations its customer visits the customer should have the right to decide upfront if he or she is comfortable with that tracking for the purposes disclosed by the provider.

183. As EFF explains, BIAS providers can acquire a lot of information "about a customer's beliefs and preferences—and likely future activities—from Web browsing history or Internet usage history, especially if combined with port information, application headers, and related information about a customer's usage or devices."[512] For instance, a user's browsing history can provide a record of her

[507] *See, e.g.*, Paul Ohm Testimony at 4-5 (explaining that a list of websites visited reveals a customer's reading history); Upturn Comments at 3-4 (explaining that web addresses can reveal web page content); OTI White Paper at 3-5. Some commenters raise the issue of cases drawing distinctions between "content" and "metadata" in the context of ECPA as standing for the proposition that all non-content data is non-sensitive. *See, e.g.*, Letter from Sydney M. White, Counsel to the Internet Commerce Coalition, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Oct. 13, 2016) (ICC Oct. 13, 2016 *Ex Parte*). We disagree. While the text of ECPA requires a court to make determinations of what is and is not "content" of communications to determine that statute's applicability, neither the statute nor the case law interpreting it suggests that information other than content cannot be considered sensitive under the Communications Act.

[508] *See, e.g.*, Letter from Dallas Harris, Policy Fellow, Public Knowledge to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1-2 (filed Oct. 21, 2016) (Public Knowledge Oct. 21, 2016 *Ex Parte*) (noting that the confidentiality of communications is not limited to their content in Sections 222 and 705).

[509] *See, e.g.*, Letter from Gaurav Laroia, Policy Counsel, Free Press, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 3 (filed Oct. 7, 2016).

[510] *See, e.g.*, AT&T Oct. 17, 2016 *Ex Parte* at 3; Google Oct. 3, 2016 *Ex Parte* at 1.

[511] *See, e.g.*, OTI White Paper at 3-5 (explaining that "[b]ecause of their special role handling all of a user's Internet traffic, ISPs have a uniquely detailed and comprehensive perspective on the activities of their subscribers."); Upturn White Paper at 6 (explaining that, even with encryption, "ISPs can still almost always see the domain names that their subscribers visit."); CDT Reply at 21 ("[A] BIAS provider's access to a consumer's data is unique because the BIAS provider serves as the gatekeeper between the consumer and the internet and the shepherd of the consumer's data across the internet . . . [A] BIAS provider [in the case of location information] will always have some form of location data for the consumer with the phone. . .simply because the BIAS provider cannot serve a phone that it cannot find."); Public Knowledge White Paper at 45 (arguing that "[b]roadband providers uniquely enjoy a confluence of both a total view into subscribers' Internet access habits on the one hand, and knowledge of physical information about the subscribers such as home address and financial information on the other."); Online Trust Alliance Comments at 1.

[512] EFF Comments at 4. *See also* 18MillionRising.Org Petition and Comments at 1 ("The tracking and cataloguing of consumers' online habits are especially harmful to marginalized communities, for whom information regarding immigration status, mental health, race, and religion can be particularly sensitive."); Julie Brill, Comm'r, Fed. Trade Comm'n, Net Neutrality and Privacy: Challenges and Opportunities, Keynote Address at Georgetown Institute for

(continued….)

reading habits—well-established as sensitive information[513]—as well as information about her video viewing habits,[514] or who she communicates with via email, instant messaging, social media, and video and voice tools. Furthermore, the domain names and IP addresses may contain potentially detailed information about the type, form, and content of a communication between a user and a website. In some cases, this can be extremely revealing: for instance, query strings within a URL may include the contents of a user's search query, the contents of a web form, or other information.[515] 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.[516] More detailed analysis of browsing history can more precisely determine detailed information, including a customer's financial status, familial status, race, religion, political leanings, age, and location.[517] The wealth of information revealed by a customer's browsing history indicates that it, even apart from communications content, deserves the fullest privacy protection.[518]

184. Web browsing, however, is only one form of sensitive information about a customer's online activities.[519] The use of other applications besides web browsers also provides a significant amount

(Continued from previous page)
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/publicstatements/2015/11/net-neutrality-privacy-challenges-opportunities ("Even 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.").

[513] *See* Paul Ohm Testimony at 4-5; *see also* Paul Ohm July 28, 2016 *Ex Parte* at 4-5; Future of Privacy Forum Reply at 6-7 (explaining that "sensitive data would include the content of detailed browsing histories"); Consumer Watchdog Comments at 2-3; *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044 (Colo. Sup. Ct. 2002) (en banc) (protecting privacy in book purchases).

[514] The cable and satellite privacy provisions of the Act were created in significant part to protect the privacy of video viewing habits. *See* H.R. Rep. No. 934, 98th Cong., 2d Sess. 29 (1984) ("Subscriber records from interactive systems can reveal details about bank transactions, shopping habits, political contributions, viewing habits and other significant personal decisions"); 47 U.S.C. § 551; 47 U.S.C. § 338(i). Video rental records have also been recognized by Congress as worthy of particular privacy protection. VPPA, 18 U.S.C. § 2710 et seq. As such, we disagree with Google's assertions that web browsing has not traditionally been considered sensitive information. Google Oct. 3, 2016 *Ex Parte* at 1 (drawing a distinction between medical records and shopping habits).

[515] *See, e.g.*, Andrew G. West & Adam J. Aviv, On the Privacy Concerns of URL Query Strings, 2014 Proc. of the 8th Workshop on Wed 2.0 Sec. and Privacy, available at http://w2spconf.com/2014/papers/privacy_query_strings.pdf; Reisman and Narayanan June 17, 2016 *Ex Parte* at 22-24 (customer names and other PII included in some URLs); *see also* Peter Swire Working Paper at 9 (noting that encryption can block access to detailed URLs, which "can reveal granular details of a user's search or other online activities").

[516] *See, e.g.*, OTI White Paper at 5.

[517] *See* OTI Oct. 13, 2016 *Ex Parte* at 7-9; Letter from Brandi Collins, Director of Campaigns: Economic, Environmental, & Media Justice Departments, Color of Change, to Tom Wheeler, Chairman, FCC, WC Docket No. 16-106 (filed Oct. 20, 2016) (Color of Change Oct. 20, 2016 *Ex Parte*); Letter from Laura M. Moy & Eric. G. Null, New America's Open Technology Institute, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Sept. 12, 2016); Letter from Brandi Collins, Director of Campaigns: Economic, Environmental & Media Justice Departments, Color of Change, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 at 2-3 (filed Oct. 3, 2016) (Color of Change Oct. 3, 2016 *Ex Parte*).

[518] *See, e.g.*, Public Knowledge White Paper at 47 ("The IP address of the service being accessed can indicate much information about the subscriber based on the nature of the service: a household with children, for example, is likely to visit Disney's website; a domestic violence victim far more likely to be accessing helpline information.").

[519] *See, e.g.*, Feamster ISP Data Use Comments at 5 ("A user's DNS lookups can reveal activity patterns, the website that a user is visiting, and (due to website fingerprinting attacks) possibly even the web *pages* that a user visits. . . . This concern is likely to grow as consumers increasingly deploy [Internet of Things devices] in their homes, as the (continued….)

of insight into a user's behavior. Any of the information transmitted to and from a customer via a browser can just as easily be transmitted via a company-specific or use-specific application. Whether on a mobile device or a desktop computer, the user's newsreader application will give indications of what he is reading, when, and how; an online video player's use will transmit information about the videos he is watching in addition to the video contents themselves; an email, video chat, or over-the-top voice application will transmit and receive not only the messages themselves, but the names and contact information of his various friends, family, colleagues, and others; a banking or insurance company application will convey information about his health or finances; even the mere existence of those applications will indicate who he does business with. A customer using ride-hailing applications, dating applications, and even games will reveal information about his personal life merely through the fact that he uses those apps, even before the information they contain (his location, his profile, his lifestyle) is viewed.[520]

185. Considering the particular visibility of this information to telecommunications carriers, we therefore find that web browsing history and application usage history, and their functional equivalents, are sensitive customer PI.[521] Web browsing history and application usage history includes information from network traffic related to web browsing or other applications (including the application layer of such traffic), and information from network traffic indicating the website or party with which the consumer is communicating (e.g., their domains and IP addresses). We include their functional equivalents to ensure that the privacy of customers' online activities (today most frequently encompassed by browsing and application usage history) will be protected regardless of the specific technology or architecture used. We expect this to be particularly significant as the Internet of Things continues to develop. While a customer may expect that the people and businesses she interacts with will know some things about her—her bookstore will know what she's bought by virtue of having sold it to her—this is distinct from having her voice or broadband provider extract that information from her communications paths and therefore knowing every store she has visited and everything she has purchased.[522] Furthermore, as mentioned above, a carrier not only has the technical ability to access the information about the customer's calls to the bookstore or visits to its website; it could also, unlike the store, associate that information with the customer's other communications.[523] Edge providers, even those that operate ad networks, simply do not have sufficient access to an individual to put together such a comprehensive view of a consumer's online behavior. And, to the extent a customer wants to prevent edge providers from collecting information about her, she can adopt a number of readily available privacy-enhancing technologies.[524] While the knowledge of any one fact from a customer's online history (the use of an online app) may be known to several parties (including the BIAS provider, the app itself, the server of an in-app advertisement),[525] the BIAS provider has the technical ability to access the most complete and most unavoidable picture of that history. We therefore disagree with commenters who believe that browsing history or application usage are not sensitive in the context of the customer/BIAS provider relationship.[526]

(Continued from previous page)
DNS and IPFIX traffic from these devices may reveal an increasing amount of information about user behavior and activity.") (emphasis in original).

[520] *See, e.g.*, OTI Oct. 13. 2016 *Ex Parte* at 8-9.

[521] We do not take a position on how sensitive this information would be in other contexts, or what levels of customer approval would be appropriate in those circumstances.

[522] *See, e.g.*, 2012 FTC Privacy Report at 56; CDT Reply at 10; OTI Comments at 3-9; McDonald Reply at 6-7.

[523] *See supra* note 511.

[524] *See, e.g.*, Reisman and Narayanan June 17, 2016 *Ex Parte* at 34-35.

[525] *See, e.g.*, Comcast Comments at 26-27.

[526] *See, e.g.*, James Cooper Comments at 3 (noting that "it is clear that certain data (e.g. social security and credit card numbers, bank account information, drivers' license numbers, insurance information) may raise the risk of
(continued….)

186. Also, contrary to some commenters' arguments, the existence of encryption on websites or even in apps does not remove browsing history from the scope of sensitive information. As noted above,[527] encryption is far from fully deployed;[528] the volume of encrypted data does not represent a meaningful measure or privacy protection;[529] and carriers have access to a large and broad amount of user data even when traffic is encrypted, including, frequently, the domains and IP addresses that a customer has visited.[530] Comcast argues that because BIAS providers are limited to this information, they have less access to information overall.[531] While the record indicates that BIAS providers have a less granular view of encrypted web traffic than unencrypted, it does not change the breadth of the carrier's view or the fact that it acquires this information by virtue of its privileged position as the customer's conduit to the internet. Nor does it change the fact that this still constitutes a record of the customer's online behavior, which, as noted above, can reveal details of a customer's life even at the domain level.

187. In deciding to treat broadband customers' web browsing history, application history, and their functional equivalents as sensitive information, we agree with commenters, including technical experts, who explain that attempting to neatly parse customer data flowing through a network connection into sensitive and non-sensitive categories is a fundamentally fraught exercise.[532] As a number of commenters have noted, a network provider is ill-situated to reliably evaluate the cause and meaning of a customer's network usage.[533] We therefore disagree with the suggestion made by some commenters that web browsing is not sensitive, because providers have established methods of sorting data which do not require them to "manually inspect" the contents of packets.[534]

(Continued from previous page)
new- or existing-identity theft, and geolocation data may increase safety risks from stalking. Less clear, however, is the theory by which data, such as browsing histories, shopping records, MAC address, and application usage statistics, threaten privacy.").

[527] *See supra* para 34.

[528] *See, e.g.*, Reisman and Narayanan June 17, 2016 *Ex Parte* at 17-19; Upturn White Paper at 3-6; McDonald Reply at 4-5.

[529] *See, e.g.*, Upturn White Paper at 3-5. Comcast notes that few dispute on the record that a growing volume of traffic is encrypted. Comcast Reply at 38. However, the volume of encrypted data is not indicative of how much customer privacy is protected. For instance, a very small amount of browsing information can reveal that a customer is visiting a site devoted to a particular disease, while many times that data, unencrypted, would only reveal that the user had streamed a particular video. *See* Reisman and Narayanan June 17, 2016 *Ex Parte* at 10-16.

[530] Upturn White Paper at 6-9; Reisman and Narayanan June 17, 2016 *Ex Parte* at 26; SIIA Comments 3 ("Broadband service providers are unique in their ability to see the domains that their subscribers visit, even in cases where a web site uses encryption. Recent technical analysis has noted that '[b]ecause the user's computer is assigned by default to use the ISP's DNS server, the ISP is generally capable of retaining and analyzing records of the queries, which the users themselves send to the ISP in the normal course of their browsing.'"); Consumer Action Comments at 1; Consumer Watchdog Comments at 4; Internet Association Reply at 7.

[531] Comcast Reply at 38.

[532] *See, e.g.*, Narayanan and Reisman Reply at 3-4 (explaining that it is "technically infeasible" for ISPs to determine the sensitivity of Internet traffic); Upturn White Paper at 6-9 (describing how DNS information and encrypted network traffic can be highly revealing); EFF Comments at 5-6 (arguing that BIAS providers should not be able to "identify or inspect" network information "in order to determine whether it falls into a 'sensitive' category"); *see also* Common Sense Kids Action Oct. 5, 2016 *Ex Parte* at 1 (observing that privacy protections for children under COPPA extend to "how a child moves across different sites and services over time").

[533] *See, e.g.*, Public Knowledge Comments at 24-26; Public Knowledge July 26, 2016 *Ex Parte* at 3; Paul Ohm Reply at 10-12; National Consumers League Comments at 2.

[534] *See, e.g.*, Future of Privacy Forum Reply at 8 (suggesting that providers could "scan" or "categorize" network information into sensitive and non-sensitive categories).

188. This remains true even when providers do not attempt to classify customers' browsing and application usage as they use BIAS, but instead employ blacklists or whitelists of sensitive or non-sensitive sites and applications.[535] Although commenters cite various industry attempts to categorize consumer interests, and identify the sensitive categories among those, the definitions vary significantly between them.[536] Even within one set of classifications, the lines between what is and is not considered sensitive information can be difficult to determine. For instance, as Common Sense Kids Action points out, determining when browsing information belongs to a child, teen, or adult customer or user would require more than knowing the user's online destination.[537] Further, as OTI notes, something that is non-sensitive to a majority of people may nevertheless be sensitive to a minority, which may have the unintended consequence of disparately impacting the privacy rights of racial and ethnic minorities and other protected classes.[538] By treating all web browsing data as sensitive, we give broadband customers the right to opt in to the use and sharing of that information, while relieving providers of the obligation to evaluate the sensitivity and be the arbiter of any given piece of information.

189. We also observe that treating web browsing and application usage history as sensitive in the context of the BIAS/customer relationship is consistent with industry norms among BIAS providers. Until recently, for example, to participate in AT&T's GigaPower Premium Offer (i.e., to receive the fixed broadband service GigaPower at a lower cost), customers had to opt in to AT&T Internet Preferences. Under AT&T's Internet Preferences, "you agree to share with us your individual browsing, like the search terms you enter and the webpages you visit, so we can tailor ads and offers to your interests."[539] AT&T explained that "AT&T Internet Preferences works independently of your browser's privacy settings regarding cookies, do-not-track and private browsing" and that "[i]f you opt-in to AT&T Internet Preferences, AT&T will still be able to collect and use your Web browsing information independent of those settings."[540] In short, AT&T appears to have tracked web browsing history only pursuant to customer opt-in. Similarly, participation in Verizon's Verizon Selects program is on an opt-in basis. That opt-in program uses web browsing and application usage data, along with location, to develop marketing information about its customers.[541]

---

[535] *See, e.g.*, ICC Oct. 18. 2016 *Ex* Parte at 3; Letter from Christopher L. Shipley, Attorney & Policy Advisor, INCOMPAS, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Oct. 18, 2016); Advertisers Oct. 19, 2016 *Ex Parte* at 2.

[536] *See* Ohm Reply at 11-12 (noting that "[a]dvertisers can definitely target ads to people suffering from a particular disability on DAA platforms, definitely not on Facebook, and probably not on Google or NAI. Genomic information is only prohibited within the NAI definition [of sensitive information], arguably within Googles, and likely not Facebook's or DAA's. Ads targeted to symptoms might be barred by Google and maybe NAI, but probably not by Facebook or DAA.")

[537] Common Sense Kids Action Oct. 5, 2016 *Ex Parte* at 2.

[538] *See, e.g.*, OTI Oct. 13, 2016 *Ex Parte* at 2; Letter from Laura M. Moy & Eric. G. Null, New America's Open Technology Institute, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Sept. 12, 2016); Letter from 38 Public Interest Organizations to Chairman Tom Wheeler, Sept. 7, 2016, at 3-4; Letter from Brandi Collins, Director of Campaigns: Economic, Environmental & Media Justice Departments, Color of Change, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 at 2-3 (filed Oct. 3, 2016) (Color of Change Oct. 3, 2016 *Ex Parte*).

[539] AT&T, *U-verse With AT&T Gigapower*, https://www.att.com/esupport/article.html#!/u-verse-high-speed-internet/KM1011211 (last visited Sept. 13, 2016).

[540] *Id*.

[541] Torod Neptune, Verizon Wireless, How Verizon Selects from Verizon Wireless Works, Dec. 3, 2012, http://www.verizonwireless.com/news/article/2012/12/verizon-selects.html ("Verizon Selects will use location, web browsing and mobile application usage data, as well as other information including customer demographic and interest data, to create specific insights."); Verizon Wireless, Verizon Selects FAQs, http://www.verizonwireless.com/support/verizon-selects-faqs/ (last visited Oct. 5, 2016) ("Verizon Selects uses . .

(continued….)

190. We disagree with the assertions made by a number of advertising trade associations that web browsing history should not be considered sensitive customer PI because courts have "found that the advertising use of web browsing histories tied to device information does not harm or injure consumers."[542] We find this to be inapposite to the task we confront in applying Section 222 of the Act. These cases deal with a factually different, and significantly narrower, scenarios than we address through web browsing history in this Order.[543]

191. We recognize that there are other types of information that a carrier could add to the list of sensitive information, for example information that identifies customers as belonging to one or more of the protected classes recognized under federal civil rights laws. Commenters also describe as sensitive other forms of governmental identification,[544] biometric identifiers,[545] and electronic signatures.[546] Other privacy frameworks, both governmental and commercial, identify other types of information as particularly sensitive, such as race, religion, political beliefs, criminal history, union membership, genetic data, and sexual habits or sexual orientation.[547] Most of these categories already overlap with our established categories, or the use or sharing of such information would be subject to opt-in requirements pursuant to the requirement to obtain opt-in consent for the use and sharing of content and web browsing and application usage history. Moreover, as explained above, carriers are welcome to give their customers the opportunity to provide opt-in approval for the use and sharing of additional types of information. However, we recognize that as technologies and business practices evolve, the nature of what information is and is not sensitive may change,[548] and as customer expectations or the public interest may require us to refine the categories of sensitive customer PI, we will do so.

(Continued from previous page)
.[i]nformation about your wireless device including websites you visit, apps and features you use, and device and advertising identifiers . . .."). We provide these examples only to demonstrate that BIAS providers already treat web browsing and application usage history as sensitive and as subject to opt-in consent, and we do not mean to suggest that these existing or past programs are reasonable or consistent with the rules and standards we discuss in this Order.

[542] Advertisers Oct. 10, 2016 *Ex Parte* at 4.

[543] For instance, in both cases, the courts found that plaintiffs had failed to allege that they had suffered "loss" as that term is narrowly defined under the Computer Fraud and Abuse Act. *Mount v. PulsePoint, Inc.*, No. 13 Civ. 6592 (S.D.N.Y. Aug. 17, 2016), 2016 WL 5080131 at *7-8; *LaCourt v. Specific Media, Inc.*, No. SACV 10-1256 (C.D. Cal. April 28, 2011), 2011 WL 1661532 at *6. We do not adopt the CFAA's definitions of "damage" or "loss" for the purposes of this Order.

[544] WISPA Comments at 21; Electronic Transactions Association at 13.

[545] Paul Vixie Comments at 29; CDT Comments at 8.

[546] CDT Comments at 8.

[547] *See, e.g.*, EU General Data Protection Regulation, Article 9, Processing of Special Categories of Personal Data; Google, Sensitive Categories, http://www.google.com/policies/privacy/key-terms/#toc-terms-sensitive-categories; Google, Sensitive Personal Information, http://www.google.com/policies/privacy/key-terms/#toc-terms-sensitive-info; Facebook, Restricted information for Lead Ads, https://www.facebook.com/policies/ads/#lead_ads.

[548] For instance, some commenters have suggested that information considered non-sensitive at one point might reveal through later analysis information about protected classes. *See, e.g.*, Color of Change Oct. 3, 2016 *Ex Parte* at 2-3 ("[I]nformation drawn from the non-sensitive data can easily become proxy for protected class and sensitive information").

### (ii) Opt-In Approval Required for Use and Sharing of Sensitive Customer PI and Retroactive Material Changes in Use of Customer PI

192. As the FTC recognizes, "the more sensitive the data, the more consumers expect it to be protected and the less they expect it to be used and shared without their consent."[549] We therefore require BIAS providers and other telecommunications carriers to obtain a customer's opt-in consent before using, disclosing, or permitting access to his or her sensitive customer PI, except as otherwise required by law and subject to the other exceptions outlined in Part III.D.2.

193. Consistent with the Commission's existing CPNI rules and wider precedent,[550] opt-in approval requires that the carrier obtain affirmative, express consent from the customer for the requested use, disclosure, or access to the customer PI. Because Section 222(a) requires protection of the confidentiality of all customer PI, we include all types of sensitive customer PI, and not just sensitive, individually identifiable CPNI, within the definition of opt-in approval.[551] The broad support in the record for protecting sensitive information nearly unanimously argues that use and sharing of sensitive customer information be subject to customer opt-in approval.[552] The record demonstrates that customers expect that their sensitive information will not be shared without their affirmative consent, and sensitive information, being more likely to lead to more serious customer harm, requires additional protection.[553] For instance, the FTC recognizes that consumer expectations drive increased protections for sensitive information.[554] We find that requiring opt-in approval for the use and sharing of sensitive customer PI reasonably balances burdens between carriers and their customers. If a carrier's uses or sharing of customers' sensitive personal information benefits those customers,[555] the customer has every incentive to make that choice, and the carrier has every incentive to make the benefits of that choice clear to the customer.[556] We anticipate that this will increase the amount of clear and informative information that customers will have about the costs and benefits of participation in these programs. Carriers' incentives to encourage customer opt-in will likely be tempered by carriers' desire to avoid alienating customers with too-frequent solicitations to opt in.[557]

194. In contrast, we find that opt-out consent would be insufficient to protect the privacy of sensitive customer PI. Research has shown that default choices can be "sticky," meaning that consumers

[549] FTC Staff Comments at 21.

[550] *See* 47 CFR § 64.2003(k); NAI, NAI Code of Conduct at 6, http://www.networkadvertising.org/code-enforcement/code (last visited Oct. 13, 2016); NAI, NAI Mobile Application Code at 3, https://www.networkadvertising.org/mobile/NAI_Mobile_Application_Code.pdf (last visited Oct. 13, 2016).

[551] *See* Access Now Comments at 6.

[552] *See supra* note 477.

[553] *See, e.g.*, CenturyLink Comments at 16; James Cooper Comments at 3; ANA Comments at 25-26; CTIA Comments at 96-97; NTCA Comments at 28 ("[T]he proposition that Social Security numbers, date and place of birth, mother's maiden name, and unique government identification numbers . . . are guarded by customer is likely consistent with current consumer expectations."); CCA Reply at 19.

[554] FTC Staff Comments at 19-20 ("[T]he FTC has advocated that companies provide meaningful choices to consumers, with the level of choice being tied to consumer expectations. Under this approach, the FTC supports the use of opt-in for sensitive information that could be collected by BIAS providers.").

[555] *See* Verizon Reply at 7-9; CIPL Comments at 5; CompTIA Comments at 7; Lehr et al. Comments at 2-3.

[556] Willis Reply at 12-18 (noting defaults made "slippery" through marketing encouraged opting in to certain programs).

[557] *See* CenturyLink Comments at 27 (expressing concern that opt-in requirements may force providers to balance informing customers of information-sharing programs against the possibility of annoying or confusing those customers).

will remain in the default position, even if they would not have actively chosen it.[558] Further, opt-in regimes provide additional incentives for a company to invest in making notices clear, conspicuous, comprehensible, and direct.[559] Additionally, empirical evidence shows that relatively few customers opt out even though a larger number express a preference not to share their information, suggesting that they did not receive notice or were otherwise frustrated in their ability to exercise choice.[560] In an opt-in scenario, however, we anticipate that many consumers, solicited by carriers incentivized to provide and improve access to their notice and choice mechanisms, will wish to affirmatively exercise choice options around the use and sharing of sensitive information. Although we recognize that opt-in imposes additional costs, based on these factors we find that opt-in is warranted to maximize opportunities for informed choice about sensitive information.

195. *Material Retroactive Changes.* Notwithstanding the fact that our choice framework generally differentiates between sensitive and non-sensitive information, we agree with the FTC and other commenters that material retroactive changes require a customer's opt-in consent for changes to the use and sharing of both sensitive and non-sensitive information.[561] The record demonstrates widespread conviction that material retroactive changes to privacy policies should require opt-in approval from customers.[562] Retroactive changes in privacy policies particularly risk violating customers' privacy expectations because they result in a carrier using or sharing information already collected from a customer for one purpose or set of purposes for a different purpose. Because of this, we require that telecommunications carriers obtain customers' opt-in approval before making retroactive material changes to privacy policies. It is a "bedrock principle" of the FTC that "companies should provide

[558] *See* Willis Reply at 8-10; Behavioral Economics Consulting Group at 2 ("Research in Behavioral Economics has shown that most of the time, peoples' decisions do not conform to a model in which people are information seeking rational actors, guided by self-interest. In particular, where the decision is complex, the stakes are high – and/or the arena is unfamiliar, people are more likely to procrastinate or avoid a decision. In effect, the individual 'chooses' avoidance – and ends up being assigned whatever the system's designers have designated as the proxy for 'no answer.' Whoever defined that proxy becomes the *de facto* decision maker.").

[559] *Cf.* Greenlining Institute Comments at 29 (noting "dense, slippery and confusing language" in privacy notices); Access Now Comments at 10 ("Opt-out mechanisms typically suffer from cumbersome processes, offer little notice or explanation on the nature of the use, and often even deliberately obfuscate the methods and purposes of corporate programs that track users. Moreover, opt-out is useless in situations where customers have no context to understand the program or service at issue, how it impacts their privacy, or that it even exists in the first place."); Consumer Action Comments at 2; Consumer Watchdog Comments at 6; Privacy Rights Clearinghouse Comments at 4 ("It is tenuous at best to assume that a customer has approved use or sharing merely because she has not opted out of a practice. This is especially true if an opt-out choice is buried deep in a privacy notice, and is in no way in line with customers' expectations."); CDD Comments at 17.

[560] *See, e.g.*, Willis Reply at 11-12, n.31 (citing reports that only 0.5 percent of consumers opted out of a financial privacy default, when a far larger number of consumers expressed preferences against tracking); McDonald Reply at 3 (noting that in response to NebuAd tracking, "The total percentage of users to opt out was about 1%. . . . [T]his is dramatically lower than the percentage of users who prefer not to have data collected and used for targeted advertising. A majority of users who wanted to opt out did not, and their privacy preferences were violated by their ISPs."); Paul Ohm Reply at 7-10.

[561] FTC Staff Comments at 14-15 (recommending "affirmative express consent before making changes that apply to previously collected consumer information"); 2012 FTC Privacy Report at 57-58 (rejecting arguments from AT&T and Phorm that opt-out approval was sufficient, or that approval should be scaled to sensitivity or identifiability of data); EFF Comments at 13; WISPA Comments at 14; CTIA Comments at 122-23.

[562] *See, e.g.*, FTC Staff Comments at 14-15 (recommending "affirmative express consent before making changes that apply to previously collected consumer information"); 2012 FTC Privacy Report at 57-58; Charter Reply at 7; CTIA Comments at 123; Internet Commerce Coalition Reply at 1-2; *see also* NTCA Comments at 6 (noting that retroactive material changes can violate consumer expectations of privacy). The CPBR also highlights the need for advance notice of material changes to policies, and the need for additional protections such as express affirmative consent where such changes are retroactive. 2015 Administration CPBR Discussion Draft §102(e).

prominent disclosures and obtain affirmative express consent before using data in a manner materially different than claimed at the time of collection."[563] This means that, whether customer PI is sensitive or non-sensitive, a telecommunications carrier must obtain opt-in permission if it wants to use or share data that it collected before the time that the change was made. For instance, if a carrier wanted to change its policy to share a customer's past monthly data volumes with third party marketers, it would need to obtain the customer's opt-in permission. In contrast, if the carrier changes its policy to share the customer's future monthly data volumes with those same marketers, it would only need the customer's opt-out consent.

#### b. Approval Requirements for the Use and Sharing of Non-Sensitive Customer PI

196. We recognize that customer concerns about the use and sharing of their non-sensitive customer PI will be less acute than sharing of sensitive PI, and that there are significant benefits to customers and to businesses from some use and sharing of non-sensitive customer PI. However, we reject suggestions that consumers should be denied choice about the use and sharing of any of their non-sensitive information.[564] Empowering consumers by providing choice is a standard component of privacy frameworks.[565] Further, ensuring choice is necessary as a part of effectuating the duty to protect the confidentiality of customer PI under Section 222(a) and the duty to obtain the approval of the customer before using, disclosing, or permitting access to individually identifiable CPNI under Section 222(c)(1). Therefore, consistent with the FTC privacy framework, we require BIAS providers and other telecommunications carriers to obtain the customer's opt-out approval to use, disclose, or permit access to non-sensitive customer PI.[566]

197. We define opt-out approval as a means for obtaining customer consent to use, disclose, or permit access to the customer's proprietary information under which a customer is deemed to have consented to the use, disclosure, or access to the customer's covered information if the customer has failed to object thereto after the carrier's request for consent.[567] This definition, based on the existing CPNI voice rules, applies to all non-sensitive customer PI for all covered telecommunications carriers. The current CPNI rules define opt-out approval to require a thirty-day waiting period before a carrier can consider a customer's opt-out approval effective. We eliminate this requirement, and similarly decline to apply it to BIAS providers or other telecommunications carriers. As borne out in the record, we find that requiring carriers to enable customers to opt out at any time and with minimal effort will reduce the likelihood that customers' privacy choices would not be respected. As such, we believe that the 30-day waiting period is no longer necessary and provide additional regulatory flexibility by eliminating it.[568] We make clear, however, that while we do not adopt a specific timeframe for effectuating customers' opt-out approval choices, we do not expect carriers to assume that a customer has granted opt-out consent

[563] 2012 FTC Privacy Report at 57.

[564] *See, e.g.*, Free State Foundation Comments at 9 ("By requiring ISPs create an 'opt out' policy regarding the collection of 'any information that is linked or linkable to an individual,' the Commission risks discouraging ISPs from offering consumers targeted marketing deals or selling advertisements to personally design consumer experiences.").

[565] *See supra* para. 166.

[566] We note that our requirements for customer opt-out approval serve as a floor, not a ceiling, to the level of customer approval to be provided. Thus, a carrier may set up its programs to solicit and receive customer opt-in approval if it so chooses.

[567] *See Broadband Privacy NPRM*, 31 FCC Rcd at 2523, para. 68.

[568] *See, e.g.*, Access Now Comments at 6; Consumer Federation of California Comments at 14. *But see* EFF Comments at 6 (opposing removing the 30-day timeframe); OTI Comments at 24 (suggesting in the alternative a 7-day period).

when a reasonable customer would not have had an opportunity to view the solicitation. We conclude that this flexible standard will appropriately account for the faster pace of electronic transactions, while preventing carriers from using customer PI before customers have had the opportunity to opt out.

198. We agree with commenters who assert that non-sensitive information naturally generates fewer privacy concerns for customers, and as such does not require the same level of customer approval as for sensitive customer PI.[569] From this, we conclude that an opt-out approval regime for use and sharing of non-sensitive customer PI would likely meet customers' privacy expectations. We agree with ANA that "[a]n opt-out framework for uses of non-sensitive information also matches consumers' expectations regarding treatment of their data,"[570] and CTIA that "[b]y tying its rules to the sensitivity of the data, the Commission will ensure that they align with consumer expectations and what consumers know to be fair."[571] While an opt-out regime places a greater burden than an opt-in regime upon customers who do not wish for their carrier to use or share their non-sensitive information, research suggests that those same customers will likely be more motivated to actively exercise their opt-out choices.[572] Further, we conclude that permitting carriers to use and share non-sensitive data with customers' opt-out approval—rather than opt-in approval—grants carriers flexibility to make improvements and innovations based on customer PI.[573] For example, ACA notes that an opt-out framework can allow "providers, including small providers, to explore, market, and deploy innovative, value-added services to their consumers, including home security and home automation services that will drive the 'Internet of Things.'"[574] Thus, we reject arguments that "opt-out is not an appropriate mechanism to obtain user approval" in any circumstances.[575]

199. We disagree with commenters who assert that customer approval to use and share customer PI for the purposes of all first party marketing is generally implied in Section 222.[576] We find that allowing carriers to use or share customer PI for all first party marketing does not comport with Section 222's customer approval and data protection requirements. Section 222(c)(1) explicitly requires customer approval to use and share CPNI for purposes other than providing the telecommunications

[569] *See, e.g.*, FTC Staff Comments at 22-23 (arguing that a privacy framework should "reflect the different expectations and concerns that consumers have for sensitive and non-sensitive data").

[570] ANA Comments at 27.

[571] CTIA Comments at 97.

[572] *See* Letter from Scott Bergmann, Vice President, Reg. Affairs, CTIA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 (filed Aug. 18, 2016) (CTIA Aug. 18, 2016 *Ex Parte*), Attach., ITIF White Paper, Why Broadband Discounts for Data are Pro-Consumer at 4-5 (ITIF White Paper) (describing Alan Westin's groupings of consumers by privacy preference, including "Privacy Fundamentalists" likely to value privacy highly). *But see* Consumer Watchdog Comments at 6 (citing Hoofnagle et al.'s criticisms of Westin's categorizations and Turow, *Tradeoff Fallacy*, which suggests consumer disclosure of data is due to resignation rather than actively trading on their personal information).

[573] ITIC Comments at 14-15; FTC Staff Comments at 22-23.

[574] ACA Comments at 31; *see also* SIIA Comments at 10; Letter from Joshua Seidemann, Vice President of Policy, NTCA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Oct. 14, 2016) (NTCA Oct. 14, 2016 *Ex Parte*) (arguing that the rules should not require opt-in approval for marketing services such as hardware/software systems and alarm/security services).

[575] Access Now Comments at 10; *see also, e.g.*, Consumer Action Comments at 2; Consumer Watchdog Comments at 6 ("Opt-out consent is insufficient. In fact, it is not really consent.").

[576] *See, e.g.*, Letter from Francis M. Buono, Senior Vice President, Legal Regulatory Affairs, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Sept. 22, 2016) (Comcast Sept. 22, 2016 *Ex Parte*); Letter from Michelle R. Rosenthal, Senior Corporate Counsel, T-Mobile USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 at 3 (filed Sept. 13, 2016) (T-Mobile Sept. 13, 2016 *Ex Parte*); NCTA Reply at 42-43; ICC Comments at 4; CTA Comments at 8.

service, and subject to certain other limited exceptions. Likewise, Section 222(a) imposes a duty on carriers to protect the confidentiality of customer PI. We conclude that permitting carriers to use and share customer PI to market all carrier and affiliate services based on inferred customer approval is inconsistent with these statutory obligations.[577] Our conclusion is also consistent with Commission precedent and FTC Staff comments.[578] While some comments assert that customers expect some degree of targeted marketing absent explicit customer approval,[579] the record also indicates that customers expect choice with regard to the privacy of their online communications.[580] Inferring consent for all first-party marketing would leave consumers without the right to opt out of receiving any manner of marketing from their telecommunications carrier—violating that basic precept recognized by Justice Louis Brandeis of the "right of the individual to be let alone."[581] We accordingly adopt an opt-out regime for first-party marketing that relies on non-sensitive customer PI to fulfill Section 222 and provide customers with the choice that they desire without unduly hindering the marketing of innovative services.

200. Giving consumers control of the use and disclosure of their information, even for first-party marketing, is consistent with other consumer protection laws and regulations adopted by the both the FTC and FCC. For instance, the popular and familiar National Do Not Call registry, created by the FTC, the FCC, and the states empowers consumers to opt out of most telemarketing calls.[582] Consumers have registered over 222 million phone numbers with the Do Not Call Registry in order to stop unwanted marketing calls.[583] Also, pursuant to rules adopted by both the FTC and the FCC, consumers to have the right to opt out of receiving calls even from companies with which they have a prior business relationship,

[577] *See, e.g.*, EFF Comments at 8 (arguing that implied consent in general "eliminate[s] all customer control over PII for a large range of activities, including marketing," and that this is inconsistent with the statute); EPIC Comments at 20 (claiming that "allow[ing] the use of personal information to market additional service offerings without any customer consent conflicts with Section 222(c) of the Communications Act," since it does not obtain the required customer approval); OTI Comments at 37-38 (arguing that there is no implied approval for marketing, and that marketing is not "necessary to, or used in" provision of service); Public Knowledge May 9, 2016 *Ex Parte* at 1 ("While there is precedent establishing that an opt-out system is sufficient to show customer approval, there is no authority for the proposition that a customer 'impliedly' approves of a carrier using his or her information for the purposes of Section 222(c)."); Letter from Dallas Harris, Policy Fellow, Public Knowledge, to Marlene H. Dortch, Secretary, FCC, WC Docket no. 16-106, at 1 (filed May 27, 2016); Paul Vixie Comments at 13 (arguing that implied consent for marketing "denies consumer any choice or control").

[578] FTC Staff Comments at 16. This same rationale applies to other telecommunications carriers. We note that, as discussed below, limited types of first-party marketing (of categories of service to which a customer subscribes, and services necessary to, or used in, those services) do not require customer approval.

[579] *See, e.g.*, Comcast Comments at 49-50; *see also* AT&T Reply at 9 ("Until now, all online companies have been free to use nonsensitive customer-specific information to engage in first-party marketing without any consent mechanism."); Verizon Comments at 24, 31 (asserting that for decades, businesses have "sen[t] ads or promotions to customers for the provider's and its affiliates' products or services"); NTCA Comments at 45-46 (suggesting that "[c]ustomers largely expect firms that have access to their data to use their data" and that "consumers expect providers to identify the services and uses that best meet their needs"); T-Mobile Comments at 8-9 (arguing that customers expect their information to be used for different purposes, including marketing, as adjusted to the sensitivity of the information); ACA Comments at 31.

[580] *See supra* note 208; *see also* ACLU Comments at 8-9; Access Now Comments at 9; CDT Reply at 6; Public Knowledge Comments at 29-30.

[581] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 195 (1890).

[582] *See* 47 CFR § 64.1200; 16 CFR Part 310; *see also, e.g.*, Mich. Comp. Laws § 445.111a (2016); N.D. Cent. Code § 51-28-09 (2016).

[583] Federal Trade Commission, Biennial Report to Congress Under the Do Not Call Registry Fee Extension Act of 2007, FY 2014 and 2015 at 1 (2015), https://www.ftc.gov/reports/biennial-report-congress-under-do-not-call-registry-fee-extension-act-2007-fy-2014-2015.

with businesses required to place the consumer on a do-not-call list upon the consumer's request.[584] The CAN SPAM Act of 2003,[585] and the rules the FTC adopted under CAN SPAM, also give consumers the right to opt out of the receipt of future commercial email from and require senders of commercial email to provide a working mechanism in their email to facilitate those opt-outs.[586] Our rules follow these many models.

### 2. Congressionally-Recognized Exceptions to Customer Approval Requirements for Use and Sharing of Customer PI

201. In this section, we detail the scope of limitations and exceptions to the customer approval framework discussed above. In the first part of this section, based on our review of the record and our analysis of the best way to implement Section 222, we find that no additional customer consent is needed in order for a BIAS provider or other telecommunications carrier to use and share customer PI in order to provide the telecommunications service from which such information is derived or provide services necessary to, or used in, the provision of such telecommunications service. These limitations on customer approval requirements allow a variety of necessary activities beyond the bare provision of services, including research to improve or protect the network or telecommunications, and limited first-party marketing of services that are part of, necessary to, or used in the provision of the telecommunications service. In the second part of this section, we apply the statutory exceptions detailed in Section 222(d) to all customer PI, allowing telecommunications carriers to use and share customer PI to: (1) initiate, render, bill, and collect for telecommunications services; (2) protect the rights or property of the carrier, or to protect users and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, telecommunications services; (3) provide any inbound telemarketing, referral, or administrative services to the customer for the duration of a call; and (4) provide customer location information and non-sensitive customer PI in certain specified emergency situations.[587] We also take this opportunity to clarify that our rules do not prevent use and sharing of customer PI to the extent such use or sharing is allowed or required by other law.

202. The statutory mandate of confidentiality is not an edict of absolute secrecy. The need to use and share customer information to provide telecommunications services, to initiate or render a bill, to protect the network, and to engage in the other practices identified above are inherent in a customer's subscription. While Congress specified this in the context of its more detailed provisions on customer approval for CPNI in Sections 222(c)-(d), it left to the Commission the details of determining the scope of the duty of confidentiality. We therefore exercise our authority to adopt implementing rules in order to harmonize the application in our rules of Section 222(a) as to customer PI with the limitations and exceptions of Sections 222(c)-(d). Doing so ensures that carriers are not burdened with disparate or duplicative approval requirements based upon whether a particular piece of information is classified as CPNI, PII, or both.[588] We disagree with commenters who argue that extending these limitations and exceptions to approval requirements unduly risk customers' privacy.[589] We make clear that carriers using

[584] *See* 47 CFR § 64.1200(d)(3); 16 CFR § 310.4(b)(1)(iii).

[585] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003) ("CAN SPAM Act").

[586] 16 CFR §§ 316.1-316.6.

[587] 47 U.S.C. § 222(d).

[588] *See supra* Part III.B.3 (noting that the categories of CPNI and PII are not mutually exclusive).

[589] *See, e.g.*, EFF Comments at 8 (arguing that access to all customer PI includes access to communications content, contrary to Stored Communications Act); OTI Comments at 38-39 (sensitive information not useful for exceptions and exposes customers to greater risk of harm); Access Now Comments at 9 ("The proposal as written does not provide meaningful limits on sharing CPNI, which can include sensitive user information, such as location and browsing habits. Instead, the proposal should only permit the sharing of CPNI to the extent that any PII or other private data is scrubbed and only 'whenever reasonably necessary to prevent future cyber security threats or risk of (continued….)

or sharing customer PI should remain particularly cognizant of their obligation to comply with the data security standards in Part III.E, below. We also emphasize that carriers should be particularly cautious about using sensitive customer PI, especially the content of communications, and carriers should carefully consider whether its use is necessary before making use of it subject to these limitations and exceptions. Furthermore, we observe that BIAS providers and other telecommunications carriers remain subject to all other applicable laws and regulations that affect their collection, use, or disclosure of communications, including but not limited to, the Electronic Communications Privacy Act (ECPA), the Communications Assistance for Law Enforcement Act (CALEA), Section 705 of the Communications Act, and the Cybersecurity Information Sharing Act (CISA).[590]

#### a. Provision of Service and Services Necessary to, or Used in, Provision of Service

203. Section 222 makes clear that no additional customer consent is needed to use customer PI to provide the telecommunications service from which it was derived, and services necessary to, or used in the telecommunications service.[591] Consent to use customer PI for the provision of service is implied in the service relationship.[592] Customers expect their information to be used in the provision of service—after all, customers fully intend for their communications to be transmitted to and from recipients—and they necessarily give their information to the carrier for that purpose.[593] For instance, a number of commenters objected to our inclusion of IP addresses as forms of customer PI, because they are necessary to route customers' communications, or otherwise provide telecommunications service.[594] This concern is misplaced; while a BIAS provider needs to share its customer's IP address to provide the broadband service, there is no basis to share that information for other non-exempt purposes absent customer consent. Indeed, because of the explicit limitation described by Section 222(c)(1)(A) and implemented here, we do not need to exclude IP addresses or other forms of information from the scope of customer PI in order to allow the provision of telecommunications service, or services necessary to or used in providing telecommunications service. Thus, we import these statutory mandates into our rules and apply them to all customer PI.

204. We continue to find, as did previous Commissions, that telecommunications customers expect their carriers to market them improved service offerings within the scope of service to which they already subscribe, and as such, conclude that such limited first-party marketing is part of the provision of the telecommunications service within the meaning of Section 222(c)(1)(A).[595] As with earlier CPNI orders, we decline to enumerate a definitive list of "services necessary to, or used in, the provision of . . . telecommunications service" within the meaning of Section 222(c)(1).[596] However, we provide guidance

(Continued from previous page)
vulnerabilities.' Further, the language should only permit the sharing of information for cybersecurity attacks or risk of vulnerabilities only to the extent it does not risk user privacy or security.").

[590] 18 U.S.C. § 2510-2522 (ECPA); 47 U.S.C. § 1001 et seq. (CALEA); 47 U.S.C. § 605 (Section 705); 6 U.S.C. § 1503(c)(1) (CISA).

[591] *See* 47 U.S.C. § 222(c)(1).

[592] We note that the need for providers to transmit and disclose certain types of customer PI (including IP addresses and the contents of communications) in the course of providing service in no way obviates customers' privacy interests in this information.

[593] *See 2015 Open Internet Order*, 30 FCC Rcd at 5748, para. 339 ("[A] broadband Internet access service provider's representation to its end-user customer that it will transport and deliver traffic to and from all or substantially all Internet endpoints necessarily includes the promise to transmit traffic to and from those Internet end points back to the user.").

[594] *See* Cincinnati Bell Comments at 6; Audience Partners Comments at 11; NCTA Comments at 74-75.

[595] *1998 CPNI Order*, 13 FCC Rcd at 8083, para. 30.

[596] *1998 CPNI Order*, 13 FCC Rcd 8061; *1999 CPNI Reconsideration Order*, 14 FCC Rcd 14409.

with respect to certain services raised in the record, and specifically find that this exception includes the provision and marketing of communications services commonly bundled together with the subscriber's telecommunications service, customer premises equipment, and services formerly known as "adjunct-to-basic services." We further find that the provision of inside wiring and technical support; reasonable network management; and research to improve and protect the network or the telecommunications either fall within this category or constitute part of the provision of telecommunications service.[597]

205. *Services that are Part of, Necessary to, or Used in the Provision of Telecommunications Service.* The Commission has historically recognized that, as a part of providing service, carriers may, without customer approval, use and share CPNI to market service offerings among the categories of service to which the customer already subscribes.[598] We therefore adopt a variation of our proposal, which mirrored the existing rule, and permit telecommunications carriers to infer approval to use and share non-sensitive customer PI to market other communications services commonly marketed with the telecommunications service to which the customer already subscribes. For example, the carrier could infer consent to market voice (whether fixed and/or mobile) and video service to a customer of its broadband Internet access service.[599] We limit this exception to the use and sharing of non-sensitive information, because we agree with a number of commenters that this type of marketing remains part of what customers expect from their telecommunications carrier when subscribing to a service.[600] For example, under our rules, a BIAS provider can offer customers new or different pricing or plans for the customers' existing subscriptions (e.g., a carrier may, without the customer's approval, use the fact that the customer regularly reaches a monthly usage cap to market a higher tier of service to the customer). This exception also allows carriers to conduct internal analyses of non-sensitive customer PI to develop and improve their products and services and to develop or improve their offerings or marketing campaigns generally, apart from using the customer PI to target specific customers.[601]

206. The Commission also has historically recognized certain functions offered by telecommunications carriers as inherently part of, or necessary to, or used in, the provision of telecommunications service. Consistent with Commission precedent, we reaffirm that services formerly known as "adjunct-to-basic," including, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller ID, call forwarding, and certain centrex features, are either part of the provision of telecommunications service or are "necessary to, or used in" the provision of that telecommunications service.[602] Similarly, the Commission has, in prior orders, recognized that the provision and marketing of certain other services as being "necessary to, or used in" the provision of service, such as call answering, voice mail or messaging, voice storage and retrieval services, fax storage and retrieval services, and

[597] The current voice rules also permit the use and sharing of CPNI without additional customer approval for certain first-party marketing purposes.

[598] 47 CFR § 64.2005(a).

[599] *See, e.g.*, NTCA Comments at 47 ("[C]ustomers generally expect that their broadband providers may use or share the customers' proprietary information with affiliates to market voice, video, or any types of communications-related services tailored to their needs and preferences"); AT&T Oct. 4, 2016 *Ex* Parte at 2-3 (noting that wireline carriers routinely offer, and consumers expect, "double- or triple-play options and other service packages that combine home broadband Internet with voice and video services."); WTA Comments at 8 (assuming that existing rules include MVPD service with fixed and mobile voice services as "communications-related" services).

[600] *See, e.g.*, Comcast Sept 22, 2016 *Ex Parte* at 2; T-Mobile Sept. 13, 2016 *Ex Parte* at 3; *but see* OTI Comments at 37-38; Public Knowledge Comments at 30-31.

[601] *See* Verizon Sept. 29, 2016 *Ex Parte*.

[602] *See 1998 CPNI Order*, 13 FCC Rcd at 8097-98, para. 48; 47 CFR § 64.2005(c)(3).

protocol conversion , and we continue to do so today.[603] Likewise, we continue to find that CPE, as well as other customer devices, inside wiring installation, maintenance, and repair, as well as technical support, serve as illustrative examples of services that are either part of the telecommunications service or are "necessary to, or used in" the provision of the underlying telecommunications service for the purposes of these rules.[604] Customers require working inside wiring to receive service, and often depend upon technical support to fully utilize their services.[605] As such, carriers may use and share non-sensitive customer PI, without additional customer approval, to provide and market such services.[606]

207. In importing these historical findings into the rules we adopt today and applying them to the current telecommunications environment, we make clear that our rules no longer permit CMRS providers to use or share customer PI to market all information services without customer approval.[607] In first making these findings, the Commission noted the potential to revisit this decision if it became apparent that customer expectations, and the public interest, changed.[608] The *1999 CPNI Reconsideration Order* interpreted Section 222(c)(1) as permitting CMRS providers to market information services in general to their customers without customer approval, but limited the information services for which wireline carriers could infer approval.[609] That decision was made when the mobile information services market was in its infancy. As the third party mobile application market has developed, we can no longer find that such an exception is consistent with giving consumers meaningful choice over the use and sharing of their information. Moreover, we have a strong interest in our rules being technologically neutral.

208. *Reasonable Network Management.* We agree with commenters asserting that BIAS providers need to use customer PI to engage in reasonable network management.[610] We have previously explained that a network practice is "reasonable if it primarily used for and tailored to achieving a legitimate network management purpose, taking into account the particular network architecture and technology of the broadband service."[611] We recognize that reasonable network management plays an

---

[603] *1999 CPNI Reconsideration Order*, 14 FCC Rcd at 14434, para. 45; 47 CFR § 64.2005(b)(1). Such adjunct-to-basic functions fall within the telecommunications systems management exception to the definition of "information services" in the Act. *See* 47 U.S.C. § 153(24) ("the term 'information service' . . . does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service"); *2015 Open Internet Order*, 30 FCC Rcd at 5766, para. 367 n.1029. In the *2015 Open Internet Order*, we concluded that DNS, caching, and network-oriented, security-related blocking functions including parental controls and firewalls fall within the telecommunications systems management exception and are akin to adjunct-to-basic services. *See 2015 Open Internet Order*, 30 FCC Rcd at 5766-72, paras. 367-73.

[604] In each case here and below, whether the particular function is a part of the telecommunications service or a separate service "necessary to, or used in" the telecommunications service may depend on the particular circumstances of the underlying telecommunications service and the customer, and we need not address this distinction to determine that the statutory limitation applies.

[605] *See* NTCA Comments at 45-47; WTA Comments at 10; Letter from Loretta Polk, Vice President & Associate General Counsel, NCTA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Oct. 14, 2016) (NCTA Oct. 14, 2016 *Ex Parte*); WTA Reply at 11.

[606] *See, e.g.*, ACA Oct. 18, 2016 *Ex Parte* at 4.

[607] *1999 CPNI Reconsideration Order*, 14 FCC Rcd at 14433, para. 43.

[608] *1998 CPNI Order*, 13 FCC Rcd at 8080, n.98; 14 FCC Rcd at 14434-35, n.132.

[609] *1999 CPNI Reconsideration Order*, 14 FCC Rcd at 14433-34, paras. 44-46.

[610] *See* Sandvine Comments at 17; Cincinnati Bell Comments at 9; ACA Comments at 40; WTA Comments at 23-24; Lehr et al. Comments at 3; Feamster ISP Data Use Comments at 7-8.

[611] *2015 Open Internet Order*, 30 FCC Rcd at 5700, para. 215; 47 CFR § 8.2(f). As we further elaborated in the *2015 Open Internet Order*, reasonable network management includes, but is not limited to network management practices that are primarily used for, and tailored to, ensuring network security and integrity, including by addressing (continued….)

important role in providing BIAS, and consider reasonable network management to be part of the telecommunications service or "necessary to, or used in" the provision of the telecommunications service.[612] As such, we clarify that BIAS providers may infer customer approval to use, disclose, and permit access to customer PI to the extent necessary for reasonable network management, as we defined that term in the *2015 Open Internet Order*.

209. *Research to Improve and Protect Networks or Telecommunications.* We also find that certain uses and disclosures of customer PI for the purpose of conducting research to improve and protect[613] networks or telecommunications are part of the telecommunications service or "necessary to, or used in" the provision of the telecommunications service for the purposes of these rules.[614] For instance, Professor Feamster explains that "network research fundamentally depends on cooperative data sharing agreements with ISPs," and that, lack of access to certain types of customer PI, "will severely limit vendors' and developers' ability to build and deploy network technology that functions correctly, safely, and securely."[615] Comcast also emphasizes the need to share customer PI with "trusted vendors, researchers, and academics . . . under strict confidentiality agreements . . . to improve both the integrity and reliability of the service."[616] NCTA also argues that carriers must be able to use customer data for internal operational purposes such as improving network performance.[617] Some commenters, such as CDT, caution that a research exemption, read too broadly, might permit privacy violations.[618] We share these concerns, and emphasize that in the interest of protecting the confidentiality of customer PI, carriers should seek to minimize privacy risks that may stem from using and disclosing customer PI for the purpose of research, and should ensure that the entities to which they disclose customer PI will likewise safeguard customer privacy.[619] Telecommunications carriers and researchers should design research projects that incorporate principles of privacy-by-design,[620] and agree not to publish or otherwise publicly

(Continued from previous page)
traffic that is harmful to the network; network management practices that are primarily used for, and tailored to, addressing traffic that is unwanted by end users; and network practices that alleviate congestion without regard to the source, destination, content, application, or service. *2015 Open Internet Order*, 30 FCC Rcd at 5701-02, para. 220.

[612] *See* NCTA Oct. 14, 2016 *Ex Parte* at 1 (expressing the need for carriers to use customer PI for internal purposes such as improving network performance, quality of service, and customer satisfaction).

[613] Since telecommunications carriers must be able to provide secure networks to their customers, we include security research within the scope of research allowed under this limitation. Security research also falls under the exception covered in Part III.D.2.b, *infra*, regarding uses of customer PI to protect the rights and property of a carrier, or to protect users from fraud, abuse, or unlawful use of the networks.

[614] *See, e.g.*, Antonakakis et al. Comments.

[615] Feamster ISP Data Use Comments at 7-8.

[616] Comcast Comments at 60; *see also* Letter from Nick Feamster et al., to Tom Wheeler, Chairman, FCC, WC Docket No. 16-106 (filed Aug. 6, 2016) (Security Researchers Aug. 6, 2016 *Ex Parte*); Future of Privacy Forum Comments at 12; Feamster ISP Data Use Comments at 3-4, 7-8; Lehr et al. Comments at 2-3, 8; NCTA Comments at 76-77; Nominum Comments at 5-6.

[617] NCTA Oct. 14, 2016 *Ex Parte* at 1.

[618] *See, e.g.*, CDT Reply at 12 ("For example, marketing and social science research are very much attenuated from the direct interests of BIAS customers, and allowing those forms of research may lead to abuses of purported research data that subvert the intent of the NPRM to protect consumer privacy from such uses in the first place.").

[619] Security Researchers Aug. 6, 2016 *Ex Parte*; M3AAWG Comments at 5 (explaining that "researchers attempt to use anonymous data to identify signs of a security problem, either on the host ISP network or pointing at signs on another network"); CDT Reply at 12 (stating that "the FCC must develop generic protections that bind security researchers as a condition of receiving BIAS data").

[620] This would include, for instance, practicing data minimization and not using more identifiable information than necessary for the research task.

share individually identifiable data without customer consent. In addition, the existing rules permit CMRS providers to infer customer approval to use and share CPNI for the purpose of conducting research on the health effects of CMRS.[621] We retain this limited provision, extending it to all customer PI. We reiterate that that carriers should endeavor to minimize privacy risks to customers.

**b. Specific Exceptions**

210. In addition to the activities included in the provision of service and services necessary to, or used in, provision of service, carriers do not need to seek customer approval to engage in certain specific activities that represent important policy goals detailed in Section 222(d). We apply those exceptions to the customer approval framework to all customer PI.

211. *Initiate, Render, Bill, and Collect for Service*. We import into our rules and apply to all customer PI the statutory exception permitting carriers to use, disclose, and permit access to CPNI "to initiate, render, bill, and collect for telecommunications services" without obtaining additional customer consent. As the Rural Wireless Association explains, carriers frequently need to share "certain customer information" "with billing system vendors, workforce management system vendors, consultants that assist with certain projects, help desk providers, and system monitoring solutions providers."[622]

212. *Protection of Rights and Property.* We also import into our rules and apply to all customer PI the statutory provision permitting carriers to use, disclose, and permit access to CPNI "to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services" without obtaining specific customer approval.[623] We agree with the broad set of commenters who expressed the opinion that this exception should be incorporated into the rules,[624] and further agree that it should also apply to customer PI beyond CPNI.[625] We also find that these rules comport with the Cybersecurity Information Sharing Act of 2015 (CISA), which permits certain sharing of cyber threat indicators between telecommunications providers and the federal government or private entities, "notwithstanding any other provision of law."[626]

---

[621] 47 CFR § 64.2005(c)(2); *see also* 47 CFR § 20.3 (defining "commercial mobile radio service" as including mobile broadband Internet access service").

[622] Rural Wireless Association Comments at 4; *see also* American Association of Law Libraries Comments at 3; Consumer Action Comments at 2 (recognizing that "when one does business with an internet service provider, it needs to share limited information about customers with certain other companies to provide service and prepare billing statements"); CCA Oct. 13, 2016 *Ex Parte* at 5 (explaining need for carriers to share information with third parties acting on behalf of the carrier); NTCA Oct. 14, 2016 *Ex Parte* at 2 (recognizing need to share information with third parties or affiliates for billing and similar purposes). Also, as noted below, to the extent that the carrier is using an agent to perform acts on its behalf, the carrier's agents, acting in the scope of their employment, stand in the place of the carrier, both in terms of rights and liabilities. *See infra* note 637.

[623] *See* 47 U.S.C. § 222(d)(2) (stating that Section 222 does not prohibit a telecommunications carrier from using, disclosing, or permitting access to CPNI obtained from its customers, either directly or indirectly through its agents "to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services").

[624] *See, e.g.*, M3AAWG Comments at 2; Nominum Comments at 4; Charter Reply at 27-30; NCTA Comments at 76; NCTA Reply at 50-52; CTIA Reply at 83-85; Lehr et al. Comments at 7-9; Letter from Christopher L. Shipley, INCOMPAS, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 3-4 (filed Aug. 4, 2016) (INCOMPAS Aug. 4, 2016 *Ex Parte*).

[625] *See, e.g.*, CTIA Comments at 138-39; Email Sender & Provider Coalition Comments at 6-7; NTCA Comments at 46-47 ("NTCA supports the ability of BIAS to use 'customer proprietary information' . . . to protect users or others from cyber security threats or vulnerabilities . . . ."); *see also* Comcast Comments at 59.

[626] 6 U.S.C. § 1503(c)(1). We do not assume that the scope of our exception is coterminous with the definition of cyber threat information in CISA. As noted, however, to the extent information is allowed to be shared pursuant to CISA, our rules do not inhibit such sharing.

Moreover, to the extent that other federal laws, such as CISA, permit or require use or sharing of customer PI, our rules expressly do not prohibit such use or sharing.

213. We also agree with commenters that this provision of our rules encompasses the use and sharing of customer PI[627] to protect against spam, malware such as viruses, and other harmful traffic,[628] including fraudulent, abusive, or otherwise unlawful robocalls.[629] We caution that carriers using or sharing customer PI pursuant to this section of the rules should remain vigilant about limiting such use and sharing to the purposes of protecting their networks and users, and complying with their data security requirements.[630] We acknowledge Access Now's concern that an overbroad reading of this exception could result in carriers actively and routinely monitoring and reporting on customers' behavior and traffic,[631] and make clear that the rule does not allow carriers to share their customers' information wholesale on the possibility that doing so would enhance security; use and sharing of customer PI for these purposes must be reasonably tailored to protecting the network and its users.

214. We agree with commenters that recommend that we consider this provision of our rules to encompass not only actions taken to combat immediate security threats, but also uses and sharing to research and develop network and cybersecurity defenses.[632] When combined with the immunity granted by CISA, this exception addresses carriers' concerns about participating in cybersecurity sharing initiatives.[633] Security is an essential part of preventing bad actors from gaining unauthorized access to the system or making abusive use of it with spam, malware, or denial of service attacks. Research and development into new techniques and technologies for addressing fraud and abuse may require internal use of customer PI, but also disclosures to third-party researchers and other collaborators. However, as with other applications of this exception, carriers should not disclose more information than is reasonable to achieve this purpose, and should take reasonable steps to ensure that the parties with which they share information use this information only for the purposes for which it was disclosed.[634]

---

[627] As proposed, this includes any form of customer PI, not merely calling party phone numbers. *See* FTC Staff Comments at 18-19; USTelecom Comments at 16; West Telecomm. Serv. Reply at 4-5.

[628] Email Sender & Provider Coalition Comments at 6-7; Antonakakis et al. Comments at 3; Comcast Comments at 59.

[629] *See, e.g.,* West Telecomm. Serv. Reply Comments at 3-5; FTC Staff Comments at 18; USTelecom Comments at 16-18; *see also* NTCA Comments at 46-47 ("NTCA supports the ability of BIAS to use 'customer proprietary information' . . . to address such issues as 'spoofing' and unlawful 'robocalls.').

[630] USTelecom Comments at 17 ("CPNI sharing in such circumstances is limited to just what is needed to investigate the source of the call such as the calling party telephone number, the called party telephone number, and the date and time of the call.").

[631] Access Now Comments at 8-9; *see also* CDT Reply at 12 (explaining need for protections on disclosure for security purposes); EFF Comments at 9 (advocating for limits on disclosures for security purposes).

[632] Feamster ISP Data Use Comments; Antonakakis et al. Comments at 2, 4, 6-8; Comcast Comments at 60; CDT Reply at 10-11.

[633] As noted above, CISA permits the sharing of cybersecurity threat indicators "notwithstanding any other provision of law." 6 U.S.C. § 1503(c)(1). These provisions should also alleviate the concern expressed in the interim update on information sharing from the Communications Security, Reliability, and Interoperability Council (CSRIC), that our rules may conflict with CISA. CSRIC Working Group 5, Information Sharing Barriers at 7-8 (June 2016), https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG5_Info_Sharing_Report_062016.pdf.

[634] *See, e.g.*, Security Researchers Aug. 6, 2016 *Ex Parte*. Feamster et al. suggest that security research receive a specific exemption, so long as security disclosures be limited to those that: promote security, stability, and reliability of networks; do not violate privacy; and benefit research in a way that outweighs privacy risks. They also highlight particular categories of researchers to whom disclosure represents less privacy risk. While we decline to include this specific exemption and its criteria, we note that similar steps to mitigate privacy risks and determine trustworthy recipients can be useful factors in determining reasonableness.

215. *Providing Inbound Services to Customers*. Customers expect that a carrier will use their customer PI when they initiate contact with the carrier in order to ask for support, referral, or new services in a real-time context. Therefore, within the limited context of the particular interaction, carriers can use customer PI to render the services that the customer requests without receiving additional approval from the customer. This provision represents a more generalized version of the exception in Section 222(d)(3), which specifies that carriers may use customer PI "for the duration of [a support, referral, or request for new services] call." Under the rule we adopt today, carriers may use customer PI for the duration of any real-time interaction, including voice calls, videoconferencing, and online chats. However, given the less formal nature of such requests, a carrier's authorization to use the customer PI without additional permission should only last as long as that particular interaction does, and not persist longer. We find that this provision will achieve the same purpose as existing Section 64.2008(f) of our rules, which allows carriers to waive certain notice requirements for one-time usage of customer PI. We believe that carriers' ability to use customer PI for these purposes without additional customer permission obviates the need for streamlined notice and consent requirements in one-time interactions.

216. Some commenters have argued that our rules should permit a carrier to share customer PI with its agents absent customer approval, noting the need to share customer PI with agents to provide customer support, billing, or other tasks.[635] We agree that such sharing is often necessary, and the limitations and exceptions outlined above allow carriers to share customer PI with their agents without additional customer approval. To the extent that a carrier needs to share customer PI with an agent for a non-exempt task, it needs no more customer approval than it would have needed in order to perform that task itself.[636] This is consonant with the Communications Act's requirement that carriers' agents, acting in the scope of their employment, stand in the place of the carrier, both in terms of rights and liabilities.[637]

217. *Providing Certain Customer PI in Emergency Situations*. In adopting Section 222, Congress recognized the important public safety interests in ensuring that carriers can use and share necessary customer information in emergency situations. Section 222(d)(4) specifically allows carriers to provide call location information of commercial mobile service users to: (1) certain specified emergency services, in response to a user's call for emergency services; (2) a user's legal guardian or immediate family member, in an emergency situation that involves the risk of death or serious physical harm; and (3) to providers of information or database management services solely for the purpose of assisting in the delivery of emergency services in the case of an emergency. We adopt rules mirroring these exceptions, and expand the scope of information that may be disclosed under these circumstances to include customer location information and non-sensitive customer PI.

218. While commercial mobile service users' location may be the information most immediately relevant to emergency services personnel, other forms of customer PI may also be relevant for customers using services other than commercial mobile services, especially if customers are seeking

[635] *See, e.g.*, CCA Comments at 25 (expressing concern that "the proposal to potentially limit sharing of a vast amount of information with affiliates that provide communications-related services would be concerning for competitive wireless carriers with corporate structuring that tends to include vendors and affiliates for the everyday provision of mobile broadband services"); CTIA Comments at 129-130 (arguing that "sharing a customer's name with an ISP's longstanding agent (for which the ISP has assumed liability) presents a diminished privacy risk relative to an ISP's selling a customer's web browsing activity to an anonymous data broker"); Letter from Aaron N. Goldberger, Associate General Counsel, Neustar, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 (filed Sept. 9, 2016); Verizon Reply at 14-15 (arguing that the rules should not contain special restrictions for sharing with affiliates and contractors); Level 3 Comments at 12-13; AT&T Reply at 9, 34-35.

[636] *See supra* Part III.D.1.

[637] 47 U.S.C. § 217 ("In construing and enforcing the provisions of this chapter, the act, omission, or failure of any officer, agent, or other person acting for or employed by any common carrier or user, acting within the scope of his employment, shall in every case be also deemed to be the act, omission, or failure of such carrier or user as well as that of the person.").

emergency assistance through means other than dialing 9-1-1 on a voice line.[638] Expanding the types of information available in an emergency to include non-sensitive information such as other known contact information for the customer or the customer's family or legal guardian will allow carriers the flexibility necessary to keep emergency services informed with actionable information. However, recognizing the concerns that too broad an exception could lead to increased exposure of sensitive information,[639] we extend the exception only to customer location information and non-sensitive customer PI.

219. We recognize that, as with any provision that allows disclosure of a customer's information, this exception can potentially be abused. Various bad actors may use pretexting techniques, pretending to be a guardian, immediate family member, emergency responder, or other authorized entity to gain access to customer PI.[640] As with all of the other provisions of these rules, we expect carriers to abide by the security standards set forth in Part III.E, below. Under these standards, we expect that carriers will reasonably authenticate third parties to whom they intend to disclose or permit access to customer PI. This need to act reasonably also applies to authenticating emergency services and other entities covered under this exception, as well as authenticating customers themselves.

220. We decline suggestions that we allow carriers only to divulge customer PI in emergency situations to emergency contact numbers specified by the customer in advance.[641] While such a safeguard could prevent a certain amount of pretexting, we believe that such a requirement would be overly restrictive and, in the case of call information, contrary to the statute. If such a requirement were in place, customers who failed to supply or update emergency contact information would be denied the ability for guardians or family members from being contacted. Recognizing the permissible nature of Section 222(d), we do not prohibit carriers from using such a safeguard if they so choose.

### 3. Requirements for Soliciting Customer Opt-Out and Opt-In Approval

221. In this section, we discuss the requirements for soliciting customer approval for the use and sharing of customer PI. First, we require telecommunications carriers to solicit customer approval at the point of sale, and permit further solicitations after the point of sale. Next, we require that carriers actively contact their customers in these subsequent solicitations, to ensure that customers are adequately informed. Finally, we require the solicitations to be clear and conspicuous, to be comprehensible and not misleading, and to contain the information necessary for a customer to make an informed choice regarding her privacy.

222. *Timing of Solicitation.* Based on the record before us, we conclude that BIAS providers and other telecommunications carriers must solicit customers' privacy choices at the point of sale. We agree with the FTC and other commenters that the point of sale remains a logical time for customers to exercise privacy decisions because it precedes the carriers' uses of customer PI; frequently allows for clarification of terms between customer and carrier; and avoids the need for customers to make privacy decisions when distracted by other considerations, and is the time when customers are making decisions about material terms.[642]

223. We further find that, in addition to soliciting choice at point-of-sale, a carrier seeking customer approval to use customer PI may also solicit that permission at any time after the point after the sale, so long as the solicitation provides customers with adequate information as specified in these rules.

---

[638] Texas 9-1-1 Entities Comments at 2 (noting the need for customer PI that may be associated with alternative emergency calls, including "data, video, text, and other non-legacy voice services").

[639] *See, e.g.*, Access Now Comments at 8; EFF Comments at 9.

[640] FTC Staff Comments at 16-17.

[641] *But see* FTC Staff Comments at 17.

[642] CDD Comments at 20; FTC Staff Comments at 24-25; Hughes Comments at 4-5; Hughes Oct. 14, 2016 *Ex Parte* at 2.

This allows carriers to supply customers with relevant information at the most relevant time and in the most relevant context.[643] Moreover, a carrier that makes material changes to its privacy policy must solicit customers' privacy choices before implementing those changes. Material retroactive changes require opt-in customer approval as discussed above in Part III.D.1.a(ii). Consistent with our sensitivity-based framework, prospective material changes require opt-in approval if they entail use or sharing of sensitive customer PI, and opt-out approval if they entail use or sharing of non-sensitive customer PI.

224. *Methods of Solicitation.* We agree with commenters who recommend that we not require particular formats or methods by which a carrier must communicate its solicitation of consent to customers. On this point, we agree with NTCA and USTelecom, which request flexibility in determining the means of solicitation, arguing that carriers are best placed to determine the most effective ways of reaching their customers.[644]

225. The existing voice rules contain specific requirements for solicitations sent as email, such as a requirement that the subject line clearly and accurately identify the subject matter of the email.[645] We decline to include such specific requirements and thereby provide carriers with additional flexibility to develop clear notices that best serve their customers. However, the clarity and accuracy of an email subject line are highly relevant to an overall assessment of whether the solicitation as a whole was clear, conspicuous, comprehensible and not misleading.

226. *Contents of Solicitation.* Carriers' solicitations of opt-in or opt-out consent to use or share customer PI must clearly and conspicuously inform customers of the types of customer PI that the carrier is seeking to use, disclose, or permit access to; how those types of customer PI will be used or shared; and the categories of entities with which that information is shared. The solicitations must also be comprehensible and not misleading, and be translated into a language other than English if the telecommunications carrier transacts business with the customer in that language. As with our notice requirements, we decline to specify a particular format or wording for this solicitation, so long as the solicitation meets the standards described above. The solicitation must provide a means to easily access the carrier's privacy policy as well as a means to easily access to a mechanism, described below in Part III.D.4, by which the customer can easily exercise his choice to permit or deny the use or sharing of his customer PI. Access to the choice mechanism may take a variety of forms, including being built into the solicitation, or provided as a link to the carrier's website, an email address that will receive the customer's choice, or a toll-free number that a customer can call to make his choice.[646]

227. As a point of clarification, the distinction between notice and consent solicitation is one of functionality, not necessarily of form. Choice solicitations may be combined with notices of privacy policies or notices of material change in privacy policies, but only to the extent that both the notices and solicitations meet their respective requirements for being clear and conspicuous, comprehensible, and not misleading. For instance, a carrier instituting a new program that uses non-sensitive customer PI prospectively could send an existing customer a notice of material change to the privacy policy that contained the opt-out solicitation (described in this Part) and access to the customer's choice mechanism

[643] *See* ACA comments at 52-53 (arguing that providers can best determine the timing of solicitations most relevant to the context of the interaction); CTIA Comments at 143-44; NTCA Comments at 53-54.

[644] *See, e.g.*, NTCA Comments at 54 ("NTCA supports proposals that each BIAS provider be permitted to determine the best method for soliciting customer approval."); USTelecom Comments at 12-13 ("[T]he Commission should . . . allow carriers the flexibility to determine the appropriate methods for notifying its customers and to maintain records of choice selections in ways that make sense in the context of the specific provider-customer relationship.").

[645] 47 CFR § 64.2008(d)(3)(iv).

[646] *See, e.g.*, NTCA Comments at 55 ("NTCA supports the proposition that providers may offer customers access to privacy policies and an ability to effectuate related choices through a variety of means, including via telephone or on-line interactions. Providers should have latitude to determine the most effective course of providing notice to their customers through those methods."); USTelecom Comments at 12-13.

(described in Part III.D.4, *infra*). This communication would, subject to the ease-of-use requirements, satisfy the rules. We further clarify that we are not requiring carriers to have special "customer PI" choice mechanisms that are different and stand alone from other mechanisms that may exist, so long as those mechanisms satisfy the outcomes required by our rules (such as, among other things, that they be clear and conspicuous). Likewise, we are not mandating a "blanket" choice mechanism. A carrier is free to give the customer the ability to pick and choose among which marketing channels the customer will opt out of. At the same time, if a carrier wanted to give the customer the ability to opt out of all marketing with a single click, that would be consistent with our rules.[647]

#### 4. Customers' Mechanisms for Exercising Privacy Choices

228. In soliciting a customer's approval for the use or sharing of his or her customer PI, we require carriers to provide customers with access to a choice mechanism that is simple, easy-to-use clear and conspicuous, in language that is comprehensible and not misleading, and made available at no additional cost to the customer. This choice mechanism must be persistently available on or via the carrier's website; on the carrier's app, if it provides one for account management purposes; and on any functional equivalents of either.[648] If a carrier lacks a website, it must provide a persistently available mechanism by another means such as a toll-free telephone number. However, we decline to specify any particular form or format for this choice mechanism. Carriers must act upon customers' privacy choices promptly.

229. *Format.* As with our requirements for notices and for solicitations of approval, the actual mechanism provided by the carrier by which customers may inform the carrier of their privacy choices must be clear and conspicuous, and in language that is comprehensible and not misleading. Because users' transaction costs, in terms of time and effort expended, can present a major barrier to customers exercising choices, carriers' choice mechanisms must also be easy to use, ensuring that customers can readily exercise their privacy rights.

230. We encourage but do not require carriers to make available a customer-facing dashboard. While a customer-facing dashboard carries a number of advantages, we are mindful of the fact that it may not be feasible for certain carriers, particularly small businesses, and that improved technologies and user interfaces may lead to better options.[649] Preserving this flexibility benefits both carriers and customers by enabling carriers to adopt a mechanism that suits the customer's abilities and preferences and the carrier's technological capabilities. As noted, we are particularly mindful of the needs of smaller carriers. For example, WTA explains that "[a] privacy dashboard as envisioned in the NPRM would require providers to aggregate information that is likely housed today on multiple systems and develop both internal and external user interfaces."[650] ACA adds that creating a privacy dashboard would be a "near-impossible task" for small BIAS providers.[651] Particularly in light of the concerns expressed by small providers and their representatives, we decline to mandate that BIAS providers make available a customer-facing dashboard.

231. *Timing to Implement Choice.* We require carriers to give effect to a customer's grant, denial, or withdrawal of approval "promptly."[652] Aside from the ordinary time that might be required for

[647] NCTA Oct. 20, 2016 *Ex Parte* at 8.

[648] We intend for this requirement to mirror the requirements for a provider's provision of its notice of privacy policies.

[649] *See, e.g.*, Hughes Comments at 5-6; Sprint Comments at 13-14; CTIA Comments at 104-05; NTCA Comments at 41-42; Rural Wireless Association Comments at 7; WTA Comments at 11-12.

[650] WTA Reply at 9-10.

[651] ACA Comments at 38-39.

[652] *See, e.g.*, Hughes Oct. 14, 2016 *Ex Parte* at 2 (arguing that providers should be required to "update consumers' decisions regarding privacy preferences when they are affirmatively communicated to the provider").

processing incoming requests, customers must be confident that their choices are being respected. The flexibility of this standard enables carriers to account for the relative size of the carrier, the type and amount of customer PI being used, and the particular use or sharing of the customer PI.[653] Since the carrier process and technical mechanics of implementing a customer denial of approval for a new use may well differ from implementing a customer's denial of a previously approved practice, we do not expect that the time frames for each will necessarily be the same.[654] The Commission has long held this interpretation to be consistent with the language and design of Section 222.[655]

232. *Choice Persistence.* As in our existing rules and as proposed in the *NPRM*, we require a customer's choice to grant or deny approval for use of her customer PI to remain in effect until a customer revokes or limits her choice.[656] We find that customers reasonably expect that their choices will persist and not be changed without their affirmative consent (in the case of sensitive customer PI and previously collected non-sensitive customer PI) or at least the opportunity to object (in the case of yet to be collected non-sensitive customer PI).

233. *Small Carriers.* Some small carriers expressed concern on the record that their websites do not allow for customers to manage their accounts, and thus could not offer an in-browser way for customers to immediately exercise their privacy choices on the carriers' websites.[657] Since we decline to require a specific format for accepting customer privacy choices, any carriers, including small carriers, that lack choice mechanisms that customers can operate directly from the carrier's website or app may be able to accept customer preferences by providing on their websites, in their apps, and any functional equivalents, an email address, 24-hour toll-free phone number, or other easily accessible, persistently available means to exercise their privacy choices.

### 5. Eliminating Periodic Compliance Documentation

234. We eliminate the specific compliance recordkeeping and annual certification requirements in Section 64.2009 for voice providers. Eliminating these requirements reduces burdens for all carriers, and particularly small carriers, which often may not need to record approval if they do not use or share customer PI for purposes other than the provision of service.[658] We find that carriers are likely to keep records necessary to allow for any necessary enforcement without the need for specific requirements, and that notifications of data breaches to customers and to enforcement agencies (including the Commission) will ensure compliance with the rules and a workable level of transparency for customers.

---

[653] NTCA Comments at 38 (requesting that the rules account for context).

[654] *See, e.g.*, Letter from Jennifer Manner, Senior Vice President, Regulatory Affairs, Hughes Network Systems, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, Attach. at 1 (filed July 26, 2016) (requesting 10-day timeframe "to implement a consumer's request to opt-in or opt-out of permitted uses of their customer PI."); Hughes Oct. 14, 2016 *Ex Parte* Attach. at 1 (same).

[655] *See 1998 CPNI Order*, 13 FCC Rcd at 8151, para. 116 (explaining that "the language of Section 222(d)(3) stating that carriers may 'provide inbound telemarketing, referral, or administrative services to the customer *for the duration of the call*' suggests that Congress expressly limited the duration of approval where it wanted to so specify, and thus the absence of similar language in Section 222(c)(1) evidences that Congress did not limit as a statutory matter the time period within which customer approval remains valid").

[656] 47 CFR § 64.2007(a)(2); *Broadband Privacy NPRM*, 31 FCC Rcd at 2552, para. 147.

[657] *See, e.g.*, Letter from Patricia Cave, Director, Government Affairs, WTA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2-3, n.4 (filed Aug. 22, 2016) (WTA Aug. 22, 2016 *Ex Parte*).

[658] *See infra* note 690.

### E. Reasonable Data Security

235. In this section, we adopt a harmonized approach to data security that protects consumers' confidential information by requiring BIAS providers and other telecommunications carriers to take reasonable measures to secure customer PI. The record reflects broad agreement with our starting proposition that strong data security practices are crucial to protecting the confidentiality of customer PI.[659] There is also widespread agreement among industry members, consumer groups, academics, and government entities about the importance of flexible and forward-looking reasonable data security practices.[660]

236. In the *NPRM* we proposed rules that included an overarching data security expectation and specified particular types of practices that providers would need to implement to comply with that standard, while allowing providers flexibility in implementing the proposed requirements (e.g., taking into account, at a minimum, the nature and scope of the provider's activities and the sensitivity of the customer PI held by the provider). Based on the record in this proceeding, we have modified the overarching data security standard to more directly focus on the reasonableness of the providers' data security practices. Also based on the record, we decline to mandate specific activities that providers must undertake in order to meet the reasonable data security requirement. We do, however, offer guidance on the types of data security practices we recommend providers strongly consider as they seek to comply with our data security requirement—recognizing, of course, that what constitutes "reasonable" data security is an evolving concept.

237. The approach we take today underscores the importance of ensuring that providers have robust but flexible data security practices that evolve over time as technology and best practices continue to improve. It is consistent with the FTC's body of work on data security,[661] the NIST Cybersecurity Framework (NIST CSF),[662] the Satellite and Cable Privacy Acts,[663] and the CPBR,[664] and finds broad support in the record.[665] In harmonizing the rules for BIAS providers and other telecommunications carriers we apply this more flexible and future-focused standard to voice providers as well, replacing the

[659] *Broadband Privacy NPRM*, 31 FCC Rcd at 2557, para. 167; *see also* Access Now Comments at 11-12 ("[T]he ultimate policy cannot create flexibility to excuse companies or actions from failing to provide adequate protections."); National Consumers League Comments at 2 (encouraging adoption of "high baseline data security protections"); American Association of Law Libraries Comments at 4; Greenlining Institute Comments at 45-48; Consumer Action Comments at 2; Access Humboldt et al. Comments at 5.

[660] *See, e.g.*, CenturyLink Comments at 32; Comcast Reply at 26; DMA Comments at 24; National Consumers League Comments at 9; New York Attorney General Reply at 3; $S^2$ERC Center Comments at 3; Jon Leibowitz Comments at 10-11; FTC Staff Comments at 27-28; Letter From Chris Calabrese, VP of Policy, Center for Democracy & Technology, to Marlene Dortch, Secretary, FCC, at 4 (filed Sept. 29, 2016) (CDT Sept. 29, 2016 *Ex Parte*).

[661] *See* FTC Staff Comments at 27-28 (outlining the FTC's "technology-neutral, process-based approach to security [it has applied] for two decades"); FTC, Data Security, https://www.ftc.gov/datasecurity ("[A] company's data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities.").

[662] *See infra* note 682.

[663] *See* 47 U.S.C. §§ 551(c)(1), 338(i)(4) (directing cable operators and satellite carriers, respectively, to "take such actions as are necessary to prevent unauthorized access to [subscriber information]"); *see also Cox Consent Decree*, 30 FCC Rcd at 12302, para. 3 ("Congress and the Commission have made clear that cable operators such as Cox must 'take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator.'").

[664] *See infra* note 681.

[665] *See, e.g.*, NTCA Comments at 59-60; CTIA Comments at 156-58.

more rigid data security procedures codified in the existing rules and thus addressing the potential that these existing procedures are both under- and over-inclusive—with the expectation that strong and flexible, harmonized, forward-looking rules will benefit consumers and industry.

### 1. BIAS and Other Telecommunications Providers Must Take Reasonable Measures to Secure Customer PI

238. The rule that we adopt today requires that every BIAS provider and other telecommunications carrier take reasonable measures to protect customer PI from unauthorized use, disclosure, or access. To comply with this requirement, a provider must adopt security practices appropriately calibrated to the nature and scope of its activities, the sensitivity of the underlying data, the size of the provider, and technical feasibility.[666]

239. As we observed in the *NPRM*, privacy and security are inextricably linked.[667] Section 222(a) imposes a duty on telecommunications carriers to "protect the confidentiality of proprietary information of and relating to . . . customers."[668] Fulfilling this duty requires a provider to have sound data security practices.[669] A telecommunications provider that fails to secure customer PI cannot protect its customers from identity theft or other serious personal harm, nor can it assure its customers that their choices regarding use and disclosure of their personal information will be honored. As commenters point out, contemporary data security practices are generally oriented toward "confidentiality, integrity, and availability,"[670] three dynamic and interrelated principles typically referred to together as the "CIA" triad.[671] Confidentiality refers specifically in this context to protecting data from unauthorized access and disclosure;[672] integrity refers to protecting information from unauthorized modification or destruction;[673] and availability refers to providing authorized users with access to the information when needed.[674] We

[666] *See infra* Appx A.

[667] *See generally Broadband Privacy NPRM*, 31 FCC Rcd at 2557, para. 167 ("Strong data security protections are crucial to protecting the confidentiality of customer PI.").

[668] 47 U.S.C. § 222(a).

[669] *See TerraCom Consent Decree*, 30 FCC Rcd at 7075, para. 2 ("The failure to reasonably secure customers' proprietary information violates a carrier's duty under the Communications Act . . ."); *2007 CPNI Order*, 22 FCC Rcd at 6959, para. 64 ("We fully expect carriers to take every reasonable precaution to protect the confidentiality of proprietary or personal customer information.").

[670] *See* Paul Vixie Comments at 31 ("The textbook security objectives are normally confidentiality, integrity, and availability in the enterprise case."); International Association of Privacy Professionals Comments at 2 ("Data security is concerned with the confidentiality, integrity and availability of any information."); NTCA Comments at 58-59.

[671] *See, e.g.*, Techopedia, CIA Triad of Information Security, https://www.techopedia.com/definition/25830/cia-triad-of-information-security (last visited Oct. 5, 2016); *see also* 44 USC § 3552(b)(3) (defining "integrity," "confidentiality," and "availability" as the constituent elements of "information security"); Office of Management and Budget, Circular No. A-130, Managing Information as a Strategic Resource at 36 (2016), https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf (defining "[s]ecurity control" as "the safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information").

[672] *See* ATIS, *ATIS Telecom Glossary: Confidentiality* (Sept. 12, 2016), http://www.atis.org/glossary/definition.aspx?id=6609; *see also* 44 U.S.C. § 3552(b)(3)(B). Our discussion of "confidentiality" as part of the CIA triad of data security principles is not intended to suggest that the term has the same meaning under Section 222 of the Act as it has in the CIA context.

[673] *See* ATIS, *ATIS Telecom Glossary: Integrity* (Sept. 12, 2016), http://www.atis.org/glossary/definition.aspx?id=458; *see also* 44 U.S.C. § 3552(b)(3)(A).

[674] *See* ATIS, *ATIS Telecom Glossary: Availability* (Sept. 12, 2016), http://www.atis.org/glossary/definition.aspx?id=5637; *see also* 44 U.S.C. § 3552(b)(3)(C).

agree with NTCA that confidentiality, integrity and availability are best understood as "elements of a single duty" to secure data, and their collective purpose is to "illustrate the various considerations that must be engaged when the management of confidential information is considered."[675] The record confirms that these are core principles that underlie the modern-day practice of data security.[676] Thus, we expect providers to take these principles into account when developing, implementing, and monitoring the effectiveness of adopted measures to meet their data security obligation.

240. By requiring providers to take reasonable data security measures, we make clear that providers will not be held strictly liable for all data breaches.[677] Instead, we give providers significant flexibility and control over their data security practices while holding these practices to a standard of reasonableness that respects context and is able to evolve over time. There is ample precedent and widespread support in the record for this approach. FTC best practices guidance advises companies to "make reasonable choices" about data security,[678] and in numerous cases the FTC has taken enforcement action against companies for failure to take "reasonable and appropriate" steps to secure customer data.[679] Many states also have laws that require regulated entities to take "reasonable measures" to protect the personal data they collect.[680] The CPBR reaffirms this standard, directing companies to "establish, implement and maintain safeguards reasonably designed to ensure the security of" personal customer information.[681] Placing the responsibility on companies to develop and manage their own security practices is also a core tenet of the NIST CSF.[682] A diverse range of commenters in this proceeding support adoption of a data security requirement for BIAS providers that is consistent with these

[675] NTCA Comments at 58. Additionally, one commenter notes that increasing security may affect availability. *See* Paul Vixie Comments at 31 ("We believe availability to be fully on par with the other objectives mentioned for a utility-like service such as broadband service. A desire for security must NOT be allowed to potentially degrade availability."); *see also* International Association of Privacy Professionals Comments at 2 ("Data security is concerned with the confidentiality, integrity and availability of any information.").

[676] *See supra* note 670.

[677] *But see* FTC Staff Comments at 27-28 ("[T]he proposed rule text would impose strict liability on companies for 'ensuring' security."); CenturyLink Comments at 32-33; CTIA Comments at 159-161.

[678] *See* Federal Trade Commission, Start with Security: A Guide for Business at 1 (2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (2015 FTC Security Guide for Business).

[679] *See, e.g.*, GMR Transcription Services, Inc., Complaint, F.T.C. File No. 122-3095 (2014), https://www.ftc.gov/system/files/documents/cases/140821gmrcmpt.pdf (GMR Transcription Services Complaint); GeneLink, Inc., Complaint, F.T.C. File No. 112-3095 (2014) https://www.ftc.gov/sites/default/files/documents/cases/140107genelinkcmpt.pdf (GeneLink Complaint); Accretive Health, Inc., Complaint, F.T.C. File No. 122-3077 (2014), https://www.ftc.gov/system/files/documents/cases/140224accretivehealthcmpt.pdf; *see also FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015) (upholding FTC authority to bring data security cases under the Section 5 "unfairness" prong).

[680] *See, e.g.*, Md. Code Ann., Com. Law § 14-3503(a) (2016); Utah Code Ann. § 13-44-201 (2016); Fla. Stat. § 501.171(2) (2016); Cal. Civ. Code § 1798.81.5(b)-(c) (2016).

[681] *See* 2015 Administration CPBR Discussion Draft § 105(a)(2); *see also* 2012 White House Privacy Blueprint at appx. A ("Consumer Privacy Bill of Rights").

[682] *See* National Institute for Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity at 2 (2014) http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf (NIST CSF) ("The [NIST CSF] is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the [NIST CSF] will vary.").

principles.[683] Indeed, several providers acknowledge the importance of and need for reasonable data security.[684]

241. By clarifying that our standard is one of "reasonableness" rather than strict liability, we address one of the major concerns that providers—including small providers and their associations—raise in this proceeding.[685] WTA, for instance, argues that a strict liability standard "is particularly inappropriate for small providers that lack the resources to install the expensive and constantly evolving safeguards necessary to comply with a strict liability regime."[686] We agree with these parties, and others such as the Federal Trade Commission staff,[687] that our rules should focus on the reasonableness of the providers' practices and not hold providers, including smaller providers, to a standard of strict liability.

242. We also agree with those commenters that argue that the reasonableness of a provider's data security practices will depend significantly on context.[688] The rule therefore identifies four factors that a provider must take into account when implementing data security measures: the nature and scope of its activities; the sensitivity of the data it collects; its size; and technical feasibility. Taken together, these factors give considerable flexibility to all providers. No one factor, taken independently, is determinative.

243. We include "size" in part based on the understanding in the record that smaller providers employ more limited data operations in comparison to their larger provider counterparts. While the other contextual factors already account considerably for the varying data collection and usage practices of providers of different sizes, we agree with commenters that size is an independent factor in what practices are reasonable for smaller providers, particularly to the extent that the smaller providers engage in limited data usage practices.[689] For instance, WTA explains that "its members do not currently, and have no plans to, retain customer Internet browsing histories and related information on an individual subscriber basis because the cost . . . would significantly outweigh any potential monetary benefit derived from data

[683] *See, e.g.*, FTC Staff Comments at 27-28; National Consumers League Comments at 9 (citing Kamala D. Harris, Cal. Dep't of Justice, *California Data Breach Report 2012-2015* 5 (2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf ) ("What constitutes *reasonable* data security today will not constitute reasonable data security tomorrow.") (emphasis added); Direct Marketing Association Comments at 24 ("Adequate protections for consumers can be effectively achieved by requiring BIAS providers to maintain 'reasonable' data security practices. . . ."); Jon Leibowitz Comments at 10-11; Electronic Transactions Association Comments at 2; New York Attorney General Reply at 3; $S^2$ERC Comments at 3; Online Trust Alliance Comments at 3; CompTIA Comments at 1-2; ViaSat Comments at 6-7; CDT Sept. 29, 2016 *Ex Parte* at 4; Letter From Harold Feld, Senior VP, Public Knowledge, to Marlene Dortch, Secretary, FCC at 3 (filed Oct. 3, 2016) (Public Knowledge Oct. 3, 2016 *Ex Parte*).

[684] *See* CenturyLink Comments at 32; Comcast Comments at 22; Verizon Comments at 65; T-Mobile Comments at 47; NCTA Reply at 54; CCA Reply at 10; WTA Aug. 22, 2016 *Ex Parte* at 3.

[685] *See, e.g.*, ACA Reply at 9-10; WTA Reply at 12-13; CenturyLink Comments at 32-33; T-Mobile Comments at 47-48.

[686] WTA Reply at 12; *see also* U.S. Small Business Administration Reply at 3 ("The record in this proceeding would support any effort by the FCC to mitigate the disproportionate compliance burden its proposal would have on small BIAS providers.").

[687] *See* FTC Staff Comments at 27-28.

[688] *See, e.g.*, CenturyLink Comments at 32 ("[A]ll providers should adopt reasonable data security safeguards based [on contextual factors proposed in the *NPRM*].").

[689] *See, e.g.*, WTA Aug. 22, 2016 *Ex Parte* at 3 ("WTA also argued that size should be a factor for consideration when assessing the implementation of reasonable security measures in order to avoid unreasonably holding small carriers with only a handful or two of employees to the same standard as providers that employ armies of technical and security professionals and drive industry best-practices.").

relating to the small subscriber bases of [rural carriers]."[690] Several small provider commenters also point out that many such providers have few employees and limited resources.[691] Accordingly, certain security measures that may be appropriate for larger providers, such as having a dedicated official to oversee data security implementation, are likely beyond the needs and resources of the smallest providers.[692] Our inclusion of "size" as a factor makes clear that small providers are permitted to adopt reasonable security practices that are appropriate for their businesses.[693] At the same time, we emphasize that all providers must adopt practices that take into account all four contextual factors. For instance, a small provider with very expansive data collection and usage practices could not point to its size as a defense for not implementing security measures appropriate for the "nature and scope" of its operations.[694]

244. The rule also takes into account the distinction between sensitive and non-sensitive information that underlies our customer approval requirements. Because the protection of both sensitive and non-sensitive customer PI is necessary to give effect to customer choices about the use and disclosure of their information,[695] our data security rule must cover both.[696] At the same time, we decline to require

[690] WTA Aug. 22, 2016 *Ex Parte* at 2-3; *see also* RWA Reply at 2 ("[U]nlike large or nationwide BIAS providers, [our] members do not generally collect, store, analyze, and exploit [CPNI]"); WTA Comments at 19 ("Small BIAS providers also do not engage in the collection and retention of sensitive consumer information to the extent that other industry participants that are subject to the FTC enforcement do."); CCA Comments at 33 ("[M]any CCA carrier members that fall under CCA's proposed definition of small provider do not share customer information with third parties for advertising purposes."); NTCA Comments at 1 ("As a general matter . . . NTCA members do not broker their customers' information."); ACA Comments at 5 (explaining that "ACA members generally do not use their customers' information for purposes requiring opt-in consent—often because they lack the incentive or resources to do so").

[691] *See* ACA Comments at 8 ("Most ACA members have few employees: half of ACA's members have ten or fewer employees."); Education and Research Consortium et al. Comments at 10; RWA Comments at 10-12; WISPA Comments at 26-27; WTA Aug. 22, 2016 *Ex Parte* at 3.

[692] *See* RWA Comments at 12 ("Saddling small carrier employees with qualification requirements in rural markets (where workforce demands are often already difficult to meet) is counterproductive and may force small rural carriers into unnecessary additional hires, solely for the purpose of meeting such requirements."). ACA Oct. 18, 2016 *Ex Parte* at 2 (urging the Commission to "[r]ecognize the limited financial resources of smaller ISPs in determining whether their data security practices are 'reasonable.'") (internal formatting omitted). Our decision not to adopt minimum required security practices should further allay concerns about the impact of the rule on small providers. *See, e.g.*, WTA Aug. 22, 2016 *Ex Parte* at 3 ("Because risk management requires tough decisions regarding which risks are reasonably acceptable in light of an organization's activities, size and resources, WTA urged the Commission to provide flexibility for small carriers and refrain from imposing specific security requirements beyond a generalized duty to employ reasonable security measures."); RWA Reply at 11 (citing WTA Comments at 21) ("[A]llow each BIAS provider to determine the particulars of and design its own risk management program, taking into account the probability and criticality of threats and vulnerabilities, as well as the nature and scope of a provider's business activities and the sensitivity of the underlying data."); ACA Reply at 44 ("[E]xempt small providers from the specific minimum data security requirements . . . ."); CTIA Reply at 10.

[693] *See* ACA Comments at 23; CCA Comments at 42; WTA Comments at 18-25; U.S. Small Business Administration Reply at 3-4; Letter From Joshua Seidemann, Vice President of Policy, NTCA, to Marlene Dortch, Secretary, FCC at 2-3 (filed Sept. 16, 2016) (NTCA Sept. 16, 2016 *Ex Parte*).

[694] *See* National Consumers League Reply at 21 ("[P]rotecting consumers' data is a part of running a modern company."). *But see* ACA Oct. 18, 2016 *Ex Parte* at 2 ("[The Order] should explicitly state that a higher relative cost for a smaller ISP to implement a practice on a per customer basis compared to a larger ISP is a factor in determining whether an ISP's implementation of a practices is reasonable.").

[695] *See supra* Part III.D.

[696] The State Privacy and Security Coalition argues that the security rule proposed in the *NPRM* would be too burdensome when applied to non-sensitive information. *See* State Security and Privacy Coalition Comments at 5, 11-12; *see also* Letter From Michelle Rosenthal, Senior Corporate Counsel, Government Affairs, Federal Regulatory, T-Mobile, to Marlene Dortch, Secretary, FCC at 2 (filed Sept. 14, 2016) (T-Mobile Sept. 14, 2016 *Ex*

(continued….)

"the same, strict data security protections" for all such information.[697] Rather, we direct providers to calibrate their security measures to "the sensitivity of the underlying data."[698] This approach finds broad support in the record[699] and is consistent with FTC guidance and precedent.[700] Similarly, our inclusion of "technical feasibility" as a factor makes clear that reasonable data security practices must evolve as technology advances.[701] Because our rule gives providers broad flexibility to consider costs when determining what security measures to implement over time, we do not find it necessary to include "cost of security measures" as a separate factor as AT&T and other commenters propose.[702] This means that every provider must adopt security measures that reasonably address the provider's data security risks.

245. In their comments, the National Consumers League recommended that we establish data security threshold requirements that providers could build on, but not fall below.[703] We find that unnecessary in light of the rules we adopt today. We believe that the flexible and forward-looking rule we adopt combined with the discussion that follows regarding exemplary practices makes clear that the rule sets a high and evolving standard of data security.[704] A provider that fails to keep current with industry best practices and other relevant guidance in designing and implementing its data security practices runs the risk of both a preventable data breach and that it will be found out of compliance with our data security rule. We also observe that we have already acted in multiple instances to enforce carriers' broad statutory obligations to take reasonable precautions to protect sensitive customer information.[705] In the *TerraCom* proceeding, for instance, we took action against a carrier under Section 222 of the Act for its failure to employ "appropriate security measures" to protect customers' Social Security numbers and other data from exposure on the public Internet.[706] Moreover, in *TerraCom* and other data security enforcement proceedings, parties have agreed to detailed data security obligations on individual carriers as conditions of settlement.[707] For example, as part of one consent decree entered into

(Continued from previous page)
*Parte*) ("The standard should be limited to either sensitive CPNI or CPNI that is likely to lead to an economic or physical harm in the event of an unauthorized disclosure."). We believe the modifications we have made to the proposal, including our decision not to adopt minimum required security practices, sufficiently address this concern.

[697] *Contra* National Consumers League Comments at 9; *but see* ACLU Comments at 6. As explained above, we have determined that it is both feasible and appropriate to draw a distinction between sensitive and non-sensitive information under our rules. *See supra* Part III.D.1.

[698] *See supra* para. 242. Where sensitive and non-sensitive customer PI are commingled, a carrier should err on the side of treating the information as sensitive.

[699] *See* Access Now Comments at 11; CTIA Comments at 96-97; IAB Comments at 11.

[700] *See* 2015 FTC Security Guide for Business at 1.

[701] *See, e.g.*, FTC Staff Comments at 27-28 (expressing support for a formulation of the rule that includes the "technical feasibility" factor).

[702] *But see* AT&T Comments at 78 ("The NPRM's discussion of 'reasonable' data security also ignores many factors that are highly relevant to what security measures should be adopted, such as the nature of the threats that ISPs face and the costs of security measures."); NTCA Sept. 16, 2016 *Ex Parte* at 4-5, n.5; CCA Oct. 13, 2016 *Ex Parte* at 6.

[703] *See* National Consumers League Reply at 19.

[704] *But see* Access Now Comments at 11 ("[T]he ultimate policy cannot create flexibility to excuse companies or actions from failing to provide adequate protections."); American Association of Law Libraries Comments at 4; Consumer Action Comments at 2; Access Humboldt et al. Comments at 5.

[705] *See TerraCom Consent Decree*, 30 FCC Rcd at 7075, paras. 1-2; *AT&T Consent Decree*, 30 FCC Rcd at 2808, para. 2; *Cox Consent Decree*, 30 FCC Rcd at 12303, para 4.

[706] *See TerraCom NAL*, 29 FCC Rcd at 13335, paras. 29-30.

[707] *See generally TerraCom Consent Decree*; *AT&T Consent Decree*; *Cox Consent Decree*.

by AT&T and the Commission's Enforcement Bureau, AT&T agreed to develop and implement a compliance plan aimed at preventing recurrence of a major data security lapse.[708] We have the ability to pursue similar remedial conditions in the context of any enforcement proceeding that may arise under the data security rule we adopt today, based on the facts of the case.

246. In addition, the flexibility we have built into our rule addresses concerns about potential conflict with the NIST Cybersecurity Framework (NIST CSF) and with other initiatives to confront data security as well as broader cyber threats.[709] The Commission values the NIST CSF and has demonstrated its commitment to promoting its adoption across the communications sector,[710] and we have accordingly fashioned a data security rule that closely harmonizes with the NIST CSF's flexible approach to risk management. The rule gives providers ample flexibility to implement the NIST CSF on a self-directed basis, and it imposes on BIAS providers a standard for data security similar to that which governs edge providers and other companies operating under the FTC's general jurisdiction.[711] We also reject any suggestions that our rule will impinge on BIAS providers' efforts to improve Internet security or protect their customers from malware, phishing attacks, and other cyber threats.[712] Indeed, protecting against such attacks and threats will only bolster a company's claims that it has reasonable data security practices. Moreover, as explained above, the rules adopted in this Report and Order do not prohibit or impose any constraint on cyber threat information sharing that is lawfully conducted pursuant to the Cybersecurity Information Sharing Act of 2015 (CISA).[713] Indeed, we believe that information sharing is a vital part of promoting data security across the industry.

247. Finally, we recognize that there is more to data security than the steps each individual provider takes to secure the data it possesses. For instance, effective consumer outreach and education can empower customers to be pro-active in protecting their own data from inadvertent or malicious disclosures. We also encourage providers to continue to engage constructively with the Commission, including through the CSRIC and related efforts, to develop and refine data security best practices. Also, as carriers develop and manage their security practices, we encourage them to be forward-looking. In particular, carriers should make efforts to anticipate future data security threats and proactively work to mitigate future risk drivers.

### 2. Practices That Are Exemplary of Reasonable Data Security

248. While we do not prescribe specific practices that a provider must undertake to comply with our data security rule, the requirement to engage in reasonable data security practices is set against a

[708] *See AT&T Consent Decree*, 30 FCC Rcd at 2808, para. 2.

[709] *See, e.g.*, Information Technology Industry Council Comments at 15 ("[The] proposed requirements contradict existing cybersecurity public policy – such as that embedded in the [NIST Cybersecurity Framework] – that risk management is a continuous process demanding flexibility . . ."); NTCA Sept. 16, 2016 *Ex Parte*.

[710] *See* Communications, Security, Reliability and Interoperability Council, Cybersecurity Risk Management Best Practices: Working Group 4: Final Report (March 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf (final report of a Commission federal advisory committee charged with developing "implementation guidance to help communication providers use and adapt the voluntary NIST Cybersecurity Framework").

[711] In late August, FTC staff issued a blog post as part of its data security education work showing how the NIST CSF and the FTC's data security work complement each other. *See* Andrea Arias, FTC, The NIST Cybersecurity Framework and the FTC (Aug. 31, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc (FTC Staff Guidance on NIST CSF).

[712] CTIA Reply at 83-85.

[713] *See* Cybersecurity Information Sharing Act of 2015, 6 U.S.C. §§ 1501-1510 (2016); *see also supra* para. 212.

backdrop of existing privacy and data security laws,[714] best practices,[715] and public-private initiatives.[716] Each of these is a potential source of guidance on practices that may be implemented to protect the confidentiality of customer PI. For the benefit of small providers, and others, below we discuss in more detail an evolving set of non-exclusive practices that we consider relevant to the question of whether a provider has complied with the requirement to take reasonable data security measures. While certain of these practices were originally proposed as minimum data security requirements,[717] we discuss them here as part of a set of practices that we presently consider exemplary of a reasonable and evolving standard of data security. We agree with commenters that dictating a minimum set of required practices could foster a "compliance mindset" that is at odds with the dynamic and innovative nature of data security.[718] Providers with less established data security programs may interpret such requirements as a checklist of what is required to achieve reasonable data security, an attitude we seek to discourage. We also seek to avoid codifying practices as the state of the art continues to rapidly evolve.[719] Our approach places the responsibility on each provider to develop and implement data security practices that are reasonable for its circumstances and to refine these practices over time as circumstances change.[720] Rather than mandate what these practices must entail, we provide guidance to assist each provider in achieving reasonable data

[714] *See, e.g.*, Federal Trade Commission Act, 15 U.S.C. § 45 (FTC Act provision setting forth the "unfair or deceptive" standard that guides FTC oversight of commercial data security practices); 42 U.S.C. § 1320d-2(d); 45 CFR §§ 164.302-164.318 (Health Insurance Portability and Accountability Act (HIPAA) "Security Rule" and related implementing regulations); 15 U.S.C. §§ 6801-6809; 16 CFR §§ 314.1-314.5 (Gramm-Leach-Bliley Act (GLBA) and its implementing regulations); Md. Code Ann., Com. Law § 14-3503(a); Utah Code Ann. § 13-44-201; Fla. Stat. § 501.171(2); Cal. Civ. Code § 1798.81.5(b)-(c) (examples of state laws on data security).

[715] *See, e.g.*, 2015 FTC Security Guide for Business; Federal Communications Commission, CSRIC Best Practices, https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm (last visited Oct. 5, 2016).

[716] *See, e.g.*, NIST, Cybersecurity Framework, http://www.nist.gov/cyberframework.

[717] *See Broadband Privacy NPRM*, 31 FCC Rcd at 2559-69, paras. 174-209.

[718] Charter Reply at 31; *see also* CTIA Comments at 151; Lenard and Wallsten Comments at 36; DMA Comments at 22 (arguing that minimum requirements "would merely add additional 'box checking'"); Cincinnati Bell Comments at 8 ("[The Commission] should future-proof its rules by encouraging BIAS providers to keep pace with rapid developments in the industry (*i.e.*, act reasonably)."); ViaSat Comments at 7. *But see* National Consumers League Reply at 19; CDT Sept. 29, 2016 *Ex Parte* at 4.

[719] For example, National Consumers League recommends adoption of multi-factor authentication as a required "minimum baseline." National Consumers League Comments at 14-16; *see also* AAJ Comments at 8. Yet the record includes discussion of a variety of techniques for robust customer authentication, not all of which would necessarily qualify as "multi-factor" in all circumstances. *See, e.g.*, Steven Bellovin Reply at 2 (recommending as a customer authentication method the use of data from commercial brokers to dynamically generate "unusual" security questions); Lorrie Faith Cranor Reply at 4 (observing that "[m]ulti-factor methods may or may not be necessary for routine transactions" but recommending that carriers always make such methods available to their customers); *see also* Consumers' Research Comments at 21 ("Log-in preferences vary widely, so when the Commission considers mandating a certain log-in technique, it is not listening to customers who are frustrated by onerous authentication methods that make account management an ordeal"); Cincinnati Bell Comments at 8-9 ("Instead of forcing rigid syntax rules (e.g., requiring certain characters), which may actually provide impostors with information as to the proper format of a valid password, ISPs should be allowed to offer flexible password strength and security features similar to current banking industry and Government agency practices when users set up access to their account information.").

[720] *But see* ITTA Comments at 23 (opposing a "one-size-fits-all" approach to data security); AT&T Comments at 79-80 (criticizing the "rigidity of the proposed rules"); ACA Comments at 23 ("The Commission's proposed prescriptive data security requirements would impose overwhelming costs and burdens on small providers.").

security on its own terms. Taking this approach will also allay concerns that overly prescriptive rules would frustrate rather than improve data security.[721]

249. While providers are not obligated to adopt any of the practices we suggest, we believe that together they provide a solid foundation for data security that providers can modify and build upon as their risks evolve and, as such, the presence and implementation of such practices will be factors we will consider in determining, in a given case, if a provider has complied with the reasonable data security requirement. However, these practices do not constitute a "safe harbor." A key virtue of the flexible data security rule we adopt today is that it permits data security practices to evolve as technology advances and new methods and techniques for data security come to maturity. We are concerned that any fixed set of security practices codified as a safe harbor would fail to keep pace with this evolutionary process.[722] The availability of a safe harbor may also discourage experimentation with more innovative data security practices and techniques. While it may be possible to construct a safe harbor "with concrete requirements backed by vigorous enforcement"[723] that also takes the evolution of data security practices into account, we find no guidance in the record on how to do so in a workable fashion. Accordingly, our approach is to evaluate the reasonableness of any provider's data security practices on a case-by-case basis under the totality of the circumstances, taking into account the contextual factors that are part of the rule. This approach is well-grounded in precedent[724] and will provide sufficient guidance to providers.[725] Our

[721] *See*, *e.g.*, CCA Comments at 41 ("CCA is concerned that if the FCC adopts its proposed specific data security requirements, it would quell the natural progression of best practices that currently is evolving, and ultimately force BIAS providers to prioritize compliance over an adaptable security risk-based management model that is required to address the evolving cyber threat landscape.") (internal quotation omitted); NCTA Reply at 55 ("[T]he specific data security obligations proposed or considered in the Notice . . . are overly prescriptive, not calibrated to incentivize protection for sensitive data, and inconsistent with state and federal policy."); WTA Comments at 18 ("Small providers do everything in their power to make sure that vulnerabilities are minimized, but they cannot be required to dedicate precious network resources to combat a vulnerability that is not likely to be a substantial threat to the rest of the network and other services provided to their customers."); T-Mobile Comments at 47 ("Providers must have the flexibility to allocate resources in accordance with the assessed risk to the provider and its customers, particularly as technology and the threat environments evolve."); AT&T Comments at 79 ("[T]he NPRM proposes that companies must 'promptly remedy *any*' security concerns that [risk management] assessments identify. On its face, this would require ISPs to address any issue identified by a security assessment, regardless of whether it is material, regardless of cost, regardless of the sensitivity of the underlying data, and regardless of the risk of a breach.").

[722] *See, e.g.*, Cincinnati Bell Comments at 8 ("[The Commission] should future-proof its rules by encouraging BIAS providers to keep pace with rapid developments in the industry (*i.e.*, act reasonably)."); *see also* WTA Comments at 19 ("Nor should the Commission establish safe harbors with respect to minimum data security standards as this could be seen by some as all that is required, rather than encouraging providers to take additional steps as appropriate to manage their cyber risk."). *But see* Hughes Oct. 14, 2016 *Ex Parte* at 3 (supporting adoption of a safe harbor).

[723] *See* FTC Staff Comments at 29.

[724] *See, e.g.*, *2015 Open Internet Order*, 30 FCC Rcd at 5659-69, paras. 133-53 (setting forth the "no-unreasonable interference/disadvantage standard" and the "factors to guide application of the rule"); *see also Implementing Public Safety Broadband Provisions of the Middle Class Tax Relief and Job Creation Act of 2012*, Order, 27 FCC Rcd 9652, 9662-64, para. 25 (2012) (articulating as "guidance" several "factors [the Commission] would likely find to be supportive of a public interest finding favorable to merit a grant" of a special temporary authorization); NCTA Comments at 87 ("A 'reasonableness' standard administered on a case-by-case basis makes sense, since it provides companies with the flexibility to adapt and innovate with regard to the manner in which they safeguard data."); CompTIA Comments at 2 (recommending implementation of "a case-by-case framework mirroring the FTC's implementation of Section 5 authority").

[725] *See* $S^2$ERC Comments at 3 ("[L]everaging the FCC's expertise to provide interpretive and technical guidance could bolster consumer privacy and simplify compliance for new and smaller BIAS providers."); T-Mobile Sept. 14, 2016 *Ex Parte* at 2 ("The final rule should include a reasonableness standard that can be supplemented by further

(continued….)

approach to data security also mirrors the FTC's, under which the reasonableness of an individual company's data security practices is assessed against a background of evolving industry guidance.[726] The CPBR also takes a similar approach.[727]

250. *Engagement with Industry Best Practices and Risk Management Tools*. We encourage providers to engage with and implement up-to-date and relevant industry best practices, including available guidance on how to manage security risks responsibly. One powerful tool that can assist providers in this respect is the NIST CSF, which many commenters endorse as a voluntary framework for cyber security and data security risk management.[728] We agree that proper implementation of the NIST CSF, as part of a provider's overall risk management, would contribute significantly to reasonable data security, and that use of the NIST CSF can guide the implementation of specific data security practices that are within the scope of that framework.[729] We encourage providers to consider use of the NIST CSF, as the widespread adoption of this common framework permits the Commission to optimize its engagement with the industry. That said, we clarify that use of the NIST CSF is voluntary, and providers retain the option to use whatever risk management approach best fits their needs. In addition, we encourage providers to look to guidance from the FTC,[730] as well as materials that have been issued to guide the implementation of data security requirements under HIPAA, GLBA, and other relevant statutory frameworks.[731] Finally, we note that a Commission multi-stakeholder advisory body, the Communications Security, Reliability, and Interoperability Council (CSRIC), has produced a rich repository of best practices on various aspects of communications security[732] as well as alerting the Commission of useful activities for which Commission leadership can effectively convene stakeholders to address industry-wide risk factors. In particular, CSRIC has developed voluntary mechanisms by which the communications industry can address cyber risk, based upon the NIST CSF. Many providers and

(Continued from previous page)
FCC guidance as to what constitutes 'reasonable security,' and that can evolve with changing technology and threat environments.").

[726] *See, e.g.*, FTC Security Guide for Business at 1 ("Distilling the facts of [more than fifty FTC data security enforcement actions] down to their essence, here are ten lessons to learn that touch on vulnerabilities that could affect your company, along with practical guidance on how to reduce the risks they pose.").

[727] *See* 2015 Administration CPBR Discussion Draft at § 105.

[728] *See, e.g.*, CenturyLink Comments at 37-38; Charter Reply at 31; NCTA Reply at 57; *see also* FTC Staff Guidance on NIST CSF ("[A]s the FTC's enforcement actions show, companies could have better protected consumers' information if they had followed fundamental security practices like those highlighted in the [NIST CSF].").

[729] *See, e.g.*, Access Now Comments at 11 ("[A]ccess controls, authentication safeguards, and notification and patching systems are all considerations in the NIST Framework.").

[730] *See, e.g.*, Ohlhausen Comments at 1 ("We [*i.e.*, the FTC] conduct extensive consumer and business outreach and guidance; coordinate workshops to foster discussions about emerging privacy and data security issues; coordinate on international privacy efforts; and advocate public policies that protect privacy, enhance data security, and improve consumer welfare."); *see also* 2015 FTC Security Guide for Business. This document imparts "lessons learned from the more than 50 law enforcement actions [regarding data security] the FTC has announced so far." *Id*. at 1.

[731] *See, e.g.*, National Institute for Standards and Technology, An Introductory Resource Guide for Implementing the Health Insurance Portability And Accountability Act (HIPAA) Security Rule at 15-17 (2008), http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist80066.pdf (NIST guidance for HIPAA Security Rule risk analyses).

[732] *See* FCC, CSRIC Best Practices, https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm.

industry associations that have participated in this proceeding are active contributors to the CSRIC's work.[733] We encourage providers to consider implementation of the CSRIC best practices as appropriate.

251. *Strong Accountability and Oversight*. Strong accountability and oversight mechanisms are another factor we consider exemplary of reasonable data security. As an initial matter, we agree with the FTC that the development of a written comprehensive data security program is a practice that is a best practice in promoting reasonable data security. As the FTC explains, putting a data security program in writing can "permit internal and external auditors to measure the effectiveness of the program and provide for continuity as staff members leave and join the team."[734] A written security program can also reinforce the specific practices a provider implements to achieve reasonable data security.

252. A second accountability mechanism that helps a company engage in reasonable data security is the designation of a senior management official or officials with personal responsibility over and accountability for the implementation and maintenance of the provider's data security practices as well as an official responsible for its privacy practices.[735] Companies that take this step are advised to couple designation of corporate privacy and security roles and responsibilities with effective interaction with Boards of Directors (or, for firms without formal Board oversight, such other structure governing the firm's risk management and oversight), to provide a mechanism for including cyber risk reduction expense within overall risk management plans and resource allocations**.** That said, we do not specify the qualifications or status that such an official would need to possess, and we recognize that for a smaller provider these responsibilities may rest with someone who performs multiple functions or may be outsourced.[736] Another practice that is indicative of reasonable data security is training employees and contractors on the proper handling of customer PI.[737] Employee training is a longstanding component of data security under the Commission's existing rules.[738] We encourage providers to seek out expert guidance and best practices on the design and implementation of efficacious training programs.[739] Finally, accountability and oversight are also relevant in the context of sharing customer PI with third parties. We agree with commenters that providers must take reasonable steps to promote the safe handling of customer PI they share with third parties.[740] Perhaps the most straightforward means of achieving this accountability is to obtain data security commitments from the third party as a condition of the disclosure.[741] We also remind providers that they are directly accountable for the acts and omissions

[733] *See* FCC, CSRIC, Membership List, https://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC_Membership_03_17_15.pdf (CSRIC membership as of March 17, 2015); *see also* CenturyLink Comments at 10-11; NTCA Sept. 16, 2016 *Ex Parte* at 2.

[734] FTC Staff Comments at 28.

[735] *See* Access Now Comments at 12 ("Digital rights like privacy and freedom of expression are material issues that require board-level oversight in information and communication technology companies."); National Consumers League Comments at 18-19.

[736] *See, e.g.*, WTA Aug. 22, 2016 *Ex Parte* at 3; RWA Comments at 12.

[737] *See* NTCA Comments at 62; Sprint Comments at 19; Greenlining Institute Comments at 47; American Association of Law Libraries Comments at 4; National Consumers League Comments at 17-18.

[738] *See 1998 CPNI Order*, 13 FCC Rcd at 8198, para. 198; *see also* 47 CFR § 64.2009(b).

[739] *See, e.g.*, International Association of Privacy Professionals Reply at 3-5 ("More than 10,000 IAPP members have already been certified under the association's various bodies of knowledge" such as the Certified Information Privacy Professional (CIPP) program, Certified Information Privacy Manager (CIPM) program, and Certified Information Privacy Technologist (CIPT) program, which are "accredited by the American National Standards Institute (ANSI) under the International Organization for Standardization's (ISO) standard 17024: 2012 . . .").

[740] *See* Greenlining Institute Comments at 45-47; Electronic Frontier Foundation Comments at 16; American Association of Law Libraries Comments at 5; AAJ Comments at 7-8; Access Humboldt et al. Comments at 5. Third party recipients of customer PI may also be subject to FTC jurisdiction. *But see* $S^2$ERC Comments at 14-15.

[741] *See* National Consumers League Comments at 21; EFF Comments at 16.

of their agents, including independent contractors, for the entirety of the data lifecycle. This means that the acts and omissions of agents will be taken into account in assessing whether a provider has engaged in reasonable data security practices.[742]

253. *Robust Customer Authentication*. The strength of a provider's customer authentication practices also is probative of reasonable data security. We have recognized that there is no single approach to customer authentication that is appropriate in all cases, and authentication techniques and practices are constantly evolving.[743] That said, the record documents some discernable trends in this area that we would currently expect providers to take into account.[744] For instance, we encourage providers to consider stronger alternatives to relying on rudimentary forms of authentication like customer-generated passwords or static security questions.[745] Providers may also consider the use of heightened authentication procedures for any disclosure that would place a customer at serious risk of harm if the disclosure were improperly made.[746] In addition, we encourage providers to periodically reassess the efficacy of their authentication practices and consider possible improvements.[747] Another practice we encourage providers to consider is to notify customers of account changes and attempted account changes. These notifications provide a valuable tool for customers to monitor their own accounts' security.[748] Providers that implement them should consider the potential for "notice fatigue" in determining how often and under what circumstances these notifications are sent.

254. *Other Practices*. The record identifies other practices that we encourage providers to consider when implementing reasonable security measures. For instance, several commenters cite the importance of "data minimization," which involves thinking carefully about what data to collect, how long to retain it, and how to dispose of it securely.[749] The principle of data minimization is also embodied in FTC guidance,[750] in the CPBR,[751] and in the Satellite and Cable Privacy Acts.[752] We encourage

[742] *See* 47 U.S.C. § 217; *Long Distance Direct, Inc.*, Apparent Liability for Forfeiture, 15 FCC Rcd 3297, 3300, para. 9 (2000) (clarifying that Section 217 imposes liability for acts of independent contractors).

[743] *See Broadband Privacy NPRM*, 31 FCC Rcd at 2564, para. 193.

[744] *See* Lorrie Faith Cranor Reply at 3-6; Steven Bellovin Reply at 1-2; National Consumers League Comments at 14-16.

[745] *See* Lorrie Faith Cranor Reply at 4 (suggesting that multi-factor authentication methods "should always be offered to customers who want to use them"); Steven Bellovin Reply at 1 (describing the use of smart-phone apps, commercial data brokers, and written requests as alternate authentication methods); $S^2$ERC Comments at 15 ("[O]ne mechanism for improving customer authentication processes might be eliminating the usage of certain identifiers . . . . such as Social Security Number and mother's maiden name."); Mozilla Comments at 7; National Consumers League Comments at 14-15; Paul Vixie Comments at 26-31.

[746] *See* Lorrie Faith Cranor Reply at 4 ("[Providers] should establish authentication procedures that are not unduly burdensome to their customers performing routine transactions, but that may require extra steps in higher-risk situations (for example when a mobile customer requests an account change but claims to have lost their phone).").

[747] *See* Lorrie Faith Cranor Reply at 4 ("Due to changing technology and differences in the ways BIAS providers interact with their customers, I recommend allowing providers some flexibility in establishing authentication procedures informed by periodic risk assessments and updated to respond to the changing technology and security landscape."); *Cf.* National Consumers League Comments at 15 (advocating for an FCC advisory council to regularly assess the efficacy of multi-factor authentication methods and recommend updates).

[748] *See* Lorrie Faith Cranor Reply at 6 ("[Account change notification] is a currently implemented best practice and makes sense to continue.").

[749] *See, e.g.*, EPIC Comments at 24; EFF Comments at 6-7; Mozilla Comments at 7.

[750] *See* 2015 FTC Guide for Business at 2 (advising businesses not to "collect personal information you don't need," and to "[h]old on to information only as long as you have a legitimate business need").

[751] *See* 2015 Administration CPBR Discussion Draft at § 104.

providers to look specifically to the FTC's "Disposal Rule" for guidance on the safe destruction and disposal of customer PI.[753] We also encourage providers to consider data minimization practices that apply for the entirety of the data lifecycle, from collection to deletion. In addition, several commenters recommend strong data encryption,[754] another practice that the FTC advises companies to consider.[755] We agree with commenters that technologically sound data encryption can significantly improve data security, in part by minimizing the consequences of a breach.[756] Finally, we believe that the lawful exchange of information regarding cyber incidents and threats is relevant to promoting data security, and encourage providers to consider engagement in established information sharing practices.

255. The exemplary practices discussed above are not an exhaustive list of reasonable data security practices. A provider that implements each of these practices may still fall short of its data security obligation if there remain unreasonable defects in its protection of the confidentiality of customer PI. Conversely, a provider may satisfy the rule without implementing each of the listed practices. The key question is whether a provider has taken reasonable measures to secure customer PI, based on the totality of the circumstances. In taking this approach, we acknowledge that the adoption of more prescriptive, bright-line requirements could offer providers greater certainty as to what reasonable data security requires. Yet virtually all providers that have addressed the issue—including small providers and their associations—oppose such requirements.[757] Rather, these providers prefer the approach we have taken in this Report and Order, i.e., the adoption of a "reasonableness" standard that mirrors the FTC's.[758] Also like the FTC, we have provided the industry with guidance on how to achieve reasonable data security in compliance with our rule. We anticipate building upon this guidance over time as data security practices evolve and with them the concept of reasonable data security.

### 3. Extension of the Data Security Rule to Cover Voice Services

256. In light of the record, we conclude that harmonization of the data security requirements that apply to BIAS and other telecommunications services is the best option for providers and consumers alike. Accordingly, we extend to voice services the data security rule we have adopted for BIAS.[759] This data security rule replaces the more inflexible data security requirements presently codified in Part 64 of the rules.[760]

257. There are many reasons to harmonize the data security requirements that apply to BIAS and voice services. As an initial matter, many providers offer services of both kinds and often sell them together in bundled packages.[761] We agree with commenters that argue that applying different security requirements to the two kinds of services may confuse customers and add unnecessary complexity to

(Continued from previous page)

[752] *See* 47 U.S.C. §§ 551(e), 338(i)(6) ("Destruction of information").

[753] *See* 16 CFR § 682.3(a); *see also* FTC Staff Comments at 28-29 (discussing the Disposal Rule). There are also state laws on data disposal that may provide additional guidance. *E.g.*, Ark. Code Ann. § 4-110-104(a); Kan. Stat. Ann. § 50-7a03; N.J. Stat. Ann. § 56:8-162.

[754] *See* EPIC Comments at 23; OTI Comments at 41; Paul Vixie Comments at 31; WTA Comments at 20-21.

[755] *See* 2015 FTC Guide for Business at 6-7.

[756] *See infra* para. 269.

[757] *See, e.g.*, ACA Comments at 23-28; WISPA Comments at 31; CCA Comments at 38; CTIA Comments at 154-56; NCTA Comments at 87-89.

[758] *See, e.g.*, CTIA Comments at 155-56 ("Rather than imposing the prescriptive regulation proposed in the NPRM, the Commission should consider a flexible reasonableness standard for data security, akin to the FTC model.").

[759] *See supra* note 68.

[760] *See supra* note 659.

[761] *See, e.g.*, *Broadband Privacy NPRM*, 31 FCC Rcd at 2536-37, n.181.

providers' data security operations, which may be particularly burdensome for smaller providers.[762] In addition, the evidence suggests that the data security requirements of the existing rules no longer provide the best fit with the present and anticipated communications environment. For instance, expert commentary on the topic of robust customer authentication indicates that this is a complex area where providers need flexibility to adapt their practices to new threats.[763] The highly specific procedures outlined in the existing voice rules are incongruous with this approach to customer authentication.[764]

258. Moreover, retaining the prescriptive data security rules that apply to voice services could impede the development and implementation of more innovative data security measures for BIAS. Providers subject to both sets of rules may determine that the easiest and most cost-effective path to compliance is to adopt for both services the more rigid data security practices that the voice rules require.[765] Such an outcome would contravene our intent to establish a robust and flexible standard for BIAS data security that evolves over time.

259. Accordingly, we find that the best course is to replace the data security rules that currently govern voice services with the more flexible standard we are adopting for BIAS. We find that the rule as written is sufficiently broad to cover BIAS and other telecommunications services. We also clarify that the exemplary practices we discuss above may be implemented differently depending on the services an entity provides. For instance, data security best practices that pertain specifically to broadband networks or services may or may not be relevant in the context of providing voice services.

260. In harmonizing the data security rules for voice services and BIAS, we acknowledge that voice providers have operated for many years under the existing rules and have tailored their data security practices accordingly. We do not expect any provider to revamp its data security practices overnight. On the contrary, as explained below, we are adopting an implementation schedule that affords providers ample time to bring their practices into compliance with the new rules.[766]

### F. Data Breach Notification Requirements

261. In this section we adopt rules requiring BIAS providers and other telecommunications carriers to notify affected customers, the Commission, the FBI, and the Secret Service of data breaches unless the provider reasonably determines that no harm to customers is reasonably likely to occur.[767] For purposes of these rules, we define a breach as any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information. The record clearly demonstrates that data breach notification plays a critical role in protecting the confidentiality of customer PI. An obligation to notify customers and law enforcement agencies when

[762] *See* ACA Comments at 57-58; RWA Comments at 10-12.

[763] *See generally* Lorrie Faith Cranor Reply at 1 (outlining "how authentication requirements may address the growing problem of mobile phone account hijacking and related fraud"); Steven Bellovin Reply; *see also* ACA Comments at 53 (characterizing the voice authentication rules as "[o]verly prescriptive"); Letter From Catherine M. Hilke, Assistant General Counsel, Verizon, to Marlene Dortch, Secretary, FCC at 1 (filed Sept. 23, 2016) (Verizon Sept. 23, 2016 *Ex Parte*) ("Harmonization also would provide the Commission with the opportunity to update its existing but outdated voice rules, including those related to authentication that may inhibit providers from taking advantage of new, more secure technologies.").

[764] The rules specify authentication procedures for different kinds of customer interactions: in person, over the telephone, and online. *See* 47 CFR § 64.2010(b)-(d). Authentication online or during a customer-initiated telephone call requires the use of a password. *See id*. at § 64.2010(b), (c).

[765] *See, e.g.*, WTA Comments at 19 (discussing the costs that would accrue to smaller providers in complying with "multiple regulatory regimes").

[766] *See infra* Part III.I.

[767] The data breach notification requirements adopted in this Report and Order extend to breaches involving a carrier's vendors and contractors. *See* 47 U.S.C. § 217.

customer data is improperly accessed, used, or disclosed incentivizes carriers to adopt strong data security practices.[768] Breach notifications also empower customers to protect themselves against further harms, help the Commission identify and confront systemic network vulnerabilities, and assist law enforcement agencies with criminal investigations. At the same time, unnecessary notification can cause notice fatigue, erosion of consumer confidence in the communications they receive from their provider, and inflated compliance costs. The approach we adopt today finds broad support in the record and will maximize the benefits of breach notification as a consumer protection and public safety measure while avoiding unnecessary burdens on providers and their customers. Furthermore, our approach is consistent with how federal law enforcement agencies, such as the FBI and Secret Service, conduct and coordinate data breach investigations.

262. First, we address the circumstances that will obligate BIAS providers and other telecommunications carriers to notify the Commission, federal law enforcement agencies, and customers of data breaches.[769] This includes a discussion of two related elements adopted today: the harm-based notification trigger and the updated definition for "breach." We then address the requirements that BIAS providers and other telecommunications carriers must follow for providing notice to the Commission and other federal law enforcement. Next, we describe the specific notification requirements that BIAS providers and other telecommunications carriers must follow in providing data breach notifications to customers, including: the required timing for sending notification; the necessary contents of the notification; and the permissible methods of notification. We then discuss the data breach record retention requirements. Finally, we explain our decision to adopt rules that harmonize data breach requirements for BIAS providers and other telecommunications carriers.

### 1. Harm-Based Notification Trigger

263. We require breach notification unless a carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. We do so to enable customers to receive the data breach notifications that they need to take steps to protect themselves, and to provide the Commission, the FBI, and Secret Service with the information they need to evaluate the efficacy of data security rules as well as detect systemic threats and vulnerabilities. In the *NPRM* we sought comment on what should trigger data breach notification, and based on the record, we conclude that the trigger most suitable for our purposes is one based on the potential for customer harm.[770] Among its many benefits, this harm-based trigger will avoid burdening providers and customers alike with excessive notifications, and it will allow providers the flexibility to focus limited resources on data security and ameliorating customer harms resulting from data breaches rather than on notifications that have minimal benefit to customers.[771] The record reflects various harms inherent in unnecessary notification, including notice fatigue,[772] erosion of consumer confidence in the communications they receive from their provider,[773] and

[768] *See, e.g.*, Access Now Comments at 12.

[769] We note that these obligations are not mutually exclusive with other data breach notification obligations stemming from other state, local, or federal laws, or contractual obligations. *See* Part III.J.

[770] *See, e.g.*, Lenard and Wallsten Paper at 28; FBI/Secret Service Reply at 3-4; CenturyLink Comments at 41-42; CTIA Comments at 176; Comcast Comments at 61-62; AT&T Comments at 80-81; INCOMPAS Comments at 16; Letter from Jacquelyne Flemming, AT&T, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1 (filed July 28, 2016) (AT&T July 28, 2016 *Ex Parte*).

[771] *See, e.g.*, XO Communications Comments at 6 (explaining that data breach notifications based on customer harm "increases the likelihood that the consumer will be motivated to read the notice and take appropriate action, such as monitoring relevant accounts, to prevent and mitigate potential harm, including identity or financial theft"); INCOMPAS Comments at 16 (arguing that without an intent or harm standard, customers will not understand the potential impact of breaches in the notification they receive); AT&T Comments at 81 (asserting that over-reporting will distract attention from genuine data security).

[772] *See, e.g.*, XO Communications Comments at 9-10 (asserting that "consumers and other notification recipients will so regularly receive such notices that they will inevitably stop reading them because it will become impossible

(continued….)

compliance costs.[774] The harm-based notification trigger we adopt addresses these concerns, by limiting the overall volume of notifications sent to customers and eliminating correspondence that provides minimal or no customer benefit.

264. Our harm-based trigger has a strong basis in existing state data breach notification frameworks.[775] The triggers employed in these laws vary from state to state, but in general they permit covered entities to avoid notifying customers of breaches where the entity makes some determination that the breach will not or is unlikely to cause harm.[776] Likewise, the 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."[777] Our rule similarly requires the carrier to reasonably determine that no harm to

(Continued from previous page)
to discern which notices involve a true threat to their identity or finances, from those that pose effectively no risk."); CompTIA Comments at 4; ICC Comments at 15; State Privacy and Security Coalition Comments at 4-5; AT&T Comments at 81; Comcast Comments at 62-63 ("If customers receive such meaningless breach notifications, they are more likely to disregard the notifications that are meaningful—not only from their ISP, but generally.").

[773] *See, e.g.*, CenturyLink Comments at 41 (asserting that "[o]ver-notification would also impose substantial disruptions on the consumer-BIAS provider relationship" and that the "harm to public perception and brand value of the BIAS provider that would result is both unnecessary and unfair – and could even, in some cases, lead consumers to opt out of broadband use entirely."); WISPA Comments at 20 ("Consumers should not be overwhelmed with inconsequential notices that potentially create unwarranted distrust of its providers."); INCOMPAS Comments at 16; T-Mobile Comments at 51-52 ("Notifications involving breaches that pose no harm – which cannot offer the consumer any meaningful steps to take in response – serve only to confuse customers and corrode faith in providers' practices based on misconceptions as to the consequences of a purported 'breach.'"); Verizon Comments at 69 ("[T]he provider responsible for these excessive breach notifications will risk losing the customer's trust for no good reason: for sending notifications when there has been no harm (or even risk of harm) to the customer's privacy interests.").

[774] *See, e.g.*, ACA Comments at 35 ("Moreover, the costs of providing notifications and associated breach costs are sky high—one recent estimate was well over $130 per person." citing Richard Kissel, Hyunjeong Moon, U.S. Dep't of Commerce, Draft NISTIR 7621 Revision 1, *Small Business Information Security: The Fundamentals* 2 (2014)); State Privacy and Security Coalition Comments at 8-9 ("[B]reach notice incidents are expensive. The average cost per record of a data breach including both out of pocket costs and harm to good will currently exceeds $200 per record." citing Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis* (2015), *available at* https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF); CTIA Comments at 175 (asserting that reporting of minor non-harmful breaches is costly to ISPs and of no use to consumers).

[775] *See generally* Nat'l Conference of State Legislatures, *Security Breach Notification Laws*; *see also* Jill Joerling, Data Breach Notification Laws: An argument For a Comprehensive Federal Law to Protect Consumer Data, 32 Wash. U. J. L. & Pol'y 467 (2010).

[776] For example, Connecticut does not require entities to disclose a breach if an investigation determines that no harm is likely. *See* Conn. Gen. Stat. § 36a-701b(b)(1); *see also* Ark. Code § 4-110-105(d) (notice not required if no reasonable likelihood of harm); Fla. Stat. § 501.171(6)(b) (notice not required if reasonably determined that breach has not and will not likely result in identity theft or any other financial harm); Iowa Code § 715C.2(6) (no notice required if no reasonable likelihood of financial harm has resulted or will result from the breach); Or. Rev. Stat. § 646A.602(1)(a) (no notice required if no reasonable likelihood of harm has resulted or will result from the breach); N.J. Stat. Ann. § 56:8-163(a) (notice not required if determined that misuse of the information is not reasonably possible); *see also* State Privacy and Security Coalition Comments at 13("A large majority of state breach notice laws (41 out of 47) contain a 'harm trigger' to distinguish between these circumstances and to avoid over-notification.").

[777] *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); *see also* Letter from James J.R. Talbot, AT&T, to Marlene H. Dortch, Secretary, FCC, WC Docket N0. 16-106, at 2 (filed Aug. 23, 2016)
(continued….)

customers is reasonably likely to occur. As such, we disagree with commenters arguing that standards based on determinations of harm leave consumers more vulnerable to that harm.[778] On the contrary, the record, and the many state laws addressing data breach notifications, demonstrate that providers have ample experience determining a likelihood of harm.[779] Additionally, the reasonableness standard that applies to both the carrier's evaluation and the likelihood of harm adds an objective component to these determinations.

265. Further, the harm-based trigger places the burden on a carrier that detects a breach to reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. This responds to concerns such as AAJ's that it is "frequently impossible" for a carrier to immediately discern the full scope and ramifications of a breach.[780] Our harm-based trigger does not relieve a carrier of its notification obligation simply by virtue of its failure or inability to ascertain the harmful effects of a breach. Rather, carriers must take the investigative steps necessary to reach a reasonable determination that no such harm is reasonably likely. Where a carrier's investigation of a breach leaves it uncertain whether a breach may have resulted in customer harm, the obligation to notify remains. By contrast, requiring customer notification *only when* a provider determines the presence of some risk of harm would create perverse incentives not to carefully investigate breaches.[781]

266. In adopting a harm-based trigger, we clarify that its scope is not limited to "easily recognized financial harm."[782] In the *NPRM*, we acknowledged that "harm" is a concept that can be broadly construed to encompass "financial, physical, and emotional harm."[783] We conclude that the same construction of harm is appropriate for our final breach notification rule. This decision is consistent with the fundamental premise of this proceeding that customer privacy is about more than protection from economic harm. The record demonstrates that commenters' privacy concerns stem from more than just avoiding financial harms.[784] As such, we disagree with commenters who assert that financial loss or identity theft should be the primary metrics for determining the level of harm or whether harm exists at

(Continued from previous page)
(AT&T Aug. 23, 2016 *Ex Parte*) (asserting that "the Commission should reduce excessive reporting by adopting the approach taken by many states of not requiring notification where a provider determines that there is no reasonable likelihood of harm to any customer resulting from the breach).

[778] *See, e.g.*, AAJ Comments at 7.

[779] *See supra* note 776.

[780] *See* AAJ Comments at 7.

[781] Some comments could be construed as supporting a standard of this kind. *See, e.g.*, CTIA Comments at 176 ("The Commission should require notification only if a breach causes harm or is likely to cause harm.").

[782] *See* Access Now Comments at 13 ("There are standard practices for response to breaches involving data such as credit card information or social security numbers. However, there is no standard practice for breaches that involve PII that cannot easily be tied to financial harm, such as personal photos. Stronger responses to a broader array of breaches would increase user trust in BIAS providers.").

[783] *See Broadband Privacy NPRM*, 31 FCC Rcd at 2575-76, para. 237 n.373 (citing *Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, Report and Order, 26 FCC Rcd 9114, 9122, para. 22 (2011) (agreeing that the term "'harm' is a broad concept that encompasses financial, physical, and emotional harm")).

[784] Privacy Rights Clearinghouse Comments at 6 ("Privacy harms are broad and nuanced, and breach victims often suffer or are at risk of suffering harms that can't be qualified as financial or economic in nature."); LGBT Technology Partnership Comments at 1-2 ("All around the country, LGBT people still face signification discrimination including bullying, rejection by families, loss of employment and even the possibility of physical harm simply for their LGBT identity . . . For this reason, LGBT individuals are fiercely protective of their privacy and may face drastic consequences if that privacy is breached."); *see also* TRUSTe & Nat'l Cyber Sec. Alliance, *U.S. Consumer Privacy Index 2016, available at* https://staysafeonline.org/download/datasets/17482/DPD[4].pdf. (showing that 68 percent of consumers were more concerned about not knowing how personal information was collected online than losing their principal income) (Consumer Privacy Index 2016).

all.[785] Some commenters have called "for the FCC to help determine how organizations can better respond to breaches in which personal, non-financial data is breached."[786] We find that within the meaning of Section 222(a), threats to the "confidentiality" of customer PI include not only identity theft or financial loss but also reputational damage, personal embarrassment, or loss of control over the exposure of intimate personal details.[787]

267. Relatedly, we establish a rebuttable presumption that any breach involving sensitive customer PI presumptively poses a reasonable likelihood of customer harm and would therefore require customer notification. This rebuttable presumption finds a strong basis in the record.[788] Even commenters that favor minimal breach reporting generally concede that customers are entitled to notification when their most sensitive information is misused or disclosed.[789] The presumption also aligns with our decision to base the level of customer approval required for use or disclosure of customer PI on whether the PI is sensitive in nature. As we explain above, this distinction upholds the widespread expectation that customers should be able to maintain particularly close control over their most sensitive personal data.[790] While breaches of sensitive customer PI often present severe risks of concrete economic harm,[791] there is a more fundamental harm that comes from the loss of control over information the customer reasonably expects to be treated as sensitive.

268. We also find that our employing a harm-based trigger will substantially reduce the burdens of smaller providers in reporting breaches of customer PI.[792] We agree with commenters stating that a framework—such as ours—that allows providers to assess the likelihood of harm to their customers will ultimately be less costly and "will not overburden small providers."[793] The record indicates that smaller providers tend to collect and use customer data, including sensitive information, far less

[785] *See, e.g.*, DMA Comments at 28; ANA Comments at 31; ITI Comments at 11; WISPA Comments at 20-22; ACA Comments at 36-37.

[786] Access Now Comments at 2 (Nathan White); *see also* 2012 FTC Privacy Report at 7-9; 2015 Administration CPBR Discussion Draft, at § 4(g) (defining "privacy risk" as "the potential for personal data, on its own or when linked to other information about an individual, to cause emotional distress, or physical, financial, professional, or other harm to an individual.").

[787] *See, e.g.*, Access Now Comments at 13.

[788] *Cf.* XO Communications Comments at 8-9 (asserting that breach notification should be sensitivity-based); State Privacy and Security Coalition Comments at 13 ("Harm exists where the unauthorized acquisition creates a material or significant risk of identity theft, fraud, or in some cases, breach of very sensitive personal information such as private medical data . . ."); CenturyLink Comments at 16 ("Consumers expect that their sensitive information will be treated differently than information that is not sensitive, such as information that is readily and publicly available and thus poses no risk of identity theft or consumer harm."); AT&T July 28, 2016 *Ex Parte* at 1.

[789] *See, e.g.*, CTIA Comments at 96-97 (asserting that "any privacy rules that the Commission promulgates should protect data based on their sensitivity"); CenturyLink Comments at 16.

[790] *See supra* Part III.D.

[791] *See, e.g.*, FBI/Secret Service Reply at 3 (explaining that information about customers can be exploited by criminal groups to steal the identities of these customer or to target them for other criminal purposes, such as to implant malicious software on their devices, to extort money from them by encrypting devices, to compromise other online account the customer maintains, or to make them the target of any number of fraudulent schemes).

[792] *See, e.g.*, WTA Comments at 8-9, 17 (raising concerns about the impact on smaller providers of providing multiple notices).

[793] ACA Comments at 41-42 (arguing for the superiority of a data breach notification rule that provides a "safety valve for good faith disclosures so that small providers can avoid counterproductive strict liability enforcement actions associated with inflexible and overly prescriptive regimes.").

extensively than larger providers.[794] More modest collection and usage of customer PI leaves a provider less prone to breaches that would trigger a data breach notification obligation under our rule.

269. Finally, we clarify that our harm-based notification trigger applies to breaches of data in an encrypted form. Whether a breach of encrypted data presents a reasonable likelihood of harm will depend in significant part on the likelihood that unauthorized third parties reasonably would be expected to be able to decrypt the data.[795] Factors that make decryption more or less likely are therefore relevant in determining whether a reasonable likelihood of customer harm is present in such instances. These factors may include the quality of the encryption and whether third parties can access the encryption key. Ultimately, a provider must notify affected customers if it cannot reasonably determine that a breach poses no reasonable likelihood of harm, regardless of whether the breached data is encrypted.

270. With our adoption of a harm-based trigger, we have removed the need for a separate trigger based on intent. Thus, for purposes of these rules, we adopt the definition of breach that we proposed in the *NPRM* and define a breach as any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information. This definition is broader than the definition in our existing rules, which includes an intent element, and only applies to breaches of CPNI, in recognition that the record indicates that the relevant factor for breach reporting is not intent, but effect on the customer.[796]

271. We agree with other commenters that inadvertent breaches can be just as severe and harmful for consumers as intentional breaches,[797] and consumers are likely to care about serious breaches even when they occur by accident or mistake.[798] Moreover, whether or not a breach was intentional may not always be immediately apparent.[799] By defining breach to include unintentional access, use, or disclosure we ensure that in the event of a breach the provider has an incentive to investigate the cause and effect of the breach, and the opportunity to respond appropriately. Some commenters recommend that the definition of breach include an intent element to avoid equating inadvertent disclosure of customer PI to an employee or contractor of a provider with intentional hacking of customer records.[800]

---

[794] *See, e.g.*, WTA Aug. 22, 2016 *Ex Parte* at 1 (explaining that its small rural local exchange carrier members typically either refrain entirely from any use of CPNI for marketing purposes or alternatively providing customers the option to opt-out of marketing upon signing up for service, and that any sharing of information typically occurs "solely between the RLEC and its affiliates that provide services to their customers or third-parties that provide services related to the provision of telecommunications services, including but not limited to billing, help-desk representatives, and installation contractors").

[795] It also will depend on, among other things, the scope and magnitude of potential harm if the data were unencrypted.

[796] *See, e.g.*, OTI Comments at 33 ("Customer proprietary information, such as financial details included in applications for Lifeline service, can include highly sensitive information that must be adequately protected."); American Association for Justice Comments at 7; OTI Comments at 29; Access Now Comments at 13; AT&T Comments at 85.

[797] *See* American Association for Justice Comments at 7; OTI Comments at 29, 30-31 ("[C]onsumers may need to take action to protect themselves against inadvertent breaches of private information, which could harm consumers just as much as intentional breaches.").

[798] American Association for Justice Comments at 7 ("Whether a data breach was intentional or inadvertent has no bearing on the severity of the breach or the amount of information that is compromised."); Access Now Comments at 12; *see also* Online Trust Alliance Comments at 4

[799] *See* Paul Vixie Comments at 11 ("It is not always easy—or even possible—to determine what an intruder has accessed when a computer is breached."); *see also* OTI Comments at 29-30 (explaining that if an accidental breach is discovered, there is a possibility that a malicious breach took place as well).

[800] *See, e.g.*, XO Comments at 10-11; NTCA Comments at 34; WTA Comments at 8; CTIA Comments at 11.

The adoption of a harm-based trigger—in lieu of a trigger based on intent—creates a consistent obligation to report breaches that may harm consumers, regardless of the source or cause of the breach.

272. Commenters also argue that including an intent element in the definition of breach would prevent excessive data breach notifications.[801] Commenters making this argument raise the prospect of a flood of notifications for breaches that have no impact on the consumer, including such good-faith errors as an employee inadvertently accessing the wrong database.[802] We share their general concern about the risk of over-notification—it is costly to providers, without corresponding benefit to consumers, and can lead to notice fatigue and possibly consumer de-sensitization. However, in this context the argument is misplaced. Identifying a data breach is only the first step towards determining whether data breach notification is necessary. The harm-based trigger that we adopt today relieves a provider from notifying its customers and government agencies of breaches that result from minor mistakes that create no risk of harm to the affected customers. Based on this analysis, we find eliminating the word "intentionally" from our breach definition equally warranted for all telecommunications carriers.

273. Our adoption of a harm-based trigger also addresses concerns about the breadth of our breach definition. For example our definition includes incidents where a person gains unauthorized access to customer PI but makes no further use of the data.[803] We agree with AAJ that we must account for the difficulties a provider faces in determining when "access translates to acquisition and when acquisition leads to misuse."[804] Our rule appropriately requires providers to issue notifications in cases where a provider is unable to determine the full scope and impact of a breach. However, the definition of breach does not create an obligation to notify customers of an unauthorized gain of access—such as an employee opening the wrong file—once the provider reasonably determines that no harm is reasonably likely to occur. This accords with AT&T, which explains that "not requiring notification where a provider determines that there is no reasonable likelihood of harm to any customer resulting from the breach" will "reduce excessive reporting."[805]

274. Similarly, our harm-based trigger allays the concern that extending breach notification obligations beyond CPNI to customer PI more broadly would vastly expand the range of scenarios where notification is required.[806] This concern is largely premised on the assumption that we would require customer notification of all breaches of customer PI, regardless of the severity of the breach or the sensitivity of the PI at issue. As explained above, we have instead adopted a more targeted obligation that takes into account the potential for customer harm. In addition, we observe that many, if not all, state data breach notification requirements explicitly include sensitive categories of PII within their scope.[807]

---

[801] *See, e.g.*, INCOMPAS Comments at 15-16; ITTA Comments at 23; CompTIA Comments at 4; WTA Comments at 8-9; Internet Commerce Coalition Comments at 15; State Privacy and Security Coalition Comments at 17; CTIA Comments at 177-78.

[802] *See, e.g.*, WTA Comments at 8-9; T-Mobile Comments at 51; State Privacy and Security Coalition Comments at 17.

[803] We note that this aspect of our definition of "breach" is consistent with our prior definition. *See 2007 CPNI Order*, 22 FCC Rcd at 6978.

[804] American Association for Justice Comments at 7.

[805] AT&T Aug. 23, 2016 *Ex Parte* at 2.

[806] ACA Comments at 35; AT&T Comments at 78; CTIA Comments at 175.

[807] *See, e.g.*, Alaska Stat. § 45.48.090(7); Haw. Rev. Stat. §487N-1; Mass. Gen. Laws ch. 93H § 1(a) (financial account/credit or debit number can be *with or without* required access codes or passwords) (emphasis added); Minn. Stat. § 325E.61(1)(e)-(f); Mont. Code Ann. § 30-14-1704(4)(b); Ohio Rev. Code Ann. § 1349.19(A)(7)(a); Okla. Stat. § 24-162(6); Utah Code Ann. § 13-44-102(3); Ark. Code § 4-110-103(7); Del. Code Ann. tit. 6 § 12B-101(4); Ky. Rev. Stat. § 365.732(1)(c)); Mich. Comp. Laws § 445.63(3)(r); Miss. Code Ann. § 75-24-29(2)(b); Nev. Rev. Stat. § 603A.040; N.H. Rev. Stat. Ann. § 359-C:19(IV); N.J. Stat. Ann. § 56:8-161(10); 73 Pa. Stat. § 2302; 11 R.I.

(continued….)

Under our rule, breaches involving such information would presumptively meet our harm trigger and thus require notification. We think it is clear that the unauthorized exposure of sensitive PII, such as Social Security numbers or financial records, is reasonably likely to pose a risk of customer harm, and no commenter contends otherwise. We therefore find it appropriate for our breach notification rule to apply broadly to customer PI, including PII.

### 2. Notification to the Commission and Federal Law Enforcement

275. In this section, we describe rules requiring telecommunications carriers to notify the Commission and federal law enforcement of breaches of customer PI, under the harm-based notification trigger discussed above. We also specify the timeframe and methods by which providers must provide this information.

276. *Scope*. As proposed in the *NPRM*, we require notification to the Commission of all breaches that meet the harm-based trigger and, when the breach affects 5,000 or more customers, the FBI and Secret Service. We expect that this notification data will facilitate dialogue between the Commission and telecommunications carriers, and will prove extremely valuable to the Commission in evaluating the efficacy of its data security rules, as well as in identifying systemic negative trends and vulnerabilities that can be addressed with individual providers or the industry as a whole including to further the goal of collaborative improvement and refinement of data security practices.[808] Still, we retain discretion to take enforcement action to ensure BIAS providers and other telecommunications carriers are fulfilling their statutory duties to protect customer information.

277. We adopt an additional trigger of at least 5,000 affected customers for notification to the Secret Service and FBI, in order to ensure that these agencies are not inundated with notifications that are unlikely to have significant law enforcement implications. This threshold finds support in the comments of the FBI and Secret Service[809] and is also consistent with or similar to provisions in various legislative and administration proposals for a federal data breach law.[810] We recognize that there may be circumstances under which carriers want to share breach information that does not meet the harm trigger we adopt today as part of a broader voluntary cybersecurity and threat detection program, and we encourage providers to continue these voluntary efforts.[811]

278. *Timeframe*. The dictates of public safety and emergency response may require that the Commission and law enforcement agencies be notified of a breach in advance of customers and the

(Continued from previous page)
Gen. Laws § 11-49.2-5(c); Tenn. Code App. § 47-18-2107(a)(3); Va. Code Ann. § 18.2-186.6(A); W. Va. Code § 46A-2A-101(6); D.C. Code § 28-3581(3).

[808] National Consumers League Comments at 24-25 ("Breaches indicate lapses or vulnerabilities in security that companies will be forced to recognize and fix. NCL believes that an ancillary benefit of these breach notification requirements is the creation of incentives for companies to share information in order to minimize the impact for themselves and for customers." (citations omitted)).

[809] FBI/Secret Service Reply at 6.

[810] *Cf.* Data Security and Breach Notification Act of 2015, H.R. 1770, 114th Cong. § 3(a)(5) (2015) (requiring 10,000 individuals); Data Security and Breach Notification Act of 2015, S. 177, 114th Cong. § 4 (2015) (requiring 10,000 individuals); Updated Data Breach Notification 2 (2015), *in* Letter from Shaun Donovan, Dir., Office of Mgmt. & Budget, Exec. Office of the President, to the Hon. John A. Boehner, Speaker of the H.R. (Jan 13, 2015), *available at* https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf (OMB proposed legislation and text for the *Personal Data Breach Notification and Protection Act* to the House of Representatives and the Senate, requiring 10,000 individuals).

[811] *See supra* para. 246.

general public.[812] Thus, for breaches affecting 5,000 or more customers, we require carriers to notify the Commission, the FBI, and the Secret Service within seven (7) business days of when the carrier reasonably determines that a breach has occurred, and at least three (3) business days before notifying customers. For breaches affecting fewer than 5,000 customers, carriers must notify the Commission without unreasonable delay and no later than thirty (30) calendar days following the carrier's reasonable determination that a reach has occurred. Both of these thresholds remain subject to the harm-based trigger. We agree with commenters that the timeline for data breach notification should not begin when a provider first identifies suspicious activity.[813] At the same time, we clarify that "reasonably determining" a breach has occurred does not mean reaching a conclusion regarding every fact surrounding a data security incident that may constitute a breach. Rather, a carrier will be treated as having "reasonably determined" that a breach has occurred when the carrier has information indicating that it is more likely than not that there was a breach. To further clarify, the notification timelines discussed herein run from the carrier's reasonable determination that a breach has occurred, not from the determination that the breach meets the harm-based notification trigger.

279. We agree with the FBI and the Secret Service that advance notification of breaches will enable law enforcement agencies to take steps to avoid the destruction of evidence and to assess the need for further delays in publicizing the details of a breach.[814] We reject arguments that the timeframes for Commission and law enforcement notification that we adopt are too burdensome.[815] Rather, we agree with AT&T and other commenters in the record that allowing carriers seven (7) business days to notify the Commission and law enforcement furnishes those providers with sufficient time to adequately investigate suspected breaches.[816] Further, to address concerns expressed in the record regarding the

[812] FBI/Secret Service Reply at 5 (arguing that early notification to federal law-enforcement agencies would help assess the intrusion, secure evidence, facilitate interagency coordination, and consider whether there is a need to further delay customer notification).

[813] *See, e.g.*, Letter from Jacquelyne Flemming, AT&T, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1 (filed Sept. 21, 2016) (AT&T Sept. 21, 2016 *Ex Parte*) (arguing that providers should be allowed an opportunity to distinguish actual breaches from merely suspicious activity or conduct); CenturyLink Comments at 43 ("Ultimately, any notification timeline should be tied initially to the determination that a breach has occurred."); *see also* $S^2$ERC Comments at 16 ("A clearer definition of what constitutes the "discovery" of a breach may be necessary to aid in compliance with the timeline requirements.").

[814] FBI/Secret Service Reply at 5 ("Early notification to the Federal Law Enforcement Agencies will enable law enforcement to assess the intrusion and engage meaningfully with the Service Provider when it may be possible to obtain vital evidence that could become obscured or destroyed over time. Early notification will also permit the Federal Law Enforcement Agencies to coordinate their efforts so that any law enforcement response can maximize the resources available to address and respond to the intrusion. . . Another benefit of early notification to the Federal Law Enforcement Agencies is that early notice will allow law enforcement agencies sufficient opportunity to determine whether there is a need for delayed notice to customers . . .").

[815] *See*, *e.g.*, Hughes Comments at 7 (recommending a 30 day renewable time from for notices to the Commission and law enforcement to ease compliance); WISPA Comments at 32 ("The proposed deadlines would require notification to Federal law enforcement and customers much more quickly than nearly all state laws require such that it may be difficult for even larger providers to comply with the Commission's proposals.") (footnote omitted); INCOMPAS Comments at 14-15, 17-18; ACA Comments at 35-36, 54-55.

[816] AT&T Aug. 23, 2016 *Ex Parte* at 2 (supporting a framework requiring Commission notification without unreasonable delay and within seven (7) business days as opposed to 7-10 days); AT&T July 28, 2016 *Ex Parte* at 2 (supporting business day framework for notification deadlines); *see* ViaSat Comments at 7 (proposing that BIAS providers should have ten (10) total "business" days to notify consumers, the Commission, and federal law enforcement as opposed to the "10 days" proposed in the NPRM); *but see* Online Trust Alliance May 27, 2016 *Ex Parte* at 3-4 (supporting ten (10) business day standard for customer breach notification deadline but seven (7) calendar day standard for Commission and law enforcement breach notification); Hughes Network Systems, LLC July 26, 2016 *Ex Parte* at 1-2 (supporting general 30 day requirement for data breach reporting).

complexity and costs of data breach notification for smaller providers,[817] we relax the notification timeframe for breaches affecting fewer than 5,000 customers. Carriers must notify the Commission of breaches affecting less than 5,000 customers without unreasonable delay and no later than thirty (30) calendar days following the carrier's reasonable determination that a breach has occurred. We find that a 30-day notification timeframe for breaches affecting fewer than 5,000 customers provides the Commission with the data necessary to monitor trends and gain meaningful insight from breach activity across the country, while at the same time reducing and simplifying the requirements for all carriers, particularly smaller providers, whose limited resources might be better deployed toward remediating and preventing breach activity, particularly in the early days of addressing a relatively small breach.

280. We also recognize that a carrier's understanding of the circumstances and impact of a breach may evolve over time. We expect carriers to supplement their initial breach notifications to the Commission, FBI, and Secret Service, as appropriate.[818] Early notification of breaches will improve the Commission's situational awareness and enable it to coordinate effectively with other agencies, including with the FBI and Secret Service on breaches not reportable directly to these agencies that may nevertheless raise law enforcement concerns. Furthermore, time is of the essence in a criminal investigation.[819] Learning promptly of a significant, large-scale breach gives law enforcement agencies an opportunity "to coordinate their efforts so that any law enforcement response can maximize the resources available to address and respond to the intrusion."[820] Given the vital interests at stake in cases where a data breach merits a law enforcement response, we find that the seven (7) business day reporting deadline for such breaches is necessary as a matter of public safety and national security.

281. To further advance the needs of law enforcement, we permit the FBI or Secret Service to direct a provider to delay notifying customers and the public at large of a breach for as long as necessary to avoid interference with an ongoing criminal or national security investigation.[821] This provision replaces the more prescriptive requirements in the existing rules specifying the timing and methods for law enforcement intervention.[822] Consistent with our overall approach in this proceeding, we adopt rules that incorporate flexibility to account for changing circumstances. Several commenters agree that this provision for law enforcement, which is embodied in the existing rules, remains prudent.[823] We also observe that the laws of several states and the District of Columbia include similar law enforcement delay provisions.[824] We are not persuaded that such a provision unduly interferes with the interests of

[817] Letter from Thomas Cohen, Attorney, Kelley Drye & Warren, LLP, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 4 (filed Oct. 5, 2016) (American Cable Association Oct. 5, 2016 *Ex Parte*) (arguing that small providers should be allowed to notify the Commission of smaller breaches at the same time that customers are notified).

[818] *See, e.g.*, AT&T Aug. 23, 2016 *Ex Parte* at 2 (proposing a modified notification framework that accounts for ongoing data breach investigations stretching beyond the initial 30 day window).

[819] *See* FBI/Secret Service Reply at 5.

[820] *Id.*

[821] *See id.* at 6.

[822] *See* 47 CFR § 64.2011(b)(3).

[823] National Consumers League Comments at 32 (stating that this requirement "strikes the appropriate balance between customers' need to know and the ability of federal law enforcement to properly investigate the origins of the breach."); FTC Staff Comments at 33.

[824] *See* Ariz. Rev. Stat. § 18-545(C); Ark. Code § 4-110-105(c); Cal. Civ. Code § 1798.82(c) (*amended by* 2015 Cal. Assem. B. 739); Conn. Gen. Stat. § 36a-701b(d); D.C. Code § 28-3852(d); Ga. Code Ann. § 10-1-912(c); Ky. Rev. Stat. § 365.732(4); La. Stat. Ann. § 51:3074(D); Me. Rev. Stat. tit. 10, § 1348(3); Minn. Stat. § 325E.61(1)(c); Mont. Code Ann. § 30-14-1704(3); Nev. Rev. Stat. § 603A.220(3); N.J. Stat. Ann. § 56:8-163(c)(2); N.Y. Gen. Bus. Law § 899-aa(4); N.D. Cent. Code § 51-30-04; 11 R.I. Gen. Laws § 11-49.3-4(b); S.C. Code Ann. § 39-1-90(C); Tex. Bus. & Com. Code Ann. § 521.053(d).

customers in taking informed action to protect themselves against breaches.[825] As the FBI and Secret Service explain, customer notification delays are not routine but are requested as a matter of practice only in "exceptional circumstances" involving a serious threat of harm to individuals or national security.[826] In addition, decisions regarding when to publicly disclose details of a criminal investigation are a matter that lies within the expertise of law enforcement agencies. We therefore find that the best course is to defer to the judgment of the FBI and Secret Service on when the benefits of delaying customer notification outweigh the risks.

282. *Method*. We will create a centralized portal for reporting breaches to the Commission and other federal law enforcement agencies. The Commission will issue a public notice with details on how to access and use this portal once it is in place. The reporting interface will include simple means of indicating whether a breach meets the 5,000-customer threshold for reporting to the FBI and Secret Service. The creation of this reporting facility will streamline the notification process,[827] reducing burdens for providers, particularly small providers. Any material filed in this reporting facility will be presumed confidential and not made routinely available for public inspection.[828]

### 3. Customer Notification Requirements

283. In order to ensure that telecommunications customers receive timely notification of potentially harmful breaches of their customer PI, we adopt rules specifying how quickly BIAS providers and other telecommunications carriers must notify their customers of a breach, the information that must be included in the breach notification, and the appropriate method of notification.

#### a. Timeline for Notifying Customers

284. We require BIAS providers and other telecommunications carriers to notify affected customers of reportable breaches of their customer PI without unreasonable delay, and no later than 30 calendar days following the carriers' reasonable determination that a breach has occurred, unless the FBI or Secret Service requests a further delay.[829] This approach balances affected customers' need to be notified of potentially harmful breaches of their confidential information with carriers' need to properly determine the scope and impact of the breach, and to the extent necessary, to most immediately focus resources on preventing further breaches. Also, the specific customer notification timeline we adopt has broad record support.[830]

---

[825] $S^2$ERC Comments at 16 ("The three-day notification delay requirement considered at the request of law enforcement is understandable but such regulations are often not in the best interest of consumers. Such delays may allow criminals to wipe out the assets of a customer using stolen PI before the customer becomes aware of the threat. Restitution following such an incident is not always complete and is rarely timely or convenient for the victims. Additionally, the delay requirement may raise the liability of BIAS providers significantly as criminals may continue to rack up damages during the waiting period. At the very least, BIAS providers should not be liable for harms that occur after a breach is reported to law enforcement – especially when these harms could have been prevented with earlier notification.").

[826] FBI/Secret Service Reply at 4.

[827] *See, e.g.*, ACA Comments at 56-57 (asserting that the Commission "should create a one-stop shop for Commission and law enforcement notifications to avoid the need to [*sic*] duplicative notification").

[828] *See* 47 CFR § 0.457.

[829] *See supra* Part III.F.2.

[830] *See, e.g.*, Comcast Comments at 63 (stating that "the Commission should follow other well-established breach laws and allow at least 30 days after discovery of a breach to notify consumers"); Hughes Comments at 6-7 (stating that "a more equitable solution would be to stipulate that broadband service providers must report a breach within 30 days from the discovery of that breach, with leave to extend the reporting period by 30 day increments if the broadband service provider can demonstrate that more time is needed to determine the scope of the breach, to conduct risk assessments, and to restore reasonable integrity to the network"); AT&T Aug. 23, 2016 *Ex Parte* at 2 (continued….)

285. As an initial matter, we agree with commenters that clear and straightforward notification deadlines are necessary to ensure that customers are timely notified of breaches that affect them.[831] We also agree with commenters that providing more time to notify customers than the 10 days we initially proposed will enable carriers to conduct a more thorough and complete investigation of breaches in advance of the notification.[832] This extra time for investigation will minimize duplicative and incomplete breach notices, avoid customer confusion, allow providers to focus first on stopping further breaches, and minimize burdens on providers.[833] The FBI and Secret Service, which have extensive experience with data breach notification and, more specifically, experience with our existing data breach notification rules, generally support a customer notification timeframe of between 10 and 30 days.[834] FTC staff recommends that breach notifications occur without unreasonable delay, but within an outer limit of between 30-60 days.[835] State data breach laws vary, but most states do not require notification within a specific time frame and the majority of states that do provide 45 days or more to provide notice.[836]

286. Our adoption of a customer notification period longer than that initially proposed also responds to concerns raised by smaller carriers. For example, the Rural Wireless Association argues that "[s]mall BIAS providers need additional time [beyond ten days] to determine the extent of any breach, as well as to consult with counsel as to the appropriate next steps."[837] The American Cable Association similarly argues that compliance with a compressed notification timeline would require small providers "to divert senior and technical staff solely to data breach response for the duration of the breach response period" and otherwise incur high compliance costs.[838] We are mindful of the compliance burdens that a 10-day period for customer notification would impose on small carriers in particular, and accordingly adopt a more flexible requirement to notify customers of reportable breaches without unreasonable delay and in any event no longer than 30 calendar days. These commenters and others proposed longer notification periods and, alternatively, an open-ended non-specific timeframe for small providers.[839] While we are sensitive to these concerns, we also note, however, that customer exposure to avoidable or

(Continued from previous page)
(supporting a framework to notify affected customers without unreasonable delay and no later than 20 business days after notification to the Commission).

[831] *See, e.g.*, OTI Comments at 43.

[832] State Privacy and Security Coalition Comments at 14 ("When a breach or suspected breach occurs, a company's top priorities are to ascertain the nature of the event, restore the security and integrity of the affected system, and determine the scope of the incident and who was affected. Time is of the essence. A requirement to report very quickly after discovery of a breach takes important resources away from remediation and investigation."); Hughes Comments at 6-7 ("This minimal modification of the proposed rule will give time for quick action while recognizing the real time needed accurately to respond to a reported breach.").

[833] *See, e.g.*, State Privacy and Security Coalition Comments at 13-14; INCOMPAS Aug. 4, 2016 *Ex Parte* at 3.

[834] FBI/Secret Service Reply at 5 ("The Federal Law Enforcement Agencies are primarily concerned with breaches involving suspected criminal activity, and would support a more relaxed reporting timeline for those breaches not involving potential criminal activity.").

[835] FTC Staff Comments at 33.

[836] *See* ACA Comments at 54-55; Jill Joerling, Data Breach Notification Laws: An Argument For a Comprehensive Federal Law to Protect Consumer Data, 32 Wash. U. J. L. & Pol'y 467, 477 (2010).

[837] RWA Comments at 13.

[838] ACA Comments at 34-35.

[839] *See* RWA Comments at 13 (arguing for a 45-day notification timeline where state law does not mandate a specific timeline); ACA Comments at 34-35 (arguing for an "as soon as reasonably practical" standard); Letter from Rebecca Murphy Thompson, Executive Vice President and General Counsel, Competitive Carriers Association, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 4 (filed Oct. 19, 2016) (CCA Oct. 19, 2016 *Ex Parte*) (arguing for a 60-day customer notification timeline for small providers).

mitigable risk continues to grow in the aftermath of a breach. We therefore emphasize the value of notifying affected customers as soon as possible to allow the customer to undertake time-sensitive mitigation activities and encourage carriers to notify consumers as soon as practicable.

287. Requiring carriers to notify affected customers without unreasonable delay while adopting a 30 calendar day deadline to do so creates a backstop against excessive delays in notifying customers. Of course, if a telecommunications carrier conducts a good faith, reasonable investigation within 30 calendar days but later determines that the scope of affected customers is larger than initially known, we expect that provider to notify those additional customers as soon as possible.[840] However, based on the record, we find that 30 calendar days is ample time to prepare a customer notification that meets our minimum content requirements, as discussed below.[841] Our prior rules did not specify a precise timeline for customer notice—only that it must occur after the carrier completes law enforcement notification—and we find adoption of the timeline above warranted to ensure timely notification to customers. We recognize that a carrier may identify a breach and later learn that the scope of the breach is larger than initially determined. Under such circumstances a carrier has a continuing obligation to notify without unreasonable delay any additional customers it identifies as having been affected by the breach, to the extent the carrier cannot reasonably determine that no harm is reasonably likely to occur to the newly identified affected customers as a result of the breach.

**b. Information Provided as Part of Customer Breach Notifications**

288. To be a useful tool for consumers, breach notifications should include information that helps the customer understand the scope of the breach, the harm that might result, and whether the customer should take any action in response. In the *NPRM* we proposed that providers include certain types of basic information in their data breach notifications to affected customers, and based on the record, we adopt those same basic requirements,[842] which include the following elements:

- The date, estimated date, or estimated date range of the breach;
- A description of the customer PI that was used, disclosed, or accessed, or reasonably believed to have been used, disclosed, or accessed, by a person without authorization or exceeding authorization as a part of the breach of security;
- Information the customer can use to contact the telecommunications carrier to inquire about the breach of security and the customer PI that the carrier maintains about the customer;
- Information about how to contact the Federal Communications Commission and any state regulatory agencies relevant to the customer and the service; and
- If the breach creates a risk of financial harm, information about national credit-reporting agencies and the steps customers can take to guard against identity theft, including any credit monitoring, credit reporting, or credit freezes the telecommunications carrier is offering customers affected by the breach of security.

289. While data breaches are not "one-size-fits-all," creating a measure of consistency across customer breach notifications will benefit customers and providers, particularly smaller providers, by

[840] *See, e.g.*, AT&T Aug. 23, 2016 *Ex Parte* at 2 (proposing a modified notification framework that accounts for ongoing data breach investigations stretching beyond the initial 30 day window).

[841] *See, e.g.*, AT&T July 28, 2016 *Ex Parte* at 2 ("To allow providers adequate time to identify all affected customers and prepare relevant information for them and any other relevant support such as call centers they can contact with follow-up questions, providers should be allowed up to 20 business days after making that determination to notify customers.").

[842] *See, e.g.*, OTI Comments at 42; NTCA Comments at 68; *see also* Access Now Comments at 12 (asserting that remediation options should be clearly indicated and accessible in breach notices).

removing any need to reinvent the wheel in the event of a data breach. Seventeen states and territories currently mandate that specific content be included in breach notifications and the requirements we adopt today are generally consistent with those statutes.[843] Much of the information we require consists of contact information for the Commission, relevant authorities, credit reporting agencies, and the carrier itself. Based on the record, we also require customer breach notifications to contain information about credit freezes and credit monitoring if the breach creates a risk of financial harm.[844] The foregoing elements should be easy for any provider to ascertain and for customers to understand. The remaining two elements simply define the basic elements of a breach notification—when the breach occurred and what information was breached.[845] Additionally, we hold carriers to a reasonable standard of accuracy and precision in providing this information. Rather than having to provide the exact moment a breach occurred, providers are tasked with giving an "estimated" date or, alternatively, an estimated date "range." Moreover, while a description of the customer PI involved in the breach should be as detailed, informative, and accurate as possible, the rule allows for a description of the data the telecommunications carrier "reasonably believes" was used, disclosed, or accessed.

290. We encourage providers to supplement these minimum elements with additional information that their customers may find useful or informative. For example, FTC Staff recommends that notifications include contact information for the FTC, and a reference to its comprehensive IdentityTheft.gov website.[846] In appropriate cases, providing such additional information could further empower customers to take steps to mitigate their own harm and protect themselves against the effects of any future breaches.

#### c. Notification Methods

291. As proposed in the *NPRM*, we require that customer notifications occur by means of written notification to the customer's address of record or email address, or by contacting the customer by other electronic means of active communications agreed upon by the customer for contacting that customer for data breach notification purposes. For former customers, we require carriers to issue notification to the customer's last known postal address that can be determined using commonly available sources. These options create flexibility for providers to notify customers in a manner they choose to be contacted by their provider, and they are consistent with methods permitted under other data breach

[843] *See generally* Cal. Civ. Code § 1798.82(d) (California); Haw. Rev. Stat. § 487N-2(d) (Hawaii); 815 ILCS § 530/10(a) (Illinois); Iowa Code § 715C.2(5) (Iowa); Md. Code Com. Law § 14-3504 (Maryland); Mass. Gen. Laws § 93H-3(b) (Massachusetts); Mich. Comp. Laws § 445.72(6) (Michigan); Mo. Rev. Stat. § 407.1500.2(4) (Missouri); N.H. Rev. Stat. § 359-C:20(IV) (New Hampshire); N.Y. Gen. Bus. Law § 899-aa(7) (New York); N.C. Gen. Stat § 75-65(d) (North Carolina); Or. Rev. Stat. § 646A.605(5) (Oregon); Vt. Stat. tit. 9 § 2435(b)(5) (Vermont); Va. Code § 18.2-186.6,A (Virginia); W.V. Code § 46A-2A-102(d) (West Virginia); Wyo. Stat. § 40-12-501(e) (Wyoming); P.R. Laws tit.10 § 4053 (Puerto Rico).

[844] National Consumers League Comments at 30. Several states currently require data breach notices to contain information about both credit monitoring and credit freezes. *See* Conn. Gen. Stat. §36a-701b(b); 815 Ill. Comp. Stat §530/10(a); Mass. Gen. Laws Ch. 93H § 3(b); 10-1-912(c); W. Va. Code § 46A-2A-102(d). *But see* FTC Staff Comments ("While contacting the national credit reporting agencies may be appropriate in certain circumstances, it may not be helpful in others and could create a false sense of security.").

[845] *See, e.g.*, Cal. Civ. Code § 1798.82(d) (requiring approximate date of breach and types of personal information that were or are reasonably believed to have been subject to a breach); Fla. Stat. § 501.171(4)(f) (requiring estimated date range of breach and a description of the personal information accessed or reasonably believed to have been accessed); Iowa Code § 715C.2(5) (requiring approximate date of the breach and the type of personal information obtained as a result of the breach); N.H. Rev. Stat. Ann. § 359-C:20(IV) (requiring approximate date of breach and the type of personal information obtained as a result of the breach).

[846] Several states already require this. *See* 815 Ill. Comp. Stat § 530/10(a); Md. Code. Ann., Com. Law. § 14-3504(g); N.C. Gen. Stat. § 75-65(d).

notification frameworks.[847] One of the few commenters to address this issue supports the *NPRM* proposal, while also suggesting that providers post "substitute breach notifications" on their websites.[848] While some other breach notification frameworks do include such a requirement,[849] we are not persuaded it is necessary for our purposes. Telecommunications carriers have direct relationships with their customers through which they are likely to have ready means of contacting them. We believe the options discussed above for direct notification will generally provide a sufficient array of options for reaching customers affected by a breach, and we thus decline also to require a broader, less targeted public disclosure.

#### 4. Record Retention

292. We adopt a streamlined version of the record retention requirement we proposed in the *NPRM*. We require only that providers keep record of the dates on which they determine that reportable breaches have occurred and the dates when customers are notified, and that they preserve written copies of all customer notifications. These records must be kept for two years from the date a breach was reasonably determined to have occurred. The purpose of this limited requirement is to enable Commission oversight of the customer breach notifications our rule requires. This minor recordkeeping requirement will not impose any significant administrative burden on providers.[850] On the contrary, the information that must be retained must be collected anyway, is of limited quantity, and largely comprises information we would expect carriers to retain as a matter of business practice.[851] Moreover, shortening the retention period would weaken the utility of the requirement as an enforcement tool, while not delivering any substantiated cost savings for providers.[852] As a final point, we clarify that we do not require carriers to retain records of breaches that do not rise to the level of a required Commission notification. A large percentage of breaches are therefore likely to be exempted from this requirement.

#### 5. Harmonization

293. In the *NPRM*, we proposed adoption of a harmonized breach notification rule for BIAS and other telecommunications services that would replace the existing Part 64 rule. Based on the record, we have determined to take this approach. We agree with commenters who argue that creating a harmonized rule will enable providers to streamline their notification processes and will reduce the potential for customer confusion.[853] Moreover, we find that the modifications we have made to the

[847] *See* 45 CFR § 164.404(d)(1) (HIPAA); N.Y. Gen. Bus. Law § 899-aa(5); Arizona Rev. Stat. § 44-7501(D); Ark. Code § 4-110-105(e); Colo. Rev. Stat. § 6-1-716(1)(c).

[848] National Consumers League Comments at 29 ("In addition to a choice between written and electronic notifications required in 47 U.S.C. § 64.7006(a)(1), BIAS providers should be required to post and maintain substitute breach notifications in a clearly marked section of their websites.").

[849] Some states, however, allow for substitute notice depending on the cost and number of affected individuals. *See, e.g.*, Me. Stat. tit. 10 § 1347(4)(C) ($5,000 or 1,000 residents); Mich. Comp. Laws § 445.72(12)(5)(d) ($250,000 and 500,000 residents).

[850] National Consumers League Comments at 33.

[851] *Id.*

[852] *But see* Hughes Comments at 9 ("A six month recordkeeping requirement will ensure that customers' records are retained for a reasonable period following the termination of service and give the Commission and law enforcement agencies sufficient access to records to conduct investigations of consumer complaints.").

[853] Greenlining Institute Comments at 16 ("Commenters believe that a uniform regime is not only easier for the carriers, easier of enforcement, and easier for customers to understand, it is also consistent with the Open Internet Order in terms of law and policy."); WTA Comments at 17 ("There is no reason that BIAS providers should have different customer notification requirements for breaches, particularly when many BIAS providers also provide voice and/or video service as part of a bundle. Providing more than one notice could also cause consumer confusion and would be more burdensome and costly than simply requiring one notice per affected customer."); INCOMPAS Comments at 17-18.

proposed rule, particularly the harm trigger we adopt and timeline for notifying customers, ameliorate concerns that applying the new rule to both BIAS and other telecommunications services will unduly increase burdens for voice providers.[854]

### G. Particular Practices that Raise Privacy Concerns

294. In this section we prohibit "take-it-or-leave-it" offers in which BIAS providers offer broadband service contingent on customers surrendering their privacy rights as contrary to the requirements of Sections 222, 201, and 202 of the Act. We also adopt heightened disclosure and affirmative consent requirements for BIAS providers that offer customers financial incentives, such as lower monthly rates, in exchange for the right to use the customers' confidential information. Congress has tasked the Commission with protecting the public interest, and we conclude that our two-fold approach to these practices will permit innovative and experimental service offerings and encourage and promote customer choice, while prohibiting the most egregious offerings that would harm the public interest.

#### 1. BIAS Providers May Not Offer Service Contingent on Consumers' Surrender of Privacy Rights

295. We agree with those commenters that argue that BIAS providers should not be allowed to condition or effectively condition the provision of broadband on consenting to use or sharing of a customer's PI over which our rules provide the consumer with a right of approval.[855] Consistent with our proposal in the *NPRM*, we therefore prohibit BIAS providers from conditioning the provision of broadband service on a customer surrendering his or her privacy rights.[856] We also prohibit BIAS providers from terminating service or otherwise refusing to provide BIAS due to a customer's refusal to waive any such privacy rights. By design, such "take-it-or-leave-it" practices offer no choice to consumers. The record supports our finding that such practices will harm consumers, particularly lower-income customers,[857] and we agree with Atomite that there is a difference between offering consumers "a carrot (i.e., consideration in exchange for property rights) and [] a stick (e.g., no ISP service unless subscribers relinquish their property rights)."[858] We therefore conclude that prohibiting such practices will ensure that consumers will not have to trade their privacy for broadband services.

296. As we discussed above, broadband plays a pivotal role in modern life.[859] We find that a "take-it-or-leave it" approach to the offering of broadband service contingent upon relinquishing customer

[854] *See supra* paras. 263, 284.

[855] *See, e.g.*, Privacy Rights Clearinghouse Comments at 6 ("Under no circumstances should any consumer, especially those who are members of vulnerable communities, have to choose between their rights to privacy and foregoing broadband service."); Access Now Comments a 7 ("To ensure user protection, consent must be freely and unambiguously given. This means, for instance, that the use of a service must not be contingent on consumer approval for the sharing of personal information with third parties or for the use of information for other purposes than the one it was originally collected."); ACLU Comments at 6 (arguing that requiring customers to sign away their privacy rights as a condition of service, or certain kinds of service should be prohibited as it would "create a gaping loophole that would quickly be exploited"); NTCA Comments at 71 (stating it does "not oppose disallowing practices that enable providers to deny service if customers do not relinquish certain rights").

[856] *Broadband Privacy NPRM*, 31 FCC Rcd at 2682, para. 285 (proposing to "prohibit BIAS providers from making service offers contingent on a customer surrendering his or her privacy rights").

[857] *See supra* note 855; *see also* Letter from Eric G. Null, New America's Open Technology Institute, to Marlene H. Dortch, Secretary, FCC, GN Docket No 16-106 at 3 (filed Sept. 12, 2016) ("Low-income individuals often rely on a single device, meaning the single ISP used by that person has access to extensive information about the individual. Pay-for-privacy would be particularly problematic in the Lifeline context. Lifeline subscribers, who are among the most vulnerable populations, should not be forced to give up their privacy for an Internet connection.").

[858] Atomite Comments at 6.

[859] *See supra* Part III.A.

privacy rights is inconsistent with the telecommunications carriers' "duty to protect the confidentiality of proprietary information of, and related to . . . customers."[860] Further, we find that a "take-it-or-leave-it" customer acceptance is not customer "approval" within the meaning of Section 222(c)(1), which prohibits telecommunications carriers from using, disclosing, or permitting access to CPNI without customer approval.[861]

297. We also conclude that requiring customers to relinquish all privacy rights to their PI to purchase broadband services is an unjust and unreasonable practice within the meaning of Section 201(b).[862] Requiring customers to relinquish privacy rights in order to purchase broadband services, or other telecommunications services, would also constitute unjust and unreasonable discrimination in violation of section 202(a).[863] A take-it-or-leave-it offering would discriminate unreasonably by offering the service to potential customers willing and able to relinquish privacy rights that consumers expect and deserve, and/or that are guaranteed to them under sections 222 and 201, and not offering the service to others. Consumers should not have to face such a choice. In the *2015 Open Internet Order*, we explained that with respect to BIAS services, we will evaluate whether a practice is unjust, unreasonable, or unreasonably discriminatory using the no-unreasonable interference/disadvantage standard (general conduct rule).[864] Under this standard, the Commission can prohibit, on a case-by-case basis, practices that unreasonably interfere with or unreasonably disadvantage the ability of consumers to reach the Internet content, services, and applications of their choosing.[865] In evaluating whether a practice satisfies this rule, we consider a totality of the circumstances, looking to a non-exhaustive list of factors. Among these factors are end-user control, free expression, and consumer protection.

### 2. Heightened Requirements for Financial Incentive Practices

298. Unlike the "take-it-or-leave-it" offers for BIAS discussed above, the record concerning financial incentives practices is more mixed. There is strong agreement among BIAS providers, some public interest groups, and other Internet ecosystem participants that there are benefits to consumers and

[860] 47 U.S.C. § 222(a).

[861] 47 U.S.C. § 222(c)(1).

[862] 47 U.S.C. § 201(b) (requiring that all charges, practices, classifications, and regulation for and in connection with a telecommunications service be "just and reasonable," and prohibiting "unjust and unreasonable" charges, practices, classifications, or regulations). Thus, we disagree with CTIA's assertions that the "term 'approval' must reflect the common law contract law principle that neither take-it-or-leave-it offers nor financial inducements are unconscionable." CTIA Reply at 29, n.102. Congress directed the Commission to "execute and enforce" the provisions of the Act, including the prohibition on "unjust or unreasonable" practices.

[863] 47 U.S.C. § 202(a) ("It shall be unlawful for any common carrier to make any unjust or unreasonable discrimination in charges, practices, classifications, regulations, facilities, or services for or in connection with like communication service, directly or indirectly, by any means or device, or to make or give any undue or unreasonable preference or advantage to any particular person, class of persons, or locality, or to subject any particular person, class of persons, or locality to any undue or unreasonable prejudice or disadvantage."); *see Broadband Privacy NPRM*, 31 FCC Rcd at 2593, para. 294, 2596, paras. 305-06.

[864] *2015 Open Internet Order*, 30 FCC Rcd at 5659-60, paras. 133-37.

[865] *2015 Open Internet Order*, 30 FCC Rcd at 5659, para. 135. The no-unreasonable interference/disadvantage standard requires that "Any person engaged in the provision of broadband Internet access service, insofar as such person is so engaged, shall not unreasonably interfere with or unreasonably disadvantage (i) end users' ability to select, access, and use broadband Internet access service or the lawful Internet content, applications, services, or devices of their choice, or (ii) edge providers' ability to make lawful content, applications, services, or devices available to end users. Reasonable network management shall not be considered a violation of this rule." *Id.* at 5609, para. 21. *See also* 47 CFR § 8.11, No unreasonable interference or unreasonable disadvantage standard for Internet conduct.

companies of allowing BIAS providers the flexibility to offer innovative financial incentives.[866] The record does, however, reflect concerns that these programs may be coercive or predatory in persuading consumers to give up their privacy rights.[867] We therefore find that that heightened disclosure and affirmative customer consent requirements will help to ensure that customers' decisions to share their proprietary information in exchange for financial incentives are based on informed consent.[868]

299. As we recognized in the *Broadband Privacy NPRM*, it is not unusual for business to give consumers benefits in exchange for their personal information. For example, customer loyalty programs that track consumer purchasing habits online and in the brick-and-mortar world are commonplace.[869] Moreover, the Internet ecosystem continues to innovate in ways to obtain consumer information such as earning additional broadband capacity, voice minutes, text messages, or even frequent flyer airline miles in exchange for personal information.[870] Discount service offerings can benefit consumers.[871] As MMTC

[866] *See, e.g.*, AT&T Comments at 59 ("Banning discounts in exchange for information-sharing would, by definition, increase the price and lower the output of any affected service, including broadband Internet access."); ADTRAN Comments at 12 (arguing that financial incentive "business models of providing discounts in return for access to consumers' proprietary information have been well-received by consumers both in the bricks-and-mortar world, as well as specifically in the provision of BIAS services where they have been offered as an option"); CDT Comments at 3 (asserting that BIAS providers should have flexibility under the rules to encourage customer opt-in, "including offering monetary rewards in exchange for customer opt-in"); CenturyLink Comments at 30 (stating that "any outright prohibition adopted by the Commission would disserve consumers, who might miss out on services they want and value propositions they appreciate"); Free State Foundation Comments at 9 (arguing a ban on financial incentives would "deprive consumers of their choice to enjoy free or . . . inexpensive services and applications"); NTCA Comments at 71-72 ("Providers should have the flexibility, within the boundaries of notice, choice and security, to offer consumers packages that meet their needs."); Cincinnati Bell Comments at 10 ("Once the basic privacy requirements are established on such a basis, the Commission should not prohibit BIAS providers from offering enhanced levels of security for customers who are willing to pay the extra cost that is necessary to support such services."); Sprint Comments at 20-21; T-Mobile Comments at 44; Comcast Reply at 18-19; CTIA Aug. 25, 2016 *Ex Parte* at 2-3 (arguing that financial incentives "can lead to significant cost savings for all consumers, enable more valuable services for consumers, and mirror much of the economic activity that consumers expect"); *see also id*. Attach., ITIF White Paper, Why Broadband Discounts for Data are Pro-Consumer.

[867] *See, e.g.*, Consumer Watchdog Comments at 6 (arguing that "'pay-for-privacy' polices can rapidly become coercive and predatory, especially when applied to lower-income subscribers"); Consumer Action Comments at 2 (urging the Commission "to do everything in its power to ensure that companies don't snare consumers to wittingly or unwittingly give up their privacy rights in exchange for free services or devices"); EFF Comments at 9 (expressing concern that financial incentive practices "are prone to abuse"); EPIC Comments at 25-26; OTI Comments at 45 (explaining that financial incentive "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"); California AG Comments at 4 ("Consumers *pay* their ISPs for their Internet connection; they do not and should not be expected to also 'pay' with their personal information as well"); Common Sense Kids Action Comments at 14 (emphasizing that "[p]rivacy should not be a privilege reserved for those with time, money, and technical expertise"); Letter from Ariel Fox Johnson, Senior Policy Counsel, Common Sense Kids Action, to Marlene H. Dortch, Secretary, FCC, WC 16-106, at 1 (filed Sept. 9, 2016); Color of Change Oct. 20, 2016 *Ex Parte* at 5.

[868] We limit the heightened disclosure and consent requirements discussed herein to financial incentive practices offered by BIAS providers. The record reveals concerns about these practices specific to BIAS, and as such, we limit our requirements to such services.

[869] *Broadband Privacy NPRM*, 31 FCC Rcd at 2581, para. 258; Consumers' Research Comments at 8 (stating that many consumers exchange financial incentives for consent, "based on their own preferences").

[870] *See* TPI Comments, Attach., Thomas Lenard and Scott Wallsten White Paper, An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking at 35-36 (discussing Freedompop, which allows subscribers to earn additional broadband capacity, voice minutes, or text messages by performing specified actions with their third party advertisers (e.g., completing a questionnaire or purchasing a product or service); *see also* Chantal Tode, Flyers on

(continued….)

explains, for example, such programs "significantly drive online usage" as well as "help financially challenged consumers."[872]

300. At the same time, the record includes legitimate concerns that financial incentive practices can also be harmful if presented in a coercive manner, mislead consumers into surrendering their privacy rights, or are otherwise abused.[873] This is particularly true, because as CFC has explained, "consumers have difficulty placing a monetary value on privacy" and often "have little knowledge of the details or extent of the personally identifiable data that is collected or shared by their BIAS providers and others."[874] Commenters also raise concerns about the potential disproportionate effect on low income individuals.[875] Thirty-eight public interest organizations expressed concern that financial incentives can result in consumers paying up to $800 per year—$62 per month—for plans that protect their privacy.[876]

301. Mindful of the potential benefits and harms associated with financial incentive practices, we adopt heightened disclosure and choice requirements, which will help ensure consumers receive the information they need to fully understand the implications of any such practices and make informed decisions about exchanging their privacy rights for whatever benefits a provider is offering.[877] We therefore require BIAS providers offering financial incentives in exchange for consent to use, disclose,

(Continued from previous page)
United, American can now exchange location data for miles, Mobile Marketer (Aug. 22, 2016), http://www.mobilemarketer.com/cms/news/database-crm/23473.html.

[871] *See supra* note 866.

[872] MMTC et al. Comments at 8; *see also* APPI Comments at 3 ("If the Commission were to prohibit financial inducements that were designed to support low-income broadband adoption, more vulnerable AAPI consumers would be deterred from online use.").

[873] *See supra* note 867.

[874] CFC Comments at 9.

[875] ACLU Comments 6 (asserting that "the underprivileged (and disproportionately minority) population that lacks the discretionary income to devote to privacy will lose a right available for purchase by more affluent Americans"); NBCSL Comments at 1 (expressing concern about financial incentive practices for "people of color and low income consumers" because they "face particular risks to their privacy from companies that offer free or low cost services that actually come at the cost of giving up control of personal data"); Public Knowledge et al. Comments at 2 ("In households with low income elasticity, even moderate price discrimination between privacy and no-privacy offerings can become coercive inducements. Such inducements could force low-income consumers to choose between exercising their privacy rights, and having a broadband connection at all.").

[876] Letter from Access Humboldt, et al. to Tom Wheeler, Chairman, FCC, WC Docket No. 16-106 at 5 (filed Sept. 7, 2016), citing Karl Bode, *Think Tank Argues that Giving up Privacy is Good for the Poor*, Techdirt (Aug. 18, 2016), https://www.techdirt.com/articles/20160816/07164935254/think-tank-argues-that-giving-up-privacy-is-good-poor.shtml) ("AT&T charges its U-Verse broadband customers $528 to $792 more every year (up to $62 more per month) to opt out of the company's Internet Preferences program, which uses deep packet inspection to track your online behavior -- down to the second. Not only is that not anything close to a discount, but AT&T makes opting out as cumbersome as possible.")).

[877] CDT Comments at 3 ("However, because such inducements to consent raise serious public policy concerns, these programs must be transparent and must not be coercive."); *see also* CenturyLink Comments at 30 (arguing the Commission should allow "properly informed customers" to "voluntarily [] enter contracts for lower monthly rates or to accept other financial inducements in exchange for their consent to the use and/or sharing of their information"); Letter from Jon Leibowitz to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1 (filed May 10, 2016) ("So long as broadband providers provide sufficient notice, consumers [] have the ability to make informed choices about how they value their personal data."); Greenlining Institute Comments at 14 ("There is nothing wrong with a consumer, after being fully informed, choosing to trade access to his or her personal data in return for enhanced services."); MMTC et al. Comments at 8 (arguing that "financial inducement programs that require informed consent should not be seen as presumptively coercive").

and/or permit access to customer PI to provide a clear and conspicuous notice of the terms of any financial incentive program that is explained in a way that is comprehensible and not misleading.[878] That explanation must include information about what customer PI the provider will collect, how it will be used, with what types of entities it will be shared and for what purposes.[879] The notice must be provided both at the time the program is offered and at the time a customer elects to participate in the program. BIAS providers must make financial incentive notices easily accessible and separate from any other privacy notifications and translate such notices into a language other than English if they transact business with customers in that language. When a BIAS provider markets a service plan that involves an exchange of personal information for reduced pricing or other benefits, it must also provide at least as prominent information to customers about the equivalent plan without exchanging personal information.

302. BIAS providers must also comply with all notice requirements in Section 64.2003 of our rules when providing a financial incentive notice.[880] Because of the potential for customer confusion and in keeping with our overarching goal of giving customers control over the use and sharing of their personal information, we further require BIAS providers to obtain customer opt-in consent for participation in any financial incentive program that requires a customer to give consent to use of customer PI.[881] Consistent with the choice framework we adopt today, once customer approval is given, BIAS providers must provide a simple and easy-to-use mechanism that enables customers to change their participation in such programs at any time. This mechanism, which may be the same choice mechanism as the one in Part III.D.4, must be clear and conspicuous and in language that is comprehensible and not misleading. The mechanism must also be persistently available on or through the carrier's website; the carrier's application, if it provides one for account management purposes; and any functional equivalent of either. If a carrier does not have a website, it must provide its customers with a persistently available mechanism by another means such as a toll-free telephone number. We find that the protections outlined herein will encourage consumer choice in evaluating whether to take advantage of financial incentive programs.[882]

303. We will closely monitor the development of financial incentive practices, particularly if allegations arise that service prices are inflated such that customers are essentially compelled to choose between protecting their personal information and very high prices. We caution that we reserve the right to take action, on a case-by-case basis, under Sections 201 and 222 against BIAS providers engaged in

[878] Notices that contain material misrepresentations or omissions will not be considered accurate.

[879] CDT Comments at 25.

[880] *See supra* Part III.C.

[881] We observe that BIAS providers are already requiring opt-in consent for financial incentive programs. *See* U-verse with AT&T GigaPower Internet Preferences, AT&T, https://www.att.com/esupport/article.html#!/u-verse-high-speed-internet/KM1011211 (last visited Sept. 12, 2016) (website has been taken down); *see also* Adria Tomaszewski, *Verizon Smart Rewards Gives Back to Wireless Customers* (July 21, 2014), http://www.verizonwireless.com/news/article/2014/07/smart-rewards-gives-back-to-wireless-customers.html?null ("Customers may be required to enroll in Verizon Selects, part of Precision Market Insights from Verizon, as part of the Smart Rewards registration process and will receive 2,500 bonus points for being part of Verizon Selects and 500 Rewards points per participating line each month."); Torod Neptune, *How Verizon Selects from Verizon Wireless Works* (Dec. 3, 2012), http://www.verizonwireless.com/news/article/2012/12/verizon-selects.html ("We are asking customers to opt-in to Verizon Selects because of the types of information being used and because the capabilities provided to third-party marketers gives them the ability to reach customers directly with more relevant infomation[*sic*].").

[882] Mobile Futures Comments at 7 ("The FCC should not adopt paternalistic rules that deprive consumers of the choice to voluntarily share personal information in exchange for benefits."); Comcast Comments at 58 (arguing that the Commission should not take a "paternalistic view of 'consumers' ability to make informed choices"); Public Knowledge White Paper at 64 ("Congress clearly intended that consumers should have control of their own information.").

financial incentive practices that are unjust, unreasonable, unreasonably discriminatory, or contrary to Section 222. The approach we take today enables BIAS providers the flexibility to experiment with innovative financial incentive practices while ensuring that such practices are neither predatory nor coercive.

### H. Other Issues

#### 1. Dispute Resolution

304. In the *Broadband Privacy NPRM* we sought comment on whether our current informal complaint resolution process is sufficient to address customer concerns or complaints with respect to our proposed privacy and data security rules.[883] At present, customers who experience violations of any of our rules may file informal complaints through the Consumer Inquiries and Complaints Division of the Consumer & Governmental Affairs Bureau, and carriers may not require customers to waive, or otherwise restrict their ability to file complaints with or otherwise contact the Commission regarding violations of their privacy rights.[884] The record does not demonstrate a need to modify our complaint process for purpose of the rules we adopt today.[885]

305. On the question of whether BIAS providers should adopt specific dispute resolution processes, we received significant feedback both in support of[886] and in opposition to[887] limitations on mandatory arbitration agreements. Based on that record, we continue to have serious concerns about the impact on consumers from the inclusion of mandatory arbitration requirements as a standard part of many contracts for communications services. The time has come to address this important consumer protection issue in a comprehensive way. Therefore, we will initiate a rulemaking on the use of mandatory arbitration requirements in consumer contracts for broadband and other communications services, acting on a notice of proposed rulemaking in February 2017. We observe that the Consumer Financial Protection Bureau (CFPB)—which has extensive experience with consumer arbitration agreements and dispute resolution mechanisms—issued a report last year on mandatory arbitration clauses and is currently engaged in a rulemaking on the subject in the consumer finance context.[888] We expect that

---

[883] *Broadband Privacy NPRM*, 31 FCC Rcd at 2586-88, paras. 273-75.

[884] *See* 47 U.S.C. § 208; 47 CFR §§ 1.716 to 1.719; FCC, Consumer Help Center, https://consumercomplaints.fcc.gov/hc/en-us (last visited Oct. 5, 2016); *GS Texas Ventures, LLC*, Order, 29 FCC Rcd 10541, 10543, para. 6 (WCB 2014) (invalidating an arbitration clause precluding formal complaints to the Commission); Letter from National Association of Consumer Advocates (NACA), Public Justice, Public Citizen, Public Knowledge, AAJ, and Consumers Union to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 (filed Sept. 21, 2016) (discussing need to protect the Commission's complaint procedures from contractual waivers); *see also 2015 Open Internet Order*, 30 FCC Rcd at 5718, para. 267 n.687 (permitting mandatory third-party arbitration "so long as it is subject to *de novo* review by the Commission").

[885] *See* OTI Comments at 47 ("[T]he FCC should ensure that there is an easy and clear process for consumer complaints at the FCC."); WISPA Comments at 34-36.

[886] *See* AAJ Comments at 1-3, 6; Consumer Federation of California Comments at 12; Consumers Union Reply at 6; EPIC Comments at 27; NACA, Public Citizen, and 22 Other Public Interest Organizations Comments at 2-8; OTI Comments at 46; Privacy Rights Clearinghouse Comments at 7; Letter from Dallas Harris, Policy Fellow, Public Knowledge to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1 (filed Aug. 3, 2016); Smithwick & Belendiuk, P.C. Comments 1-11. *See also* Letter from 38 Public Interest Organizations to Chairman Tom Wheeler, Sept. 7, 2016, at 4-5.

[887] *See* AT&T Comments at 114-15; Comcast Reply at 53-55; Consumers' Research Comments at 5-6; CTIA Comments at 50-59; ITTA Comments at 24-25; NCTA Reply at 64-65; Sprint Comments at 20-21; T-Mobile Comments at 55; Verizon Reply at 38-45.

[888] *See* CFPB, Arbitration Agreements, 81 Fed. Reg. 32830 (May 24, 2016); *Arbitration Study*, CFPB (Mar. 10, 2015), http://www.consumerfinance.gov/data-research/research-reports/arbitration-study-report-to-congress-2015/.

(continued….)

many of the lessons the CFPB learns and the conclusions it draws in its rulemaking will be informative and useful.

### 2. Privacy and Data Security Exemption for Enterprise Voice Customers

306. Having harmonized the current rules for voice services with the rules we adopt today for BIAS, we revisit and broaden the existing exemption from our Section 222 rules for enterprise voice customers, where certain conditions are met. Specifically, we find that a carrier that contracts with an enterprise customer for telecommunications services other than BIAS need not comply with the other privacy and data security rules under Part 64, Subpart U of our rules if the carrier's contract with that customer specifically addresses the issues of transparency, choice, data security, and data breach; and provides a mechanism for the customer to communicate with the carrier about privacy and data security concerns. As with the existing, more limited business customer exemption from our existing authentication rules, carriers will continue to be subject to the statutory requirements of Section 222 even where this exemption applies.[889]

307. Our existing voice rules include customer authentication obligations as a required data security practice, but allow business customers to bind themselves to authentication schemes that are different than otherwise provided for by our rules.[890] In adopting an alternative data security option for authenticating business customers, the Commission recognized that the privacy concerns of telecommunications customers are greatest "when using personal telecommunications service,"[891] and "businesses are typically able to negotiate the appropriate protection of CPNI in their service agreements."[892] As Level 3 argues in this rulemaking, business customers have the "knowledge and bargaining power necessary to contract for privacy and data security protections that are tailored to meet their needs."[893] Moreover, business customers may have different privacy and security needs and therefore different expectations.[894] For example, Verizon explains that "many businesses may want their CPNI used in different ways than a typical consumer."[895] Allowing sophisticated enterprise customers to

(Continued from previous page)
*See also* Consumer Federation of California Comments at 12 (discussing the CFPB report); CTIA Comments at 54 (same); AAJ Comments at 4-5 (discussing the CFPB's report and NPRM).

[889] *See* 47 U.S.C. § 222; *see also* Level 3 Comments at 5 (noting that even with an enterprise exemption, the Commission would retain the power to evaluate providers' compliance with Section 222 and to bring enforcement actions where necessary); *2007 CPNI Order*, 22 FCC Rcd at 6942-43, para. 25.

[890] *See* 47 CFR § 64.2010(g).

[891] *See 2007 CPNI Order*, 22 FCC Rcd at 6943, para. 25 (determining that carriers who contract with enterprise customers need not comply with the Commission's carrier authentication rules so long as the carrier's contracts with its business customers (1) are serviced by dedicated account representatives as the primary contacts, and (2) specifically address the carrier's protection of CPNI).

[892] *See id*.

[893] Level 3 Comments at 3; *see also* XO Comments at 5 (noting that the business customers it serves negotiate service-level agreements with various privacy and data protection provisions based on individual customer needs).

[894] *See* Level 3 Comments at 4 (stating that, because enterprise service is not personal service, "end users in the enterprise context do not have the same expectation of privacy in the use of the service and are not expected to risk exposing private information the way individual, mass-market consumers using their personal phones might"); Verizon Comments at 63 (noting that the Commission has "sensibly recognized that the privacy rules that apply to consumers may not make sense for businesses"); Letter from Nicholas G. Alexander, Associate General Counsel, Federal Affairs, Level 3 Communications, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 at 1 (filed Aug. 5, 2016) (Level 3 Aug. 5, 2016 *Ex Parte*); *see also* XO Comments at 3.

[895] Verizon Comments at 63; *see al*so Verizon Oct. 13, 2016 *Ex Parte* at 1 (arguing the Commission should allow "business customers to bind themselves to alternative privacy and data security regimes as their privacy and data security needs may differ from those of consumers.").

negotiate their own privacy and data security protections with their carriers will "allow businesses to tailor how a telecommunications service provider protects their privacy and data specifically to their individual needs"[896] and allow carriers "to compete by offering innovative pro-customer options and contracts that meet business customers' privacy and data security expectations."[897] Although the Commission previously limited the enterprise exemption to authentication, for the reasons above we are convinced to broaden the exemption to encompass all privacy and data security rules under Section 222 for the provision of telecommunications services other than BIAS to enterprise customers.[898]

308. To ensure that business customers have identifiable protections under Section 222, we limit the business customer exemption to circumstances in which the parties' contract addresses the subject matter of the exemption and provides a mechanism for the customer to communicate with the carriers about privacy and data security concerns.[899] The existing exemption applies only if the parties' contract addresses authentication; in light of the broader scope of the exemption we adopt today, we now limit the exemption to circumstances in which the parties' contract addresses transparency, choice, data security, and breach notification.[900] We reject the contention that we should exempt enterprise services from our rules entirely with regard to the two limitations above.[901] The existence of contractual terms between two businesses addressing privacy ensures that the enterprise customer's privacy is in fact protected without the need for our rules.[902] In this regard, as XO observes, an enterprise carrier would "face significant liability if it violated contractual terms governing privacy and data security."[903] We do not provide a business exemption for BIAS services purchased by enterprise customers, because BIAS services by definition are "mass market retail service[s]," and as such we do not anticipate that it will be typical for purchasers to negotiate the terms of their contracts.

309. Regardless of whether the exemption applies, we observe that carriers remain subject to the statutory requirements of Section 222. This exemption in our rules is thus not tantamount to forbearance from the statute. We agree with commenters that Section 222 provides a solid legal foundation for carriers and sophisticated business customers to negotiate adequate and effective service terms on matters of privacy and data security.[904]

---

[896] Level 3 Aug. 5, 2016 *Ex Parte* at 1.

[897] INCOMPAS et al. Aug. 4, 2016 *Ex Parte* at 2.

[898] *See* 47 CFR § 64.2010(g); *2007 CPNI Order*, 22 FCC Rcd at 6943-44, para. 25.

[899] *See* Christopher L. Shipley, Attorney & Policy Advisor, INCOMPAS, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Oct. 21, 2016) (INCOMPAS Oct. 21, 2016 *Ex Parte*).

[900] *See* Level 3 Aug. 5, 2016 *Ex Parte* at 1 ("[W]e agreed that it would be reasonable for the Commission to adopt a general rule that requires carriers to address customer choice, transparency, data security, and data breach notification when selling to business customers so long as that rule does not specify how carriers are obligated to meet that requirement.").

[901] *See* INCOMPAS et al. Aug. 4, 2016 *Ex Parte* at 1 (stating that the *Notice* "asserts that BIAS is a mass market retail service and that proposed rules would apply only to mass market customer relationships" and that the Commission should "adopt the same approach in the context of" voice services).

[902] We clarify that the contract at issue need not be a fully negotiated agreement, but can take the shape of standard order forms. *See* INCOMPAS Oct. 21, 2016 *Ex Parte* at 2.

[903] *See* XO Comments at 5.

[904] *See* INCOMPAS et al. Aug. 4, 2016 *Ex Parte* at 1; *see also* Level 3 Comments at 5 (stating that, under the strictures of Section 222, enterprise service providers would still be required to protect customer information, limit their use of carrier information and protect its confidentiality, and obtain customer approval – or infer customer approval when it is clearly warranted under the circumstances – before using, disclosing, or permitting access to CPNI for any reason other than providing voice services, or services necessary to or used in the provision of voice service, unless a statutory exemption applies).

## I. Implementation

310. To provide certainty to customers and carriers alike, in this section we establish a timeline by which carriers must implement the privacy rules we adopt today. Until these rules become effective, Section 222 applies to all telecommunications services, including BIAS, and our current implementing rules continue to apply to telecommunications services other than BIAS and to interconnected VoIP. Below, we explain when the rules we adopt will be effective, and address how carriers should treat customer approvals to use and share customer PI received before the new rules are effective. Finally, we establish an extended implementation period for small providers with respect to the transparency and choice requirements we adopt today.

### 1. Effective Dates and Implementation Schedule for Privacy Rules

311. Swift implementation of the new privacy rules will benefit consumers. Moreover, carriers that have complied with FTC and industry best practices will be well-positioned to achieve prompt compliance with the privacy rules we adopt today. We recognize, however, that carriers will need some time to update their internal business processes as well as their customer-facing privacy policies and choice mechanisms in order to come into compliance with some of our new rules.[905] Additionally, some of the new rules will require revised information collection approval from the Office of Management and Budget pursuant to the Paperwork Reduction Act (PRA approval), and it is difficult to predict the exact timeline for PRA approval.[906] We therefore adopt a set of effective dates for the new rules that is calibrated to the changes carriers will need to make to come into compliance – providing a minimum timeframe before which the rules could come into effect. In order to provide certainty about effective dates, we also direct the Wireline Competition Bureau (Bureau) to provide advance notice to the public of the precise date after PRA approval when the Commission will begin to enforce compliance with each of the new rules.

312. *Notice and Choice*. The notice and choice rules we adopt today will become effective the later of (1) PRA approval, or (2) twelve months after the Commission publishes a summary of the Order in the Federal Register.[907] We acknowledge that our new notice and choice rules may "represent a significant shift in the status quo" for carriers.[908] Carriers will need to analyze the new, harmonized privacy rules as well as coordinate with various business segments and vendors, and update programs and policies.[909] Carriers will also need to engage in consumer outreach and education. These implementation steps will take time and we find, as supported in the record, that twelve months after publication of the Order in the Federal Register is an adequate minimum implementation period to implement the new notice and approval rules. In order to provide certainty, we also direct the Bureau to release a public notice after PRA approval of the notice and choice rules, indicating that the rules are effective, and giving carriers a time period to come into compliance with those rules that is the later of (1) eight weeks from the date of the public notice, or (2) twelve months after the Commission publishes a summary of the Order in the Federal Register.

313. *Breach Notification Procedures*. The data breach notification rule we adopt today will become effective the later of (1) PRA approval, or (2) six months after the Commission publishes a summary of the Order in the Federal Register.[910] We find that six months is an appropriate minimum

[905] *See* Verizon Sept. 23, 2016 *Ex Parte* at 1; *see also* T-Mobile Sept. 13, 2016 *Ex Parte* at 1.

[906] PRA approval, as defined herein, is not complete until the Commission publishes notice of OMB approval in the Federal Register.

[907] *See infra* Appx. A, 47 CFR §§ 64.2003-64.2005. This implementation schedule also applies to the disclosure and consent requirements for financial incentive practices. *See id*., § 64.2011(b).

[908] T-Mobile Sept. 13, 2016 *Ex Parte* at 1.

[909] *See id*. at 2, n.1; *see also* Verizon Sept. 23, 2016 *Ex Parte* at 1.

[910] *See infra* Appx. A, 47 CFR § 64.2008.

implementation period for data breach implementation. Although providers of telecommunications services other than BIAS are subject to our current breach notification rule[911] and we are confident that carriers are cognizant of the importance of data breach notification in the appropriate circumstances,[912] we recognize that carriers may have to modify practices and policies to implement our new rule, we find the harm trigger we adopt and timeline for notifying customers lessen the implementation requirements.[913] Moreover, harmonization of our data breach rule for BIAS and voice services enable providers to streamline their notification processes, which should also lessen carriers' need for implementation time. Given these steps to minimize compliance burdens, we find six months is an adequate minimum timeframe. We also direct the Bureau to release a public notice after PRA approval of the data breach rule, indicating that the rule is effective, and giving carriers a time period to come into compliance with the rule that is the later of (1) eight weeks from the date of the public notice, or (2) six months after the Commission publishes a summary of the Order in the Federal Register.

314. *Data Security*. The specific data security requirements we adopt today will become effective 90 days after publication of a summary of the Order in the Federal Register.[914] We find this to be an appropriate implementation period for the data security requirements because as discussed above, carriers should already be largely in compliance with these requirements because the reasonableness standard adopted in this Order provides carriers flexibility in how to approach data security and resembles the obligation to which they were previously subject pursuant to Section 5 of the FTC Act.[915] We therefore do not think the numerous steps outlined by commenters that would have been necessary to comply with the data security proposals in the *NPRM* apply to the data security rule that we adopt.[916] Nevertheless, we encourage providers, particularly small providers, to use the adoption of the Order as an opportunity to revisit their data security practices and therefore provide an additional 90 days subsequent to Federal Register publication in which carriers can revisit their practices to ensure that they are reasonable, as provided for in this Order.

315. *Prohibition on Conditioning Broadband Service on Giving up Privacy*. The prohibition on conditioning offers to provide BIAS on a customer's agreement to waive privacy rights will become effective 30 days after publication of a summary of this Order in the Federal Register.[917] We find that unlike the other privacy rules, consumers should benefit from this prohibition promptly. As discussed above, we find that these "take-it-or-leave-it" offers give consumers no choice and require them to trade their privacy for access to the Internet. As supported in the record, these practices would harm consumers, particularly lower-income customers.[918] We therefore find no basis for any delay in the effective date of this important protection. Further, prompt implementation will not create any burdens for carriers that are committed to providing their customers with privacy choices. All other privacy rules adopted in the Order will be effective 30 days after publication of a summary of the Order in the Federal Register.

---

[911] 47 CFR § 64.2011.

[912] *See TerraCom NAL*, 29 FCC Rcd at 13339-41, paras. 39-44.

[913] *See supra* Part III.F.1.

[914] *See infra* Appx. A, 47 CFR § 64.2007.

[915] *See supra* Part III.E; *see also* 15 U.S.C. § 45.

[916] *See, e.g.*, T-Mobile Sept. 13, 2016 *Ex Parte* at 1 (asking the Commission to consider "a 12-18 month implementation time period after rules are adopted"); *see also* T-Mobile Oct. 14, 2016 *Ex Parte*, Attach. at 3; Verizon Sept. 23, 2016 *Ex Parte* at 1 (arguing that the implementation steps "will take a significant amount of time to complete, requiring approximately 18 months from the date rules are adopted"); Verizon Oct. 13, 2016 *Ex Parte* at 1.

[917] *See infra* Appx. A, 47 CFR § 64.2011(a).

[918] *See supra* Part III.G.1.

### 2. Uniform Timeline for BIAS and Voice Services

316. We adopt a uniform implementation timetable for both BIAS and other telecommunications services. Implementing our rules for all telecommunications services simultaneously will help alleviate potential customer confusion from disparate practices between services or carriers. This approach will support the benefits of harmonization discussed throughout this Order and is strongly supported in the record.[919] We emphasize that until the new privacy rules are effective and implemented with respect to voice services, the existing rules remain in place. Further, we make clear that all carriers, including BIAS providers, remain subject to Section 222 during the implementation period that we establish and beyond.[920]

### 3. Treatment of Customer Consent Obtained Prior to the Effective and Implementation Date of New Rule

317. We recognize that our new customer approval rule[921] requires carriers to modify the way they obtain consent for BIAS and voice services based on our sensitivity-based framework discussed above.[922] We seek to minimize disruption to carriers' business practices and therefore do not require carriers to obtain new consent from all their customers.[923] Rather, for BIAS, we treat as valid or "grandfather" any consumer consent that was obtained prior to the effective date of our rules and that is consistent with our new requirements. For example, if a BIAS provider obtained a customer's opt-in consent to use that individual's location data to provide coupons for nearby restaurants and provided adequate notice regarding his or her privacy rights, then the customer's consent would be treated as valid. The consent would not be invalidated simply because it occurred before the new customer approval rule became effective. However, if the customer consent was not obtained in the manner contemplated by our new rule, a new opportunity for choice is required. We recognize that consumers whose opt-in or opt-out consent is grandfathered may not be aware of our persistent choice requirement,[924] and therefore we direct the Consumer and Governmental Affairs Bureau to work with the industry to engage in a voluntary consumer education campaign.

318. We decline to more broadly grandfather preexisting consents obtained by small BIAS providers.[925] We find that the parameters set forth above create the appropriate balance to limit

[919] *See supra* Part III.C.5 (explaining the benefits of harmonization, including consistency between privacy regimes for all telecommunications services, both to reduce possible consumer confusion, and to decrease compliance burdens for all affected telecommunications carriers, particularly small providers).

[920] *See Enf. Bur. Privacy Advisory*, 30 FCC Rcd 4849 (2015).

[921] *See infra* Appx. A, 47 CFR § 64.2004.

[922] *See supra* Part III.D.1.

[923] *See* WISPA Comments at 31 (arguing it should not "not be compelled to obtain new consents…from its customers."); ACA Comments at 45; CCA Comments at 33; NTCA Comments at 55; USTelecom Comments at 19.

[924] *See infra* Appx. A, 47 CFR § 64.2004 (c) ("A telecommunications carrier must make available a simple, easy-to-access method for customers to provide or withdraw consent at any time. Such method must be clearly disclosed, persistently available, and made available at no additional cost to the customer. The customer's action must be given effect promptly after the decision to provide or withdraw consent is communicated to the carrier.").

[925] *See* USTelecom Comments at 19 ("[W]e support allowing small providers who have already obtained customer approval to use their customers' proprietary information to grandfather in those approvals for first and third party uses."). WTA argues that the Commission should permit "small BIAS providers to grandfather existing opt-out approvals as it has done in the past" citing the Commission's *2002 CPNI Order*, in which the Commission allowed carriers to use preexisting opt-out approval with the limitation that such approval only be used for marketing of communications-related services by carriers, their affiliates that provide communications-related services, and carriers' agents, joint venture partners and independent contractors. *See* Letter from Patricia Cave, Director, Government Affairs, WTA, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 16-106 at 2 (filed Aug. 22, 2016); *see also 2002 CPNI Order*, 17 FCC Rcd at 14897, para. 85.

compliance costs with our new notice and customer approval rules while providing consumers the privacy protections they need. As we explain above, BIAS providers are in a unique position as gateways to the Internet and we need to ensure consumers are aware of their privacy rights and have the ability to choose how their personal information is used and shared.

319. As with BIAS services, customer consent obtained by providers of other telecommunications services subject to the legacy rules remains valid for the time during which it would have remained valid under the legacy rules. As such, opt-out consent obtained before the release date of this order remains valid for two years after it was obtained, after which a carrier must conform to the new rules.[926] Opt-in consent that is valid under the legacy rules remains valid. This approach is consistent with established customer expectations at the time the consent was solicited, and should reduce notice fatigue.[927] Maintaining the validity of customer consent for voice services will also help reduce the up-front cost of compliance of the new rules. We reiterate that a customer's preexisting consent is valid only within its original scope. For instance, if a carrier previously received a customer's opt-in consent to use information about the characteristics of the customer's service to market home alarm services, the carrier could not claim that same consent applies to use of different customer PI (e.g., a Social Security Number) or a different use or form of sharing (e.g., selling to a data aggregator). Similarly, opt-out consent to use and share CPNI to market communications-related services could not be used to support use of different customer PI or different forms of use or sharing (e.g., marketing non-communications-related services).

#### 4. Limited Extension of Implementation Period for Small Carriers

320. In the *NPRM* we sought comment on ways to minimize the burden of our proposed privacy framework on small providers,[928] and throughout this Order we have identified numerous ways to reduce burdens and compliance costs while providing robust privacy protections to their customers.[929] To further address the concerns raised by small providers in the record, we provide small carriers an additional twelve months to implement the notice and customer approval rules we adopt today.[930]

---

[926] *See* 47 CFR § 64.2008(a)(2).

[927] *See, e.g.*, CTA Comments at 11 (expressing concern that certain Commission proposals would induce notice fatigue); *see also* INCOMPAS Comments at 10 (arguing that notice fatigue will lessen the effectiveness of consumer notices).

[928] *See Broadband Privacy NPRM*, 31 FCC Rcd at 2553, para. 151.

[929] *See supra* Part III.C.5 (explaining that harmonizing our BIAS and voice definitions under Section 222 will simplify compliance for small providers who collect less customer information, use it for narrower purposes, and do not have the resources to maintain a bifurcated system); *see also supra* para. 14358 (eliminating the pre-existing every-two-year notice requirement from our Section 222 rules to reduce burdens smaller carriers); *supra* Part III.C.3 (declining to require a standardized format of privacy notices as it would decrease flexibility for small carriers); *id*. (only requiring providers to convey their notices of privacy policies to customers in another language, if the customer transacts business with the BIAS provider or other telecommunications carrier in that other language so as not to overburden small providers); *id.* (directing the CAC to develop a safe harbor standardized form, to be used by small providers if they choose so they can easily adopt a compliant form and format for their notices); *supra* para. 241 (clarifying that the data security standard is one of "reasonableness" rather than strict liability and establishing a non-exhaustive rather than prescriptive list of reasonable data security to allow easier compliance for small providers); *supra* Part III.F.1 (employing a harm-based trigger or data breaches to substantially reduce the burdens of smaller providers in reporting breaches of customer PI); *supra* Part III.F.3.a (changing the timeline for notifying customers of a data breach from 7-days to 30-days to allow more time for small providers to comply).

[930] CCA asserts that "any compliance burdens produced by privacy rules will be compounded by many additional regulations including Title II regulation, enhanced transparency rules, and outage reporting requirements." *See* CCA Oct. 13, 2016 *Ex Parte* at 2. Consideration of the effect of separate requirements was taken into account in developing this implementation plan.

321. We find that an additional one-year phase-in will allow small carriers—both broadband providers and voice providers—time to make the necessary investments to implement these rules.[931] The record reflects that small providers have comparatively limited resources and rely extensively on vendors over which they have limited leverage to compel adoption of new requirements.[932] We recognize our notice and choice framework may entail up- front costs for small providers. We also agree with NTCA that small providers will "be aided by observing and learning from the experience of larger firms who by virtue of their size and scale are better position to absorb the learning curve."[933] As such, we find that this limited extension is appropriate.

322. For purposes of this extension, we define small BIAS providers as providers with 100,000 or fewer broadband connections and small voice providers with 100,000 or fewer subscriber lines as reported on their most recent Form 477, aggregated over all the providers' affiliates. In the *NPRM* we sought comment on whether we should exempt carriers that collect data from fewer than 5,000 customers a year provided they do not share customer data with third parties.[934] Commenters objected that the 5,000 threshold was too narrow to accurately identify small providers and that the limitation on information sharing was too restrictive.[935] We therefore find that given the limited scope of relief granted to small carriers, increasing the numeric scope from the 5,000 to 100,000 is suitable because it will benefit additional providers without excess consumer impact. We also decline to count based on the number of customers from whom carriers collect data, as we recognize that some data collection is necessary to the provision of service.[936] Additionally, we decline to impose any requirement that small providers not share their information with third parties to qualify for the exception. Moreover, cabining the scope of this limited extension to providers serving 100,000 or fewer broadband connections or voice subscriber lines is consistent with the *2015 Open Internet Order*, in which we adopted a temporary exemption from the enhancements to the transparency rule for BIAS providers with 100,000 or fewer broadband subscribers.[937] Therefore for these reasons, and the critical importance of privacy protections to

[931] *See* CCA Reply Comments at 40-41 (advocating for 24-month extension after effective date of new privacy rules); *see also* WISPA Comments at 28-29 (same).

[932] *See* WISPA Comments at 28 ("This additional time will enable small providers to assess their obligations, budget for lawyers, consultants, train personnel, and establish internal systems to ensure compliance.") *see also* ACA Comments at 8 (arguing that "very few of these [small] providers have in-house technical or compliance personnel with extensive expertise in privacy and data security compliance. Some are forced to outsource some of their security functions to outside vendors at a significant cost").

[933] NTCA Oct. 14, 2016 *Ex Parte* at 4.

[934] *See Broadband Privacy NPRM*, 31 FCC Rcd at 2553, para. 151.

[935] *See, e.g.*, CCA Reply at 40-41 (advocating for 24-month extension after effective date of new privacy rules); WISPA Comments at 28-29 (same); U.S. Small Business Administration Reply at 4 (same); ACA Comments at 46 (arguing the Commission "should extend the effective dates for small providers to comply with any new privacy and data security rules by at least one year beyond any general compliance deadline"); RWA Comments at 4 (explaining that "certain customer information is shared with billing system vendors, workforce management system vendors, consultants that assist with certain projects, help desk providers, and system monitoring solutions providers").

[936] *See supra* Part III.D.2.a.

[937] *See 2015 Open Internet Order*, 30 FCC Rcd at 5677-78, para. 172; *see also Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order, 30 FCC Rcd 14162, 14166-67, para. 10 (CGB Dec. 15, 2015) (*Small BIAS Provider Transparency Extension Order*) (maintaining the 100,000 threshold for the small business extension as it "remains a reasonable basis to delineate which providers are likely to be most affected by the burden of complying with the enhanced disclosure requirements."); *Rural Call Completion*, WC Docket No. 13-39, Report and Order and Further Notice of Proposed Rulemaking, 28 FCC Rcd 16154, 16168-69, para. 27 (2013) (exempting smaller providers from the recording, retention, and reporting rules if they provide long-distance voice service that make the initial long-distance call path choice for less than 100,000 domestic retail subscriber lines (counting the total of all business and residential fixed subscriber lines and mobile phones and aggregated over all of the

(continued….)

consumers, we decline to adopt CCA's recommendation to define small BIAS providers as either companies with up to 1,500 employees or serving 250,000 subscribers or less.[938]

323. We decline to provide any longer or broader extension periods or exemptions to our new privacy rules.[939] We find that our "reasonableness" approach to data security mitigates small provider concern about specific requirements, such as annual risk assessments and requiring specific privacy credentials.[940] Moreover, as advocated by small carriers, we adopt a customer choice framework that distinguishes between sensitive and non-sensitive customer information, as well as decline to mandate a customer-facing dashboard to help manage their implementation and compliance costs.[941] Furthermore, we find our data breach notification requirements and "take-it-or-leave-it" prohibition do not require an implementation extension as compliance with these protections should not be costly for small carriers that generally collect less customer information and use customer information for narrower purposes. Also, although smaller in company size and market share, small carriers still retain the ability to see and collect customer personal information and therefore, it is appropriate to extend these important protections to all customers on an equal timeframe.

### J. Preemption of State Law

324. In this section, we adopt the proposal in the *NPRM* and announce our intent to preempt state privacy laws, including data security and data breach laws, *only* to the extent that they are inconsistent with any rules adopted by the Commission.[942] This limited application of our preemption authority is consistent with our precedent in this area.[943] We have long appreciated and valued the important role states play in upholding the pillars of privacy and protecting customer information.[944] As the Office of the New York Attorney General has explained, the State AGs are "active participants in ensuring that [their] citizens have robust privacy protections" and it is critical that they continue that

(Continued from previous page)
providers' affiliates)); RWA Reply at 5 (supporting the 100,000 threshold established in the *2015 Open Internet Order*).

[938] *See* CCA Oct. 13, 2016 *Ex Parte* at 1-2; *see also Small BIAS Provider Transparency Extension Order*, 30 FCC Rcd at 141266, para. 10 (declining to broaden the small provider threshold, as it would "substantially increase the number of consumers who would be temporarily excluded from receiving the information that the Commission has deemed essential for them to make informed choices about broadband services.").

[939] *See* WISPA Comments at 27-28 (seeking a two-year extension for all the Commission rules); CCA Reply at 40 ("If the Commission declines to adopt a small provider exemption . . . CCA urges the Commission to allot those providers an extension of time to comply with new regulations."); RWA Reply at 7 ("If the Commission declines to adopt these broader exemptions, RWA urges the adoption of a 24-month extended compliance deadline for small providers.").

[940] *See supra* Part III.E.1; *see also* WTA & Nex-Tech Apr. 25, 2016 *Ex Parte* at 2 (explaining how such data security proposals would unduly burden small carriers).

[941] *See supra* Part III.D.1 *see also supra* para. 230.

[942] *See Broadband Privacy NPRM*, 31 FCC Rcd at 2511, 2588 paras. 27, 276. State law includes any statute, regulation, order, interpretation, or other state action with the force of law.

[943] *See 1998 CPNI Order*, 13 FCC Rcd at 8075, para. 16 ("We conclude that, in connection with CPNI regulation, the Commission may preempt state regulation of intrastate telecommunications matters where such regulation would negate the Commission's exercise of its lawful authority . . . ."); *2002 CPNI Order*, 17 FCC Rcd at 14890-91, para. 70 ("Should states adopt CPNI requirements that are more restrictive than those adopted by the Commission, we decline to apply any presumption that such requirements would be vulnerable to preemption.").

[944] *See 2002 CPNI Order*, 17 FCC Rcd at 14891, para. 71 (observing that "our state counterparts . . . bring particular expertise to the table regarding competitive conditions and consumer protection issues in their jurisdictions, and privacy regulation, as part of general consumer protection, is not a uniquely federal matter"); *2007 CPNI Order*, 22 FCC Rcd at 6958, para. 60.

work.[945] As such, we further agree with the New York Attorney General's Office that "it is imperative that the FCC and the states maintain broad authority for privacy regulation and enforcement."[946] We also agree with those providers and other commenters that argue that neither telecommunications carriers nor customers are well-served by providers expending time and effort attempting to comply with conflicting privacy requirements.[947] We therefore codify a very limited preemption rule that is consistent with our past practice with respect to rules implementing Section 222. By allowing states to craft and enforce their own laws that are not inconsistent with our rules with respect to BIAS providers' and other telecommunications carriers' collection, use, and sharing of customer information, we recognize and honor the important role the states play in protecting the privacy of their customer information.

325. As the Commission has previously explained, we may preempt state regulation of intrastate telecommunications matters "where such regulation would negate the Commission's exercise of its lawful authority because regulation of the interstate aspects of the matter cannot be severed from regulation of the intrastate aspects."[948] In this case, we apply our preemption authority to the limited extent necessary to prevent such instances of incompatibility. Where state privacy laws do not create a conflict with federal requirements, providers must comply with federal law and state law.

326. As we have in the past, we will take a fact-specific approach to the question of whether a conflict between our privacy rules and state law exists.[949] If a provider believes that it is unable to comply

[945] Letter from Kathleen McGee, Chief, Bureau of Internet and Technology, New York Attorney General, to Chairman Tom Wheeler, FCC, WC Docket No. 16-106 at 4 (filed June 30, 2016) (NY Attorney General *Ex Parte*); *see also* Letter from Bill Schuette, Michigan State Attorney General, et al., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 at 1 (filed Sept. 15, 2016) ("As Attorneys General, we are always concerned with protecting consumers' privacy and defending the protections our consumers have been afforded via our various state laws. It is of paramount importance that any federal regulations not impair states' ability to vigorously protect their citizens as they deem appropriate."); Letter from Karl A. Racine, District of Columbia Attorney General, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 at 1 (filed Oct. 12, 2016).

[946] NY Attorney General *Ex Parte* at 4; *see also* California Office of Attorney General Reply at 2; PA PUC Reply at 4 (arguing that the Commission "should not preclude state authorities from developing privacy standards based upon independent state law so long as those standards do not unduly burden interstate commerce and advance a compelling state interest"); Greenlining Institute Comments at 51 (explaining that "neither federal nor state agencies have sufficient resources to fully protect consumers, and it is important that 'cooperative federalism' be maintained in this vital area").

[947] *See, e.g.*, Hughes Comments at 7 ("Hughes also supports the FCC preempting state privacy laws to the extent that they are inconsistent with any rules adopted by the Commission."); ViaSat Comments at 7 (agreeing with our adopted method, by stating for example, "that the Commission make clear that any data breach notification requirements adopted in this proceeding preempt all *inconsistent* state requirements") (emphasis added); CTIA Comments at 183 (arguing that the Commission should be clear "about the extent to which it would preempt state law requirements" so providers can avoid having to address conflicting state and federal notice requirements).

[948] *1998 CPNI Order*, 13 FCC Rcd at 8075-76, para. 16; *see also 2002 CPNI Order*, 17 FCC Rcd at 14890, para. 69. We reject ITTA's argument that we lack authority to preempt inconsistent state laws regarding non-CPNI customer PI because its argument is premised on the incorrect assumption that our legal authority under Section 222 is limited to CPNI. *See infra* Part IV.A.2 (concluding that the Commission has authority to reach customer PI under Section 222(a) of the Act); *contra* Letter from Michael J. Jacobs, Vice President Regulatory Affairs, ITTA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 3 (filed Aug. 9, 2016) ("State Attorneys General, furthermore, have jurisdiction . . . to enforce their own privacy and unfair practice laws, which the FCC would not be empowered to preempt in light of its own lack of statutory authority regarding non-CPNI consumer information.").

[949] The Commission reviews petitions for preemption of CPNI rules on a case-by-case basis. *See 2002 CPNI Order*, 17 FCC Rcd at 14893, para. 74 ("By reviewing requests for preemption on a case-by-case basis, we will be able to make preemption decisions based on the factual circumstances as they exist at the time and on a full and a complete record."); *see also id.* at 14890-93, paras. 69-74 (recognizing the potential burdens associated with different regulatory requirements); ViaSat Comments at 8 (expressing concern about being subject to "a potentially confusing patchwork of conflicting breach notification requirements at the state level").

simultaneously with the Commission's rules and with the laws of another jurisdiction, the provider should bring the matter to our attention in an appropriate petition. Examining specific conflict issues when they arise will best ensure that consumers receive the privacy protections they deserve, whether from a state source or from our rules.

327. The states have enacted many laws aimed at ensuring that their citizens have robust privacy protections.[950] We agree with the Pennsylvania Attorney General that it is important that we not "undermine or override state law providing greater privacy protections than federal law,"[951] or impede the critical privacy protections states continue to implement. Rather, as supported in the record, we encourage the states to continue their important work in the privacy arena, and adopt an approach to preemption that ensures that they are able to do so.[952] In so doing, we reaffirm the Commission's limited exercise of our preemption authority to allow states to adopt consumer privacy protections that are more restrictive than those adopted by the Commission provided that regulated entities are able to comply with both federal and state laws.[953]

328. In taking this approach, we reject ACA's suggestion that we should "preempt state data breach notification laws entirely."[954] As stated above, we continue to provide states the flexibility to craft and enforce their own privacy laws, and therefore we only preempt state laws to the extent that they impose inconsistent requirements. Our privacy rules are designed to promote "cooperative federalism" and therefore unless providers are unable to comply with both the applicable state and Commission requirements, we find it inappropriate to categorically preempt these state data breach laws.[955]

329. Commenters have identified data breach notification as one area where conflicts may arise. We agree with commenters that it is generally best for carriers to be able to send out one customer data breach notification that complies with both state and federal laws,[956] and we welcome state agencies to use our data breach notification rules as a model.[957] However, we recognize that states law may require differently timed notice or additional information than our rules, and we do not view such privacy-protective requirements as necessarily inconsistent with the rules we adopt today since carriers are capable of sending two notices at two different times. However, in the interest of efficiency and

[950] *See, e.g.*, California Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code § 22577(a); California Consumer Protection Against Computer Spyware Act, Cal. Bus. & Prof. Code § 22947.1(k); Cal. Civ. Code § 1798.82(h); Conn. Gen. Stat. § 36a-701b(a); N.Y. Gen. Bus. L. §§ 899-aa(1)(a), (b); La. Stat. § 51:3073(4); Fla. Stat. § 501.171(1)(g).

[951] PA PUC Reply at 2.

[952] *See, e.g.*, NY Attorney General *Ex Parte* at 4; *see also* National Consumers League Comments at 33-34 (stating our approach "will ensure that States will be able to continue to innovate in protecting consumers' data, set a high bar for consumer protection, and help to clarify the baseline that BIAS providers must adhere to").

[953] *See 2002 CPNI Order*, 17 FCC Rcd at 14890-92, paras. 69-71; *see also Broadband Privacy NPRM*, 31 FCC Rcd at 2588, para. 277.

[954] ACA Comments at 56-57; *see also* ACA Reply at 5.

[955] *See supra* note 946.

[956] State Privacy and Security Coalition Comments at 5 (arguing that "requiring notification in many situations that involve no risk of harm makes 'notice fatigue' more likely with consumers ignoring notice of serious breaches that actually create risk"); *see also* ACA Comments at 57 ("By reducing the number of government-level notifications that BIAS providers must make from over 50 notifications to a single notification, the Commission will significantly reduce the costs that BIAS providers must assume in the event of a breach while preserving the benefits of notifications to the customer.").

[957] *See* National Consumers League Comments at 34 (explaining that "[i]t is NCL's hope that the robust and comprehensive data security and breach notification set out by the FCC will also serve as a model for other states and agencies").

preventing notice fatigue, we invite carriers that find themselves facing requirements to send separate consumer data breach notices to fulfill their federal and state obligations to come to the Commission with a proposed waiver that will enable them to send a single notice that is consistent with the goals of notifying consumers of their data breach. Additionally, as explained by CTIA, a situation could arise where a state law enforcement agency requests a delay in data breach notice due to an ongoing investigation.[958] We encourage both carriers and state law enforcement officials to come to the Commission in such a situation, as we have authority to waive our rules for good cause and recognize the importance of avoiding interference with a state investigation.[959]

330. We clarify that we apply the same preemption standard to all aspects of our Section 222 rules. Although the Commission, in its previous orders, had applied its preemption standard with respect to all of the Section 222 rules, the preemption requirement is currently codified at Section 64.2011 of our rules, which addresses notification of data breaches.[960] Recognizing that states are enacting privacy laws outside of the breach notification context, and consistent with historical Commission precedent, we conclude that the preemption standard should clearly apply in the context of all of the rules we adopt today implementing Section 222. Therefore, as we proposed in the *NPRM*, we remove the preemption provision from that section of our rules, and adopt a new preemption section that will clearly apply to all of our new rules for the privacy of customer proprietary information.[961] In doing so, we enable states to continue their important role in privacy protection.

331. Further, we find that the same preemption standard should apply in both the voice and BIAS contexts to help provide certainty and consistency to the industry.[962] Accordingly, we adopt a harmonized preemption standard across BIAS and other telecommunications services.[963] By applying the same preemption standard to BIAS providers and to other telecommunications carriers, we ensure that states continue to serve a role in tandem with the Commission, regardless of the specific service at issue.

## IV. LEGAL AUTHORITY

332. In this Report and Order, we implement Congress's mandate to ensure that telecommunications carriers protect the confidentiality of proprietary information of and relating to customers. As explained in detail below, the privacy and security rules that we adopt are well-grounded in our statutory authority, including but not limited to Section 222 of the Act.[964]

### A. Section 222 of the Act Provides Authority for the Rules

333. Section 222 of the Act governs telecommunications carriers in their use, disclosure, and protection of proprietary information that they obtain in their provision of telecommunications services. The fundamental duty this section imposes on each carrier, as stated in Section 222(a), is to "protect the

[958] CTIA Comments at 183-84 (asking "would the Commission's [] rule for notice to customers trump that request?").

[959] *See* 47 U.S.C. § 1.3; *see also WAIT Radio v. FCC*, 418 F.2d 1153, 1159 (D.C. Cir. 1969) (waivers must show a deviation will serve the public interest).

[960] *See Broadband Privacy NPRM*, 31 FCC Rcd at 2602-03, para. 3; 47 CFR § 64.2011.

[961] *See Broadband Privacy NPRM*, 31 FCC Rcd at 2610, para. 4 (adding § 64.7007 Effect on State Law to new Subpart GG); *see also infra* Appx. A § 64.2012.

[962] *See* ACA Comments at 57 (supporting the creation of "a single privacy and data security framework for providers of multiple services as a means of reducing compliance burdens and consumer confusion"); *see also* WTA Reply at 19 (arguing that in complying with state and federal privacy regulations, "'[p]articularly for small providers, '[i]nevitability of parallel enforcement underscores the need for harmonization'").

[963] *See* 47 CFR Subpt. U; *see also Broadband Privacy NPRM*, 31 FCC Rcd at 2603-2610.

[964] 47 U.S.C. § 222; *see also* 47 U.S.C. § 201(b) ("The Commission may prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of this chapter.").

confidentiality of proprietary information of, and relating to" customers, fellow carriers, and equipment manufacturers.[965] Section 222(c) imposes more specific requirements with regard to a subset of customers' proprietary information, namely customer proprietary *network* information.[966] This Report and Order implements Section 222 as to customer PI, a category that includes individually identifiable CPNI and other proprietary information that is "of, and relating to" customers of telecommunications services. As explained below, the rules we adopt today are faithful to the text, structure, and purpose of Section 222.

### 1. Section 222 Applies to BIAS Providers Along With Other Telecommunications Carriers

334. We begin by reaffirming our conclusion in the *2015 Open Internet Order* that Section 222 applies to BIAS providers.[967] In so doing, we reject the view that Section 222 applies only to voice telephony.[968] The *2015 Open Internet Order* reclassified BIAS as a telecommunications service, making BIAS providers "telecommunications carriers" insofar as they are providing such service.[969] Section 222(a) imparts a general duty on "[e]very telecommunications carrier," while other subsections specify the duties of "a telecommunications carrier" in particular situations. The term "telecommunications carrier" has long included providers of services distinct from telephony, including at the time of Section 222's enactment. Thus, in construing the term for purposes of Section 222, we see no reason to depart from the definition of "telecommunications carrier" in Section 3 of the Act.[970] To the contrary, deviating from this definition without a clear textual basis in Section 222 would create uncertainty as to the scope of numerous provisions in the Act, regulatory imbalance between various telecommunications carriers, and a gap in Congress's multi-statute privacy regime. Moreover, commenters cite no evidence that the term "telecommunications carrier" is used more restrictively in Section 222 than elsewhere in the Act.

335. We similarly reject the claim that in reclassifying BIAS we have improperly exercised our "definitional authority" to expand the scope Section 222.[971] The relevant term that defines the scope of Section 222 is "telecommunications carrier,"[972] and we simply are applying the holding of the *2015 Open Internet Order* that this statutory term encompasses BIAS.[973] Nor does the fact that Section 230 of

[965] *See* 47 U.S.C. § 222(a). The provision reads in full: "Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier." *Id*.

[966] 47 U.S.C. § 222(c) (emphasis added).

[967] *See 2015 Open Internet Order*, 30 FCC Rcd at 5820, para. 462.

[968] *See, e.g.*, Comcast Comments at 67-68; NCTA Comments at 7-13; CTIA Comments at 19-22; USTelecom Comments at 28; U.S. Chamber of Commerce Comments at 4. *But see* Free Press Comments at 9 ("The logic for applying Section 222 to broadband is inexorable."); OTI Reply at 3-5; Free Press Reply at 5-7.

[969] *See 2015 Open Internet Order*, 30 FCC Rcd at 5615, para. 47; *see also USTA v. FCC*, 825 F.3d 674 (D.C. Cir. 2016) (upholding the *2015 Open Internet Order* in full).

[970] *See* OTI Reply at 4 ("It is presumed that use of a defined term retains its definition unless there is proof otherwise.").

[971] *See, e.g.*, NCTA Comments at 13; Comcast Comments at 68.

[972] *See* 47 U.S.C. § 222(a) ("Every telecommunications carrier has a duty . . ."), (c) ("[A] telecommunications carrier that receives or obtains . . .").

[973] *See 2015 Open Internet Order*, 30 FCC Rcd at 5615, para. 47.

the Act uses the term Internet, while Section 222 does not, compel us to disregard the clear uses of "telecommunications carrier" in Section 222.[974]

336. We also reject arguments that "telephone-specific references" contained in Section 222 serve to limit the scope of the entire section to voice telephony or related services.[975] This argument misconstrues the structure of Section 222. As explained in more detail below, Section 222(a) imposes a broad general duty to protect proprietary information while other provisions impose more-specific duties. Some of these more-specific duties concerning CPNI are indeed relevant only in the context of voice telephony.[976] But their purpose is to specify duties that apply in that limited context, not to define the outer bounds of Section 222.[977] The definition of CPNI found in Section 222(h)(1) illustrates this point. While the term is defined in Section 222(h)(1)(B) to include "the information contained in the bills pertaining to telephone exchange service or telephone toll service"[978] and to exclude "subscriber list information"[979]—categories that have no relevance for BIAS—pursuant to Section 222(h)(1)(A) the term CPNI also includes a broader category of information that carriers obtain by virtue of providing a telecommunications service.[980] This broader category articulated in Section 222(h)(1)(A) pertains to "telecommunications service[s]" in general, not only to telephony. As we have explained above, BIAS providers collect significant amounts of information that qualifies as CPNI under the broad, functional definition articulated in Section 222(h)(1)(A).[981] Whether BIAS providers also issue telephone bills or publish directories makes no difference. The reference to "call[s]" in Section 222(d)(3) is similarly inapposite as to the scope of Section 222 as a whole.[982] The "call[s]" at issue in this provision are customer service calls initiated by the customer; a customer of any service, including BIAS, can make such a call.

337. If anything, the placement of references to telephony in Section 222 supports our reading of that section as reaching *beyond* telephony. Such terms are used to define narrow provisions or exceptions, but not the outer contours of major components of the statute. Most significantly, the broad term "telecommunications carrier" is used in defining the general duty under subsection (a); the

[974] *See USTA v. FCC*, 825 F.3d at 702-03 (rejecting petitioners' Section 230-based argument against reclassification of BIAS as a telecommunications service). *But see* Comcast Comments at 67.

[975] *But see* Comcast Comments at 67.

[976] *See, e.g.*, 47 U.S.C. § 222(c)(3) (imposing a sharing condition on "local exchange carrier[s]", but not on other telecommunications carriers, in their use and disclosure of "aggregate customer information").

[977] We need not and do not construe BIAS as a "local exchange service," "telephone exchange service," or "telephone toll service" in order to bring it within the reach of Section 222. Provisions of the statute that apply only to such limited categories, or to carriers that provide services in such categories, are not part of the statutory basis for any rules we adopt in this Report and Order as to BIAS. Rather, the rules we adopt for BIAS are rooted only in those aspects of Section 222 that govern "telecommunications carriers" and "telecommunications services" writ large.

[978] *See* 47 U.S.C. § 222(h)(1)(B).

[979] *See* 47 U.S.C. § 222(h)(1), (h)(3).

[980] *See* 47 U.S.C. § 222(h)(1)(A)-(B). Under 47 U.S.C. § 222(h)(1)(A), CPNI includes "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship" other than subscriber list information.

[981] *See supra* Part III.B.3.

[982] *See* 47 U.S.C. § 222(d)(3) (carving out an exception that permits the use or disclosure of CPNI for the provision of "any inbound telemarketing, referral or administrative services to the customer for the duration of the call, if the call was initiated by the customer and the customer approves of the use of such information to provide such service"). *But see* CTIA Comments at 16.

obligation to seek customer approval for use, disclosure, or permission of access to individually identifiable CPNI under paragraph (c)(1); the obligation to disclose CPNI upon request under paragraph (c)(2); and the grant of permission to use and disclose "aggregate customer information" under paragraph (c) (3).

338. Where a component of Section 222 applies only to a subset of telecommunications carriers, Congress used a term to apply such a limit. For instance, Section 222(c)(3) permits all telecommunications carriers to use and disclose aggregate customer information, but "local exchange carrier[s]" can do so only on the condition that they make the information available to others on reasonable and nondiscriminatory terms.[983] The inclusion of a pro-competitive condition in Section 222(c)(3) that applies only to local exchange carriers is consistent with other provisions of the 1996 Act directed at opening local telephone markets to competition.[984] But the limited scope of this condition does not serve to limit the applicability of Section 222 as a whole.[985] Indeed, not even Section 222(c)(3) *itself* is limited in scope to providers of local exchange service. Rather, its primary purpose is to clarify that telecommunications carriers may use and disclose customer information when it takes the form of "aggregate customer information." BIAS providers commenting in this proceeding have expressed a strong interest in being able to use and disclose such information.[986] As telecommunications carriers, their ability to do so is made clear under Section 222(c)(3).

339. Similarly, the limited scope of providers covered by the duty to share "subscriber list information" under Section 222(e) is commensurate with the scope of the problem being addressed, namely in the publication of telephone directories.[987] In particular, the "telephone exchange service" providers subject to unbundling and nondiscrimination requirements by the provision are those that would have the "subscriber list information" needed to produce these directories.[988] The fact that Section 222 includes provisions to address such telephone-specific concerns does not change its overall character as a privacy protection statute for telecommunications, one that has as much relevance for BIAS as it does for telephone service.

340. We disagree with the view that Congress confirmed Section 222 as a telephone-specific statute when it amended subsections 222(d)(4), (f)(1) and (g) as part of the New and Emerging Technologies 911 Improvement Act of 2008 (NET 911 Act).[989] These provisions of Section 222 establish rights and obligations regarding carrier disclosure of customer information to assist in the delivery of emergency services. The NET 911 Act brought "IP-enabled voice service[s]" within their scope. Amending Section 222 in this manner addressed a narrow but critical public safety concern: IP-enabled voice services were emerging as a platform for delivery of 911 service, yet providers of these services were not classified as "telecommunications carriers" subject to Section 222.[990] The NET 911 Act

[983] 47 U.S.C. § 222(c)(3).

[984] *See generally* 47 U.S.C. §§ 251-261 ("Development of Competitive Markets"), §§ 271-276 ("Special Provisions Concerning Bell Operating Companies").

[985] *See* 47 U.S.C. § 222(c)(3). *But see* NCTA Comments at 9, n.13.

[986] *See supra* Part III.B.4.

[987] *See* H.R. Rep. No. 104-204, at 89 ("LECs have total control over subscriber list information . . . . Section 222 ensures that independent directory publishers have access to subscriber listing information gathered by all LECs.").

[988] *See* 47 U.S.C. § 222(e) (requiring the provision of subscriber list information "for the purpose of publishing directories in any format").

[989] New and Emerging Technologies 911 Improvement Act of 2008, Pub. L. No. 110-283 (2008). *See* CTIA Comments at 18; USTelecom Comments at 29.

[990] *See* H.R. Rep. No. 110-442, at 7 (2007) ("Section 222 includes exceptions to its protections to allow wireline and wireless carriers to provide customer information to PSAPs in emergency situations. There is no similar provision (continued….)

amendments ensure that all IP-enabled voice services, even to the extent they are *not* telecommunications services, are treated under Section 222 much the same as traditional telephony services for purposes related to E911 service. This treatment has nothing to do with the extent to which telecommunications services that are not voice services are subject to Section 222.[991]

341. In addition, we observe that none of the references to telephone-specific services in Section 222 that commenters identify are found in Section 222(a). As explained below, we construe Section 222(a) as a broad privacy protection mandate that extends beyond the specific duties articulated in Sections 222(b) and (c). Thus, even if commenters could establish that these more specific parts of Section 222 are qualified in ways that limit their scope to voice telephony or related services, or that exclude BIAS from their scope, we would still find that a BIAS provider—like "[e]very telecommunications carrier"[992]—has customer privacy obligations under Section 222(a). And if we accept commenters' view that the role of Section 222(a) in the statute is to identify "which entities" have duties thereunder,[993] it follows that subsections (b) and (c) apply not only to telephony or voice providers but to "every telecommunications carrier."

342. Finally, we dismiss efforts to conflate Section 222 with its implementing rules.[994] When we forbore from application of the existing implementing rules to BIAS, we made clear that the statute itself still applies.[995] Commenters do not present any compelling reason to revisit this decision.[996]

### 2. Section 222(a) Provides Authority for the Rules as to Customer PI

343. We next conclude that Section 222(a) provides legal authority for our rules. As explained below, Section 222(a) imposes an enforceable duty on telecommunications carriers that is more expansive than the combination of duties set forth subsections (b) and (c). We interpret these subsections as defining the contours of a carrier's general duty under Section 222(a) as it applies in particular contexts, but not as coterminous with the broader duty under Section 222(a). On the contrary, we construe Section 222(a) as imposing a broad duty on carriers to protect customer PI that extends beyond the narrower scope of information specified in Section 222(c). We also find that the rules adopted in this Report and Order to ensure the protection of customer PI soundly implement Section 222(a).

(Continued from previous page)
governing or granting exceptions for VoIP service. H.R. 3403 would amend section 222 to add VoIP 911 service to the established 911 exceptions.").

[991] We have exercised our ancillary jurisdiction to apply rules adopted under Section 222 to providers of interconnected VoIP services. *See 2007 CPNI Order*, 22 FCC Rcd at 6954-57, paras. 54-59; *see also* 47 CFR § 64.2003(o) (defining "telecommunications carrier or carrier" for purposes of the CPNI rules to include interconnected VoIP providers).

[992] *See* 47 U.S.C. § 222(a).

[993] *See infra* Part IV.A.2.a; *see also* Free Press Reply at 7-8 (arguing that CTIA "counsels the Commission against 'atomistic interpretation of Section 222(a)'" while at the same time urging the Commission to "ignore the entirety of the statute in favor of focusing on 'atomistic' references to telephone and voice services").

[994] *See, e.g.*, CTIA Comments at 23 ("The Commission implicitly acknowledged Section 222's inapplicability to ISPs' provision of broadband service by forbearing from applying its CPNI rules in the *Open Internet Order*.") (capitalization omitted).

[995] *2015 Open Internet Order*, 30 FCC Rcd at 5820, para. 462.

[996] *See USTA v. FCC*, 825 F.3d 674 (upholding the *2015 Open Internet Order* in its entirety). Insofar as any commenter in this proceeding requests reconsideration of the classification decision in the *2015 Open Internet Order*, the request is untimely. *See* 47 CFR §§ 1.106, 1.429.

### a. Section 222(a) Imposes on Telecommunications Carriers an Enforceable Duty to "Protect the Confidentiality" of "Proprietary Information"

344. Section 222(a) states that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to" customers, fellow carriers, and equipment manufacturers.[997] In this Report and Order we adopt the most straightforward interpretation of this text by finding that Section 222(a) imposes a "duty," on "every telecommunications carrier." A "duty" is commonly understood to mean an enforceable obligation.[998] It is well-established that the Commission may adopt rules to implement and enforce an obligation imposed by the Act, including Section 222(a).[999] The substance of the duty is to "protect the confidentiality of proprietary information"—all "proprietary information" that is "of, and relating to," the specified entities, namely "other telecommunications carriers, equipment manufacturers, and customers."[1000] This Report and Order implements Section 222(a) with respect to "customers," defining the term "customer PI" to mean that which is "proprietary information of, and relating to . . . customers."[1001] The term is thus firmly rooted in the language of Section 222(a).[1002]

345. The duty set forth in Section 222(a) concerns information "of, and relating to" customers and other covered entities. The Supreme Court has held that "the ordinary meaning of [the phrase 'relat[ing] to'] is a broad one," and in certain contexts it has described the phrase as "deliberately expansive" and "conspicuous for its breadth."[1003] The record contains no evidence that Congress intended the phrase "relating to" to be construed more narrowly for purposes of Section 222(a) than it would be ordinarily. Thus, the most natural reading of Section 222(a) is that it imposes a broad duty on telecommunications carriers to protect proprietary information, one that is informed by but not necessarily limited to the more specific duties laid out in subsections (b) and (c).[1004]

346. The treatment of "equipment manufacturers" under Section 222 provides further evidence for this interpretation. This term is used only once: Section 222(a) includes "equipment manufacturers"

---

[997] *See* 47 U.S.C. § 222(a).

[998] *See* Black's Law Dictionary 615 (10th ed. 2014) (defining a "duty" as "[a] legal obligation that is owed or due to another and that needs to be satisfied; that which one is bound to do, and for which somebody else has a corresponding right").

[999] *AT&T Corp. v. Iowa Utils. Bd.*, 525 U.S. 366, 378 (1999) (holding that the last sentence in Section 201(b) "means what it says: The FCC has rulemaking authority to carry out the 'provisions of this Act,'" including provisions added by the Telecommunications Act of 1996); *1998 CPNI Order*, 13 FCC Rcd at 8073-74, para. 14; *2007 CPNI Order*, 22 FCC Rcd at 6943, para. 27 n.94 ("Section 201(b) authorizes the Commission to 'prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of this Act,' including section 222."). *But see* USTelecom Comments at 29-30 ("But, unlike several other provisions that include an enforceable mandate for which the Commission has direct authority to create governing regulations, subsection (a) merely sets forth a duty without granting authority to the Commission to further define or enforce that duty.") (internal citation omitted).

[1000] *See* 47 U.S.C. § 222(a).

[1001] *See id*.

[1002] *But see* CTIA Comments at 24 ("The term 'customer proprietary information' appears nowhere in the Communications Act, and the Commission lacks authority to create it . . .").

[1003] *See Morales v. TransWorld Airlines*, 504 U.S. 374, 383-84 (1992).

[1004] *See* EFF Comments at 2; OTI Comments at 18-19; Free Press Reply at 8.

among the classes of entities owed confidentiality protections as part of a carrier's "general" duty.[1005] While Sections 222(b) and (c) specify in greater detail how this duty applies with respect to customers and fellow carriers—the other entities protected under Section 222(a)—there is no further statutory guidance on what carriers must do to protect the proprietary information of equipment manufacturers. Thus, the duty imposed on carriers under Section 222 with regard to equipment manufacturers must have its sole basis in Section 222(a). This would not be possible unless Section 222(a) were read to confer enforceable obligations that are independent of, and that exceed, the requirements of subsections (b) and (c).[1006]

347. Nothing in the statutory text or structure of Section 222 contradicts this interpretation. To the contrary, this plain language interpretation is further supported by the structure of Section 222 and consistent with approaches used in other parts of the Act. Section 222(a)'s heading "In General" suggests a general "duty," to be followed by specifics as to particular situations. Section 222(a) is not given a heading such as "Purpose" or "Preamble" that would indicate that the "duty" it announces is merely precatory or an inert "statement of purpose." Section 251 of the Act is structured similarly in this regard, and there is no argument that the duty announced in Section 251(a) is merely precatory.[1007] In addition, there is no textual indication that Sections 222(b) and (c) define the outer bounds of Section 222(a)'s scope.[1008] For instance, Section 222(a) does not include language such as "as set forth below" or "as set forth in subsections (b) and (c)." We also dismiss as irrelevant CTIA's observation that some provisions of the 1996 Act "can be interpreted as general statements of policy, rather than as grants of additional authority."[1009] That fact alone would have no bearing on how to interpret Section 222(a), which employs "regulatory terminology" in imparting a general "duty" on telecommunications carriers.[1010] Finally, our interpretation of subsection (a) does not render subsection (b) or (c) superfluous.[1011] The latter subsections directly impose specific requirements on telecommunications carriers to address concerns that

[1005] *See* 47 U.S.C. § 222(a) ("Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunications carriers, *equipment manufacturers* . . .") (emphasis added).

[1006] We reject any argument that the reference in Section 222(a) to equipment manufacturers is nothing more than a cross-reference to obligations contained in Section 273. Such an interpretation would give no independent meaning to Section 222(a), and therefore would be inconsistent with established principles of statutory construction. It would also be contrary to the plain meaning of Section 222(a), which contains no reference to and is plainly broader than Section 273; nothing in Section 273 applies broadly to every telecommunications carrier, as Section 222(a) clearly does.

[1007] *Compare* 47 U.S.C. § 222(a) (titled "In General" and beginning "Every telecommunications carrier has a duty . . .") (capitalization omitted) *with* 47 U.S.C. § 251(a) (titled "General Duty of Telecommunications Carriers" and beginning "Each telecommunications carrier has the duty. . .") (capitalization omitted). Also, like in Section 222, the "general duty" announced in subsection (a) of Section 251 is accompanied by more specific duties announced in the subsections that follow. *See* 47 U.S.C. § 251(b) ("Obligations of All Local Exchange Carriers") (capitalization omitted), (c) ("Additional Obligations of Incumbent Local Exchange Carriers") (capitalization omitted).

[1008] *See* Free Press Comments at 10 ("Section 222 begins with a general duty for telecommunications carriers to protect the 'proprietary information' of customers. Subsections of 222 further elaborate on, but do not narrow the scope of that general duty to protect privacy."). *But see* CenturyLink Comments at 14 (arguing that "Section 222(a) sets forth the general objective of the provision" while "[t]he specifics are then supplied by the following subsections"); T-Mobile Comments at 17 (arguing "Section 222(a) is nothing more than a general introductory provision"); Washington Legal Foundation Comments at 5.

[1009] Letter From Scott Bergmann, Vice President, Regulatory Affairs, CTIA, to Marlene Dortch, Secretary, FCC, WC Docket No. 16-106 at 8 (filed Sept. 16, 2016) (CTIA Sept. 16, 2016 *Ex Parte*).

[1010] *But see id*. (arguing that Section 222(a) "lacks the regulatory terminology present in Section 706(a)").

[1011] *But see* ADTRAN Comments at 5-6.

were particularly pressing at the time of Section 222's enactment. Our reading of Section 222(a) preserves the role of each of these provisions within the statute, while also allowing the Commission to adopt broader privacy protections to keep pace with the evolution of telecommunications services.

348. As Public Knowledge argues, the breadth of the duty announced in Section 222(a) is consistent with a broad understanding of the purpose of Section 222. We agree that this subsection endows the Commission with a continuing responsibility to protect the privacy customer information as telecommunications services evolve.[1012] Congress's inclusion in Section 222 of more specific provisions to address issues that were "front-and-center" at the time of the 1996 Act's enactment in no way detracts from this broader purpose.[1013]

349. Our interpretation of Section 222(a) is far from novel. Other provisions of the Act set forth a general rule along with specific instructions for applying the rule in particular contexts.[1014] We agree with Public Knowledge that, in addition to Section 251, another provision that bears a particularly close resemblance to Section 222 in this regard is Section 628.[1015] Subsection (b) of this provision imposes a general "prohibition" on cable operators from interfering with competitors' ability to provide satellite cable or satellite broadcast programming.[1016] Subsection (c) in turn directs the Commission to adopt rules to implement this prohibition and specifies their "minimum contents."[1017] As a general matter, the "minimum" regulations required under Section 628(c) are aimed at preventing cable operators from denying their competitors access to programming.[1018] In 2009, the D.C. Circuit upheld Commission rules adopted under Section 628(b) that prevented cable operators from entering exclusivity agreements with

[1012] *See* Public Knowledge White Paper at 16 ("Congress recognized that it could not accurately forecast what specific information might become either personally or competitively sensitive in the future as communications technologies evolved and converged to include video service and other media. Rather than wait for Congress to do a study, Congress simply delegated the authority to the FCC to consider what rules, what type of information and what specific services should be covered over time."); *see also* EFF Comments at 1-2 ("Congress enacted Section 222 following a tradition of sector-specific privacy regimes to address unique problems. Telecommunications as a telephone service posed all of the same privacy risks to consumers that modern day broadband communications does, as voice communications of sensitive information simply become digital transmissions. The Commission is now at a critical point to determine telecommunications providers' statutory obligations under Section 222 to protect consumer privacy.").

[1013] *See* OTI Reply at 4-5 ("[T]he information collection capabilities of internet providers were primitive when Congress passed Section 222 and therefore the internet likely was not front-and-center on the collective minds of Congress . . . . Congress was not legislating against today's factual backdrop, where ISPs can monitor everyone's internet traffic, but Congress left the statute broad enough that the FCC could address that issue.").

[1014] *See* 47 U.S.C. § 251 (imposing a "general duty" on telecommunications carriers and more specific duties on subcategories of carriers); *see also* Public Knowledge White Paper at 17-19. CTIA attempts to distinguish other such provisions by arguing that they do not "define in their subsequent subsections the duties *of different regulated entities* identified in their initial subsections." CTIA Reply at 18. In fact, Section 251 does define specific duties of different regulatees in subsections (b) (all local exchange carriers) and (c) (incumbent local exchange carriers), and Section 628 does apply specific duties to cable operators, satellite cable programming vendors, and common carriers, *see* 47 U.S.C. § 548(c), (j). In any event, CTIA does not explain what it believes to be the significance of this distinction.

[1015] 47 U.S.C. § 548; *see also* Public Knowledge White Paper at 17-18.

[1016] 47 U.S.C. § 548(b).

[1017] 47 U.S.C. § 548(c).

[1018] *Id*. at (c)(2). The "minimum" required regulations include, *inter alia*, "establish[ing] effective safeguards to prevent a cable operator which has an attributable interest in a satellite cable programming vendor or a satellite broadcast programming vendor from unduly or improperly influencing the decision of such vendor to sell, or the prices, terms, and conditions of sale of, satellite cable programming or satellite broadcast programming to any unaffiliated multichannel video programming distributor." *Id*. at (c)(2)(A).

owners of multi-unit buildings, an anti-competitive practice that is only tenuously related to the "minimum" regulations implemented under Section 628(c).[1019] Taking note of Section 628(b)'s "broad and sweeping terms," the court ruled that "nothing in the statute unambiguously limits the Commission to regulating practices" related to the "principal evil that Congress had in mind" when enacting Section 628, as expressed in subsection (c).[1020] Rather, it held that the Commission's "remedial powers" to enforce subsection (b) reached beyond circumstances that Congress "specifically foresaw."[1021] Similarly, we agree with OTI that the "principal" focus of Section 222 on regulating CPNI to promote competition and consumer protection in emerging telecommunications markets must be read in harmony with the "broad and sweeping" mandate of Section 222(a).[1022] In construing the latter we must give effect to the "actual words" of the provision.[1023] These words plainly impose a "duty" on "every telecommunications carrier."

350. Even if there were some ambiguity in the text, commenters that oppose our interpretation of Section 222(a) have failed to offer a compelling alternative interpretation. One proposed alternative is that Section 222(a) merely confirms Congress's intent that the newly enacted Section 222 would apply to "every telecommunications carrier," including not only the legacy carriers subject to then-existing CPNI requirements but also "the new entrants that the 1996 Act envisioned."[1024] Similar arguments in the record are that Section 222(a) "identifies which entities have responsibility to protect information, and informs the reading of subsequent subsections, which articulate how these entities must protect information,"[1025] or that the provision "merely identifies the categories of information to which Section 222 applies."[1026] These arguments are unconvincing. First, subsections (b) and (c) themselves are written broadly to apply to "telecommunications carrier[s]." There is no textual basis for interpreting either provision as applying only to a legacy subset of carriers, such as the Bell Operating Companies, AT&T, and GTE. Subsections (b) and (c) also specify the categories of information to which each applies, without reference to subsection (a). Thus, commenters' proposals for interpreting Section 222(a)

[1019] *National Cable & Telecomms. Ass'n v. FCC*, 567 F.3d 659, 661 (D.C. Cir. 2009) (*NCTA II*); *see also Cablevision Sys. Corp. v. FCC*, 649 F.3d 695, 707 (D.C. Cir. 2011).

[1020] *Id.* at 664; *see also PGA Tour v. Martin*, 532 U.S. 661 (2001) ("[T]he fact that a statute can be applied in situations not expressly anticipated by Congress does not demonstrate ambiguity. It demonstrates breadth.") (quoting *Pa. Dept. of Corr.v. Yeskey*, 524 U.S. 206, 212 (1952)).

[1021] *NCTA II*, 567 F.3d at 665.

[1022] *See* OTI Reply at 3 ("In the mid-nineties, when the Telecommunications Act was written, Congress was of course concerned with incumbent telephone services given their ability to use the data they collected in routing traffic to gain competitive advantages and target specific customers. However, Congress's concerns over some specific telephone issues does not freeze the entire statute in time, nor did those specific concerns narrow the statute to telephone services ever after. If Congress had intended to write a statute that applied to telephone services only, it could have easily done so.").

[1023] *NCTA II*, 567 F.3d at 666.

[1024] Verizon Comments at 54. Verizon argues that both the House bill and the Senate bill originally would have protected a category of customer information broader than the eventual definition of CPNI, but that "Congress ultimately rejected both approaches." *See id.* at 55. There is no evidence that Congress would have, without explanation, adopted an approach that is narrower than either chamber's bill. And, in fact, the Senate bill (which, as Verizon points out, was intended to apply broadly to "customer-specific proprietary information," S. Rep. No. 104-23 at 24), contained in its text language almost identical to what Congress ultimately enacted, creating "a duty to protect the confidentiality of proprietary information relating to other common carriers, to equipment manufacturers, and to customers." S. 652, 104th Cong., 1st Sess. § 301(d); *id.* sec. 222(a), § 256(c)(2)(E).

[1025] CTIA Comments 26; *see also* Washington Legal Foundation Comments at 5.

[1026] T-Mobile Comments at 16.

would render that provision superfluous, contrary to the canon against such interpretations.[1027] Moreover, the statute does not expressly link the duty announced in Section 222(a) with the subsections that follow. That is, the statute does not direct "every telecommunications carrier" to protect proprietary information "in accordance with subsections (b) and (c)" or anything similar.

351. Nor does our interpretation of Section 222(a) vitiate any other elements of Section 222. On the contrary, we read Section 222(a) as imposing a broad duty that can and must be read in harmony with the more specific mandates set forth elsewhere in the statute.[1028] Accordingly, we need not and do not construe Section 222(a) so broadly as to prohibit any sharing of subscriber information that subsection (e) or (g) would otherwise require.[1029] That is, subsection (a)'s duty to protect the confidentiality of customer PI is in no way inconsistent with subsection (e)'s duty to share SLI, which by definition[1030] is *published* and therefore is not confidential.[1031] Nor is it inconsistent with subsection (g)'s duty to share subscriber information "solely for purposes of delivering or assisting in the delivery of emergency services."[1032] Indeed, far from "render[ing] null" subsections (e) and (g), our reasoned interpretation of Section 222(a) preserves the full effect of both of these provisions.[1033] We thus reject the argument that subsection (a)'s absence from the "notwithstanding" clauses of subsections (e) and (g) should be taken as evidence that the former provision confers no "substantive regulatory authority."[1034] Rather, there was simply no need for Congress to have included subsection (a) in these clauses.[1035] Also, the mere omission of Section 222(a) from the these clauses would have been an exceedingly oblique and indirect way of settling upon an interpretation of Section 222(a) that runs counter to its plain meaning.[1036] Relatedly, there is no conflict because our understanding of Section 222(a) does not override any of the exceptions to Section 222(c) set forth in Section 222(d). For example, a carrier need not fear that its disclosure of CPNI "to initiate, render, bill [or] collect for telecommunications services" as subsection (d) permits might independently violate Section 222(a), because such disclosure is not inconsistent with the carrier's

[1027] *See Hibbs v. Winn*, 542 U.S. 88, 101 (2004) ("A statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant . . . .") (quoting 2A N. Singer, Statutes and Statutory Construction § 46.06, 181–186 (rev. 6th ed. 2000)); *see also* OTI Reply at 7-8.

[1028] *See RadLAX Gateway Hotel, LLC v. Amalgamated Bank*, 132 S.Ct. 2065, 2071 (2012) ("It is an old and familiar rule that, where there is, in the same statute, a particular enactment, and also a general one, which, in its most comprehensive sense, would include what is embraced in the former, the particular enactment must be operative, and the general enactment must be taken to affect only such cases within its general language as are not within the provisions of the particular enactment. This rule applies wherever an act contains general provisions and also special ones upon a subject, which, standing alone, the general provisions would include.") (citing *United States v. Chase*, 135 U.S. 255, 260 (1890)).

[1029] *But see* AT&T Comments at 106-07; CTIA Comments at 27-28; NCTA Comments at 16-17.

[1030] 47 U.S.C. § 222(h)(3) (defining "subscriber list information" as identifying information that the carrier or an affiliate has published or intends to publish in a directory format).

[1031] *See* 47 U.S.C. § 222(e)

[1032] *See* 47 U.S.C. § 222(g).

[1033] *But see* CTIA Comments at 27.

[1034] NCTA Comments at 17.

[1035] *But see, e.g.*, AT&T Comments at 106-07 (arguing that the construction of Section 222(a) proposed in the NPRM would create conflict with subsections (e) and (g)).

[1036] *See Whitman v. American Trucking*, 531 U.S. 457, 468 (2001) (*Whitman*) ("Congress, we have held, does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions—it does not, one might say, hide elephants in mouseholes."); *see also USTA v. FCC*, 825 F.3d at 703 (citing *Whitman* in rejecting the argument that language in Section 230 of the Act settles the regulatory status of broadband service as an information service).

duty to protect the confidentiality of such information.[1037] Nor do we construe Section 222(a) as negating a carrier's right under Section 222(c)(1) to use, disclose or permit access to CPNI for the specific purposes set forth in subclauses (A) and (B).[1038]

352. We also disagree with the argument that our construction of Section 222(a) enlists a "vague or ancillary" provision of the statute to "alter [its] fundamental details."[1039] Section 222(a) appears, of course, at the beginning of Section 222. The first thirteen words of Section 222(a)—and thus, of Section 222—read: "Every telecommunications carrier has a duty to protect the confidentiality of proprietary information. . . ."[1040] Congress could not have featured this language any more prominently within the statute, nor could the duty it propounds be any more clearly and directly expressed. As discussed above, a statutory structure of establishing a general duty and then addressing subsets of that duty in greater detail is not unique, even within the Communications Act.

353. Finally, we reject the view that our interpretation of Section 222(a) locates in "a long-extant statute an unheralded power to regulate a significant portion of the American economy."[1041] The Commission has exercised regulatory authority under Section 222(c) for approximately two decades and oversaw certain carriers' handling of customer PI for over two decades before that.[1042] Even assuming a contrary reading of Section 222(a), subsection (c) would still invest the Commission with substantial regulatory authority over personal information that BIAS providers and other telecommunications carriers collect from their customers, and Sections 201 and 202 would apply to carriers' practices in handling customers' information.[1043] Thus, our interpretation of Section 222(a) is a far cry from the "transformative" act of statutory interpretation struck down in *Utility Air Regulatory Group v. EPA*.[1044] There, the agency's broad construction of the term "air pollutant" would have completely upended the "structure and design" of a permitting scheme established by statute and extended that regime to broad swaths of the economy.[1045] By contrast, the net effect of our interpreting Section 222(a) as governing all customer PI is to make clear the Commission's authority over carriers' treatment of customer proprietary information that may not qualify as CPNI, such as Social Security numbers or financial records. This represents a modest but critical recognition of our regulatory purview beyond CPNI to cover additional "proprietary" information that Section 222(a) plainly reaches. Moreover, BIAS providers' treatment of such information fell squarely within the jurisdiction of the FTC prior to the Commission's reclassification of BIAS. The scope of regulatory authority we are asserting under Section 222(a) is thus far from novel or "unheralded."

#### b. The Broad Duty of Section 222(a) Extends to All "Proprietary Information" That Is "Of" or "Relating to" Customers

354. Having determined that Section 222(a) imposes on carriers an enforceable duty, we also

[1037] *See* 47 U.S.C. § 222(d)(1).

[1038] *See* 47 U.S.C. § 222(c)(1). *But see* Verizon Reply at 27.

[1039] *Whitman*, 531 U.S. at 468.

[1040] *See* 47 U.S.C. § 222(a).

[1041] *See Utility Air Regulatory Group. v. EPA*, 134 S. Ct. 2427, 2444 (2014); *see also* Comcast Comments at 75, n.200.

[1042] *See Furnishing of Customer Premises Equipment and Enhanced Services by American Telephone & Telegraph Co.*, CC Docket No. 85-26, Order, 102 F.C.C.2d 655, 692-93, para. 64 (1985) (discussing 47 CFR § 64.702 (1984) and noting that "customer proprietary information . . . belongs to the customers, and many may not want it to be made public").

[1043] *See* 47 U.S.C. §§ 222(c), 201, 202; *see also TerraCom NAL*, 29 FCC Rcd at 13335-41, paras. 31-44.

[1044] *See Utility Air Regulatory Group*, 134 S. Ct. at 2444.

[1045] *Id*. at 2442-43.

conclude that this duty extends to all "proprietary information" that is "of, or relating to" customers, regardless of whether the information qualifies as CPNI. That is, we reject the argument that Section 222(c) exhausts the duty set forth in Section 222(a) as it applies with respect to customers.

355. Once again, our interpretation follows from the plain language of Section 222. While subsection (c) establishes obligations with respect to "customer proprietary network information," subsection (a) omits the word "network." The concept of the "network" lies at the heart of CPNI: the information defined as CPNI in Section 222(h)(1) is of the sort that carriers obtain by virtue providing service over their networks. However, as we have explained above, this sort of information is not the only "proprietary information" that telecommunications carriers can and do obtain from their customers by virtue of the carrier-customer relationship.[1046] We therefore find that "proprietary information of, and relating to. . . customers" is best read as broader than CPNI. Moreover, we are convinced that the term "network" should not be read into Section 222(a), contrary to what some commenters appear to argue.[1047] We dismiss the idea that the syntax of Section 222(a) would have made it awkward to include the term "network" as an express limitation on the general duty as it applies with regard to customer proprietary information.[1048] Congress is not bound to any particular formula when drafting legislation. Section 222(a) could easily have been written to include the term "customer proprietary network information" in full, had Congress chosen to do so.[1049]

356. Even if there were some ambiguity in the text of the statute, we would conclude that the best interpretation is that Section 222(a) applies to customer proprietary information that is not CPNI. Some argue that the legislative history of Section 222 precludes this interpretation because of a statement from the Conference Report that attended passage of the 1996 Act, which reads: "In general, Section 222 strives to balance both competitive and consumer privacy interests with respect to CPNI." [1050] Commenters appear to interpret this statement as evidence that Section 222 was intended to apply *only* to CPNI.[1051] But this is clearly not so. Section 222(a) concerns not only customer information but also information "of, and relating to" fellow carriers and equipment manufacturers. Section 222(b) in turn is focused exclusively on "carrier information."[1052] Therefore, Section 222 *in general* cannot be concerned solely with CPNI. We are similarly unmoved by evidence that Congress considered but ultimately rejected a more expansive definition of CPNI than that which is codified in Section 222(h)(1).[1053] Such evidence cannot decide the question whether Section 222(a) governs a category of customer information that is *broader than* CPNI. As explained above, our interpretation follows from the plain language of the

[1046] *See supra* Part III.B.

[1047] *But see* Comcast Comments at 71-72 ("The term proprietary information was used in Section 222(a) simply because the provision covers information exchanged with three different types of entities – customers, telecommunications carriers, and equipment manufacturers – and so using the term CPNI, a term that applies solely to *customers* as addressed in Section 222(c), would not have been appropriate.").

[1048] *But see id*.

[1049] For instance, the subsection could have read: "Every telecommunications carrier has a duty to protect the confidentiality of customer proprietary network information, and of proprietary information of, and relating to, other telecommunication carriers and equipment manufacturers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier."

[1050] *See* S. Conf. Rep. No. 104-230, 205 (1996).

[1051] *See, e.g.*, ITTA Comments at 6-7; CTIA Comments at 28.

[1052] *See* 47 U.S.C. § 222(b). Furthermore, subsections (e) and (g) impose affirmative obligations on carriers in certain circumstances to share SLI, which by definition is not CPNI. *See* 47 U.S.C. §§ 222(e), (g), (h)(1), (h)(3).

[1053] *See, e.g.*, Comcast Comments at 74 ("The Conference Report [for the 1996 Act] adopted the House's proposed CPNI definition, but eliminated the catch-all provision from the CPNI definition ultimately codified in Section 222.").

provision, and the legislative history of Section 222 is not to the contrary. At the very least, any contrary evidence that may be derived from the legislative history is far from sufficient to override our reasoned interpretation of the provision.[1054]

357. We acknowledge that prior Commission orders implementing Section 222 have focused largely on CPNI rather than customer PI more broadly.[1055] Yet we do not believe this precedent should constrain our efforts in this proceeding to develop robust privacy protections for consumers under Section 222(a). In fact, the Commission made clear as early as 2007 that Section 222(a) requires carriers to "take every reasonable precaution to protect the confidentiality of proprietary or personal customer information."[1056] Our express determination in the *TerraCom* proceeding that subsection (a) covers customer proprietary information beyond CPNI merely "affirm[ed]" what the Commission had strongly implied seven years earlier.[1057] Moreover, earlier orders adopting and revising rules under Section 222 were focused so narrowly on the protection of individually identifiable CPNI that the question whether Section 222(a) covers additional customer information was never squarely addressed.[1058] This early focus on CPNI makes sense: Section 222 was adopted against the background of existing Commission regulations concerning CPNI,[1059] and the first Section 222 proceeding was instituted in response to a petition from industry seeking clarity about the use of CPNI.[1060] However, the Commission has never expressly endorsed the view that Section 222(a) fails to reach customer information beyond CPNI.[1061] We

[1054] *See Oncale v. Sundowner Offshore Servs., Inc*., 523 U.S. 75, 79 (1998) ("[I]t is ultimately the provisions of our laws rather than the principal concerns of our legislators by which we are governed."); *cf. NCTA II*, 567 F.3d at 665 ("Thus, even if legislative history could carry petitioners all the way from statutory language that literally authorizes the Commission's action to the proposition that the statute unambiguously forecloses the agency's view, *this* legislative history [i.e., that attending adoption of Section 628 of the Act] cannot.").

[1055] *See, e.g.,* AT&T Comments at 104-05; CTIA Comments at 30-32*; see also 2007 CPNI Order*, 22 FCC Rcd at 6928, para. 1 ("In this Order, [we . . . strengthen] our rules to protect the privacy of customer proprietary network information (CPNI) . . ."); *1998 CPNI Order*, 13 FCC Rcd at 8066-67, para. 4 (providing an overview of the rules being adopted in that order regarding CPNI).

[1056] *See 2007 CPNI Order*, 22 FCC Rcd at 6959, para. 64.

[1057] *TerraCom NAL*, 29 FCC Rcd at 13330, para. 14. *But see* CTIA Comments at 30-31 (contending that the reference to "proprietary or personal customer information" in paragraph 64 of the *2007 CPNI Order* is best read as limited to CPNI); *see also Lifeline and Link Up Reform and Modernization et al.*, Second Further Notice of Proposed Rulemaking, Order on Reconsideration, Second Report and Order, and Memorandum Opinion and Order, 30 FCC Rcd 7818, 7895-96, para. 234 (2015) (reminding carriers that the duty to protect customer information "includes all documentation submitted by a consumer or collected by an [eligible telecommunications carrier] to determine a consumer's eligibility for Lifeline service, as well as all personally identifiable information contained therein").

[1058] *But see* ITTA Comments at 3-4 (arguing that "the Commission *did* address [whether Section 222(a) covers customer information other than CPNI] and affirmatively decided that subsection 222(a) afforded no such 'broader' protections."). ITTA cites as the basis for this claim a discussion in the *1999 CPNI Reconsideration Order* of the relationship between Sections 222 and 272(c)(1). *See id*. at 4, n.10 (citing *1999 CPNI Reconsideration Order*, 14 FCC Rcd at 14488, para. 147). Contrary to ITTA's claim, the Commission did not "affirmatively" address the scope of customer information covered under Section 222(a).

[1059] *See 1998 CPNI Order*, 13 FCC Rcd at 8068-69, para. 7 ("Prior to the 1996 Act, the Commission had established CPNI requirements applicable to the enhanced services operations of AT&T, the BOCs, and GTE, and the CPE operations of AT&T and the BOCs, in the *Computer II*, *Computer III*, *GTE ONA*, and *BOC CPE Relief* proceedings.") (internal footnotes omitted).

[1060] *See 1998 CPNI Order*, 13 FCC Rcd at 8068, para. 6 (explaining that the proceeding was initiated "[i]n response to various informal requests for guidance from the telecommunications industry regarding the obligation of carriers under new section 222").

therefore disagree that interpreting the provision in a contrary manner will have the effect of unsettling "18 years" of Commission precedent in this area.[1062]

358. Finally, construing Section 222(a) as reaching customer information other than CPNI avoids the creation of a regulatory gap that Congress could not reasonably have intended. While the FTC has broad statutory authority to protect against "unfair or deceptive" commercial practices, its enabling statute includes a provision that exempts common carriers subject to the Communications Act.[1063] This leaves the Federal Communications Commission as the only federal agency with robust authority to regulate BIAS providers and other telecommunications carriers in their treatment of sensitive customer information obtained through the provision of BIAS and other telecommunications services. If that authority failed to reach customer PI other than CPNI, substantial quantities of highly sensitive information that carriers routinely collect and use would fall outside of the purview of either this Commission or the FTC. The facts of *TerraCom* make clear the dangers of this outcome. In that proceeding we enforced Section 222(a) against a carrier that neglected to take even minimal security measures to protect Social Security numbers and other sensitive customer data from exposure on the public Internet.[1064] Commenters that advocate a narrow construction of Section 222(a) would have us divest ourselves of authority to take action in circumstances such as these. We need not and will not leave consumers without the authority to decide under what circumstances, if any, their BIAS providers are allowed to use and share their Social Security numbers, financial and health information, and other personal information.

#### c. The Rules We Adopt as to "Customer PI" Reasonably Implement the Mandate of Section 222(a) That Carriers "Protect the Confidentiality" of Such Information

359. The rules we adopt in this Report and Order apply with respect to customer PI, which we have defined to include three overlapping categories of information: individually identifiable CPNI; personally identifiable information (PII); and the content of communications. As explained above, the information we define as customer PI is "proprietary information of, [or] relating to . . . customers" for purposes of Section 222(a).[1065] The rules we adopt in this Report and Order faithfully implement this statutory provision. As a general matter, we are adopting a uniform regulatory scheme to govern all customer PI, regardless of whether the information qualifies as CPNI. We have achieved this unity by replicating the basic structure of Section 222(c), including the exceptions set forth in Section 222(d), under Section 222(a). In doing so, we uphold the specific statutory terms that govern CPNI, while

(Continued from previous page)

[1061] We expressly disavow any prior Commission statement that could be read as endorsing such a view. *See FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 515 (2009) (holding that although an agency must acknowledge that it is changing course when it adopts a new construction of an ambiguous statutory provision, "it need not demonstrate to a court's satisfaction that the reasons for the new policy are *better* than the reasons for the old one . . . ." Rather, it is sufficient that "the new policy is permissible under the statute, that there are good reasons for it, and that the agency *believes* it to be better, which the conscious change of course adequately indicates.").

[1062] *But see* Verizon Reply at 26.

[1063] 15 U.S.C. § 45(a)(2) (exempting "common carriers subject to the Acts to regulate commerce"), § 44 (defining "Acts to regulate commerce" as including "the Communications Act of 1934 and all Acts amendatory thereof and supplementary thereto"). *See also* 47 U.S.C. § 153(51) (providing that "[a] telecommunications carrier shall be treated as a common carrier under [the Communications Act] only to the extent that it is engaged in providing telecommunications services").

[1064] *See TerraCom NAL*, 29 FCC Rcd at 13325, para. 1 ("Today, we take action against two companies that collected names, addresses, Social Security numbers, driver's licenses, and other proprietary information (PI) belonging to low-income Americans and stored them on unprotected Internet servers that anyone in the world could access with a search engine and basic manipulation.").

[1065] *See supra* Part III.B.

adapting these to the broader category of customer PI. This approach is lawful under the statute and well-supported as a matter of policy.

360. As discussed above, we understand Section 222(a) to impose a broad duty on carriers to protect customer PI that extends beyond the narrower scope of information specified in Section 222(c).[1066] Section 222(c) sets forth binding rules regarding application of the general duty to carriers' handling of CPNI. In support of this view, we note the common focus of these subsections on "confidentiality." While subsection (a) directs carriers to "protect the confidentiality of proprietary information" in general,[1067] subsection (c) concerns the confidentiality of "individually identifiable customer proprietary network information" in particular.[1068] Under our interpretation, subsection (c) provides one possible way of implementing the broad duty set forth in subsection (a). That is, subsection (c) settles what it means for a carrier to "protect the confidentiality of proprietary information" when the information at issue is individually identifiable CPNI. Given this reading of the two provisions, we find no reason that the basic scheme set forth in Section 222(c) to govern individually identifiable CPNI cannot not be replicated under Section 222(a) to govern customer PI more broadly. In adopting Section 222(c), Congress identified a scheme for "protecting the confidentiality of proprietary information" that it deemed valid at least in the context of CPNI.[1069] The statute is silent on the implementation of this general duty as it applies to customer PI more broadly. In the absence of clear statutory guidance on the matter, we must exercise our judgment to determine a regulatory scheme that is appropriate for customer PI other than individually identifiable CPNI.

361. We have good reason to adopt a single set of rules for all customer PI under Section 222(a) that is based on the scheme set forth for individually identifiable CPNI in Sections 222(c) and (d). First, the record indicates that customer expectations about the use and handling of their personal information do not typically depend on whether the information at issue is CPNI or some other kind of proprietary information. Rather, customers are far more likely to recognize distinctions based on the sensitivity of the data.[1070] The rules we adopt today uphold this widespread customer expectation.[1071] In addition, a common set of rules for all customer PI subject to 222(a) will be easier for customers to understand and for providers to implement than two distinct sets of rules.[1072] These considerations go to the very heart of Section 222: the ability of customers to make informed decisions and of providers to apply a harmonized regime to all customer data will each contribute to the protection of "confidentiality" that the statute requires. Moreover, equalizing treatment of CPNI and other customer PI more closely aligns our rules with the FTC's time-tested privacy approach.[1073]

362. We agree with Comcast that "protect[ing] confidentiality" of proprietary information involves, among other things, "preventing [such information] from being exposed without authorization."[1074] This is among the core purposes of our rules. The requirement to obtain customer

[1066] *See supra* para. 343.

[1067] *See* 47 USC § 222(a).

[1068] *See* 47 USC § 222(c).

[1069] *See id*.; *see also* CTIA Comments at 26 ("In short, the most natural reading of Section 222 is that subsection (a)'s general mandate is specifically set forth for customers in subsection (c) . . .").

[1070] *See supra* Part III.D.

[1071] *See supra* Part III.D.1 (sensitive/non-sensitive distinction), Part III.E (sensitivity of the data as a factor), and III.F.1 (harm presumption with respect to sensitive data breaches).

[1072] *See, e.g.*, WTA Comments at 19 (discussing the costs that would accrue to smaller providers in complying with "multiple regulatory regimes").

[1073] *See supra* para. 358.

[1074] Comcast Comments at 81.

approval before using, disclosing, or permitting access to customer PI directly ensures that such information is not "expose[d]" without the "authorization" of the customer.[1075] The notice requirement advances this purpose further by providing customers the information they need to make informed choices regarding such use, disclosure, and access.[1076] As for the data security rule we adopt, its essential purpose is to safeguard customer PI from inadvertent or malicious "expos[ure]."[1077] The data breach notification rule reinforces these other requirements by providing customers, the Commission, and law enforcement agencies with notice of instances in which customer PI was "exposed without authorization."[1078] Finally, we uphold customers' ability to make decisions about the "expos[ure]" of their data by prohibiting carriers from conditioning service on the surrender of privacy rights.[1079]

363. Yet "protecting the confidentiality" of customer PI involves more than protecting it from unauthorized exposure. AT&T draws a false distinction in arguing that certain aspects of the rules "have nothing to do with confidentiality concerns and instead address only the *uses* of information within an ISP's possession."[1080] On the contrary, upholding customer expectations and choices regarding the use of their proprietary information is an integral part of "protecting the confidentiality of" that information for purposes of Section 222.[1081] In support of this view, we note that restrictions on the use of individually identifiable CPNI are part of the scheme enacted under Section 222(c) to address the "confidentiality of [CPNI],"[1082] and use is the *sole* conduct regulated to address the "confidentiality of carrier information" under subsection (b).[1083] We thus believe the most natural reading of the term "confidentiality" as used in Section 222 is that it encompasses the use of information, not only "disclos[ure]" and permissions of "access." As a coalition of consumer advocacy groups explain, in creating Section 222 "Congress most explicitly directed the Commission to ensure that users are not merely protected from exposure to third parties, but can actively control how the telecommunications provider itself *uses* the information" it collects.[1084] We agree with Verizon that "'protect' and 'use' are different words [that] must have different meanings" within the statute,[1085] but our view is that these meanings differ in terms of breadth. The "protect[ion] of confidentiality" is a concept that is broad enough to cover the different kinds of conduct regulated under Section 222(c): use, disclosure, and permission of access. A carrier that uses, discloses, or permits access to individually identifiable CPNI without customer approval violates its duty under

[1075] *See supra* Part III.D.

[1076] *See supra* Part III.C.

[1077] *See supra* Part III.E.

[1078] *See supra* Part III.F.

[1079] *See supra* Part III.G.1.

[1080] AT&T Comments at 108; *see also* Comcast Comments at 81 ("Even if Section 222(a) confers an independent grant of authority, it is only the authority to adopt rules to 'protect the confidentiality of' proprietary information. This means that any authority the Commission may have under [Section 222(a)] is limited to preventing proprietary information from being exposed without authorization and does not extend to defining its permissible uses such as for marketing or advertising."); Verizon Comments at 59 ("Section 222(a) is far too thin a reed to authorize the entire regulatory apparatus the Commission proposes to erect for PII that is not CPNI. Section 222(a) requires only that carriers 'protect the confidentiality' of information; it does not govern permissible uses of information."); Letter from Loretta Polk, Vice President and Associate General Counsel, NCTA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 2 (filed Oct. 21, 2016).

[1081] *But see* Comcast Comments at 82 (urging the Commission to model its interpretation of Section 222(a) on the FTC's interpretation of different statutory language in the Gramm-Leach-Bliley Act).

[1082] 47 USC § 222(c) (capitalization omitted).

[1083] 47 USC § 222(b) (capitalization omitted).

[1084] Public Knowledge et al. Reply at 4.

[1085] *See* Verizon Comments at 60.

Section 222(c) to protect the "confidentiality" of that CPNI. The same analysis applies under Section 222(a) with regard to customer PI more broadly. Accordingly, we find Section 222(a)'s duty to "protect the confidentiality" of proprietary information supports our rules in full.

### 3. Section 222(c) Provides Authority for the Rules as to CPNI

364. In addition to our Section 222(a) authority discussed above, we have authority under Section 222(c) to adopt the rules articulated in this Order as to individually identifiable CPNI. Subsection (c) obligates carriers to obtain customer approval for any use or disclosure of individually identifiable CPNI, except to provide the underlying telecommunications service or related services.[1086] Our rules implement this mandate.

365. First, our rules establish three methods for obtaining the customer approval required under Section 222(c): inferred consent, opt-in and opt-out. There exists longstanding Commission precedent for requiring the use of these methods,[1087] and commenters generally support some combination of the three.[1088] Under the rules we adopt in this Order, whether a carrier must seek an affirmative "opt-in" depends primarily on whether the information at issue is sensitive.[1089] This distinction is permissible under Section 222(c), which requires customer approval in general for most uses and disclosures of individually identifiable CPNI but does not specify the form this approval must take in any particular circumstance. Second, we require carriers to provide their customers with notice of their privacy policies, both at the point of sale and through posting on their websites and in mobile apps.[1090] This is an essential part of customer approval, as only informed customers can make meaningful decisions about whether and how extensively to permit use or disclosure of their information. The need for this notice to be given at the point of sale is particularly acute in circumstances where approval may take the form of an "opt-out." In such cases, the notice itself is integral to the "approval": customers are presumed to approve of the use or disclosure unless and until they affirmatively "opt out" of such activity. We also prohibit carriers from conditioning the provision of service on consent to the use or disclosure of information protected under Section 222.[1091] We believe that this prohibition is necessary to give effect to the customer approval that subsection (c) requires.[1092]

366. We next require carriers to take reasonable measures to secure the individually identifiable CPNI they collect, possess, use and share.[1093] Such a requirement is necessary to uphold customer decisions regarding use and disclosure of their information and to give effect to the terms of carriers' privacy policies. These other privacy protections would be vitiated if customers lacked any assurance that their information would be secured against unauthorized or inadvertent disclosures, cyber incidents, or other threats to the confidentiality of the information. Finally, we require carriers to report data breaches to their customers, the Commission, and law enforcement, except when a carrier reasonably determines that there is no reasonable likelihood of harm to customers.[1094] The Commission has long required such reporting as part of a carrier's duty to protect the confidentiality of its customers'

---

[1086] *See* 47 USC § 222(c)(1); *see also* 47 U.S.C. § 222(d) (enumerating additional exceptions).

[1087] *See 2002 CPNI Order*, 17 FCC Rcd at 14862-63, para. 2 (providing an overview of "opt-in" and "opt-out" approval requirements adopted in that order).

[1088] *See supra* Part III.D.

[1089] *See supra* Part III.D.

[1090] *See supra* Part III.C.

[1091] *See supra* Part III.G.1.

[1092] *See supra* Part III.G.1.

[1093] *See supra* Part III.E.

[1094] *See supra* Part III.F.

information. [1095] Among other purposes, data breach notifications can meaningfully inform customer decisions regarding whether to give, withhold, or retract their approval to use or disclose their information.

367. In adopting these rules, we are respectful of other parts of the statute that limit or condition the scope of Section 222(c). For instance, our rules preserve the statutory distinction between individually identifiable "CPNI" and "aggregate customer information."[1096] As explained above, we have not modified the definition of either of these terms in a way that would impermissibly narrow the scope of Section 222(c)(3).[1097] In addition, our rules include provisions that implement the exceptions to Section 222(c) that are set forth in Section 222(d).[1098] Finally, our rules are consistent with and pose no obstacle to compliance with the requirements of Sections 222(e) and (g) that subscriber information be disclosed in certain defined circumstances.[1099]

### B. Sections 201(b) and 202(a) Provide Additional Authority to Protect Against Privacy Practices That Are "Unjust or Unreasonable" or "Unjustly or Unreasonably Discriminatory"

368. While Section 222 provides sufficient authority for the entirety of the rules we adopt in this Order, we conclude that Sections 201(b) and 202(a) also independently support the rules, because they authorize the Commission to prescribe rules to implement carriers' statutory duties not to engage in conduct that is "unjust or unreasonable" or "unjustly or unreasonably discriminatory."[1100] Our enforcement of Sections 201(b) and 202(a) in the context of BIAS finds expression in the "no unreasonable interference/disadvantage" standard adopted in the *2015 Open Internet Order*.[1101] As we explained in the *2015 Open Internet Order*, "practices that fail to protect the confidentiality of end users' proprietary information" are among the potential carrier practices that are "unlawful if they unreasonably interfere with or disadvantage end-user consumers' ability to select, access, or use broadband services, applications, or content."[1102] Above, we noted that financial incentives to surrender privacy rights in connection with BIAS are one sort of practice that could potentially run afoul of this standard, and we will accordingly monitor such practices closely. Yet, aside from prohibiting "take-it-or-leave-it" offerings, we do not engage in any *ex ante* prohibition of such practices.[1103]

369. In addition, Sections 201(b) and 202(a) provide backstop authority to ensure that no gaps are formed in Congress's multi-statute regulatory framework governing commercial privacy and data security practices. As explained above, the FTC's enabling statute grants the agency broad authority with respect to such practices, but denies it authority over common carrier activities of common carriers.[1104]

---

[1095] *See 2007 CPNI Order*, 22 FCC Rcd at 6943-45, paras. 26-32; *see also* 47 CFR § 64.2011.

[1096] *See* 47 U.S.C. § 222(h)(1) ("customer proprietary network information"), (h)(2) ("aggregate customer information").

[1097] *See supra* Part III.B.4.

[1098] *See infra* Appx. A.

[1099] *See* 47 U.S.C. § 222(e), (g).

[1100] 47 U.S.C. §§ 201(b), 202(a); *see Broadband Privacy NPRM*, 31 FCC Rcd at 2596, paras. 305-06.

[1101] *2015 Open Internet Order*, 30 FCC Rcd at 5609, para. 22, 5659-69, paras. 133-53.

[1102] *Id.* at 5662, para. 141.

[1103] *See supra* para. 297. *But see* Nokia Reply at 9 ("[F]or innovation to happen throughout the entire ecosystem, the Commission must avoid policy frameworks that impose *ex ante* prohibitions on potential sources of value creation particularly when those prohibitions are imposed on only one segment of the ecosystem: once again, in this instance, providers of BIAS.").

[1104] *See supra* Part IV.A.2.

That leaves this Commission as the sole federal agency with authority to regulate telecommunications carriers' treatment of personal and proprietary customer data obtained in the provision of BIAS and other telecommunications services. While we believe Section 222 endows the Commission with ample authority for the rules we adopt today to protect such data, both as to CPNI and other customer PI, Sections 201(b) and 202(a) provide an independent legal basis for the rules. Indeed, both this Commission and the FTC have long recognized that similar conduct would tend to run afoul of Section 201(b) and of Section 5 of the FTC Act, the statutory linchpin of the FTC's privacy and data security enforcement work.[1105] Thus, asserting Sections 201(b) and 202(a) as a basis for our rules merely preserves consistent treatment of companies that collect sensitive customer information—including Social Security numbers and financial records—regardless of whether the company operates under the FCC's or FTC's authority.

370. Accordingly, for these reasons and others discussed throughout this Report and Order, we find that Sections 201(b) and 202(a) by their own terms, consistent the *2015 Open Internet Order*'s interpretation of those provisions in the context of BIAS, provide authority for the adoption of these rules. Also, while we recognize that telecommunications services other than BIAS are beyond the reach of the open Internet rules, providers of such services remain subject to enforcement directly under Sections 201(b) and 202(a), and those provisions authorize adoption of these rules.

### C. Title III of the Communications Act Provides Independent Authority

371. With respect to mobile BIAS and other mobile telecommunications services, the rules we adopt in this Order are also independently supported by our authority under Title III of the Act to protect the public interest through spectrum licensing.[1106] Section 303(b) directs the Commission, consistent with the public interest, to "[p]rescribe the nature of the service to be rendered by each class of licensed stations and each station within any class."[1107] These rules do so.[1108] They lay down rules about "the nature of the service to be rendered" by licensed entities providing mobile telecommunications service; making clear that this service may not be offered in ways that harm the interests of consumers is protecting the confidentiality of their personal information.[1109] Today's rules specify the form this service must take for those who offer it pursuant to license. In providing such licensed service, carriers must adhere to the rules we adopt today. Section 303(r) also supplements the Commission's authority to carry out its mandates through rulemaking,[1110] and Section 316 authorizes the Commission to adopt new conditions on existing licenses if it determines that such action "will promote the public interest, convenience, and necessity."[1111] Throughout this Order, we determine that the rules adopted here will promote the public interest.

---

[1105] *See* FCC and FTC, Joint FCC/FTC Policy Statement for the Advertising of Dial-Around and Other Long-Distance Services to Consumers, 65 Fed. Reg. 44053-02, 44054 (July 17, 2000).

[1106] *See Broadband Privacy NPRM*, 31 FCC Rcd at 2598, para. 310.

[1107] 47 U.S.C. § 303(b); *see, e.g.*, *2015 Open Internet Order*, 30 FCC Rcd at 5725, paras. 285-87.

[1108] *See* Public Knowledge White Paper at 20-21. *But see* T-Mobile Comments at 23; CTIA Comments at 71-73.

[1109] *Cf., e.g.*, *Facilitating the Deployment of Text-To-911 and Other Next Generation 911 Applications*, PS Docket Nos. 11-153, 10-255, Report and Order, 28 FCC Rcd 7556, 7587-92, paras. 89-99 (2013); *Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications*, PS Docket Nos. 15-80, 11-82, ET Docket No. 16-63, Report and Order, Further Notice of Proposed Rulemaking, and Order on Reconsideration, 31 FCC Rcd 5817, 5896-97, paras. 202-05 (2016).

[1110] 47 U.S.C. § 303(r); *see 2015 Open Internet Order*, 30 FCC Rcd at 5725, para. 287 (citing *Cellco P'ship v. FCC*, 700 F.3d 534, 543 (D.C. Cir. 2012)).

[1111] 47 U.S.C. § 316(a)(1); *see 2015 Open Internet Order*, 30 FCC Rcd at 5725, para. 287.

### D. The Rules Are Also Consistent With the Purposes of Section 706 of the 1996 Act

372. We also believe that our rules are consistent with Section 706 of the 1996 Act and will help advance its objective of promoting "the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans."[1112] We agree with commenters that strong broadband privacy and data security practices tend to promote consumer trust and confidence, which can increase demand for broadband and ultimately spur additional facilities deployment.[1113] Moreover, we have adopted a flexible set of rules that are largely consistent with the FTC's approach to privacy regulation, creating a measure of consistency across the telecommunications ecosystem. We thus reject any argument that the rules will impose novel costs or burdens on BIAS providers and other telecommunications carriers that would discourage further deployment of advanced services.[1114]

### E. We Have Authority to Apply the Rules to Interconnected VoIP Services

373. In 2007, the Commission exercised ancillary jurisdiction to extend its Part 64 CPNI rules to interconnected VoIP services.[1115] Since then, interconnected VoIP providers have operated under these rules. Today, we exercise the same authority[1116] to apply to interconnected VoIP services the harmonized set of rules we are adopting for BIAS and other telecommunications services. Interconnected VoIP services remain within the Commission's subject matter jurisdiction, and we continue to find that the application of customer privacy requirements to these services is "reasonably ancillary to the effective performance" of our statutory responsibilities.[1117] As the Commission explained in 2007, "American consumers [can reasonably] expect that their telephone calls are private irrespective of whether the call is made using the service of a wireline carrier, a wireless carrier, or an interconnected VoIP provider."[1118]

---

[1112] *See* 47 U.S.C. § 1302(a).

[1113] *See* Greenlining Institute Comments at 18-19 ("[C]ommodification and use of the customer's personal information without informed consent [interferes] with a consumer's access to the BIAS telecommunications transport, and lessen consumer trust (and the public's trust) in the integrity of BIAS service."); Public Knowledge White Paper at 22-23 ("[P]rotection of CPNI may spur consumer demand . . . driving demand for broadband connections, and consequently encouraging more broadband investment and deployment consistent with Section 706.") (citing *2007 CPNI Order*, 22 FCC Rcd at 6927, para. 59).

[1114] *But see* CTIA Comments at 67. ("[F]urther network investment will not take place if ISPs lack the incentives or resources to continue to deploy broadband infrastructure."); ACA Comments at 70-71 ("In fact, the proposed rules are more likely to shove a stick in the spokes of the virtuous circle than perpetuate it."); Washington Legal Foundation Comments at 7-9.

[1115] *See 2007 CPNI Order*, 22 FCC Rcd at 6954-57, paras. 54-59; *see also* 47 CFR § 64.2003(o) (defining "telecommunications carrier or carrier" for purposes of the CPNI rules to include interconnected VoIP providers).

[1116] We make no decisions in this Order on the regulatory classification of interconnected VoIP services.

[1117] *See 2007 CPNI Order*, 22 FCC Rcd at 6955, para. 55; *see also United States v. Southwestern Cable*, 392 U.S. 157, 177-78 (1968) (setting forth the two-part "ancillary jurisdiction" test); *Comcast Corp. v. FCC*, 600 F.3d 642, 654 (D.C. Cir. 2010) (holding that ancillary jurisdiction must be "necessary to further its regulation of activities over which it does have express statutory authority"). We conclude that our jurisdiction to apply the rules in this Order to interconnected VoIP providers is just as strong as it was in 2007. In addition to the analysis in the *2007 CPNI Order*, 22 FCC Rcd at 6954-57, paras. 54-59, we observe that applying these obligations to interconnected VoIP providers is necessary to protect the privacy of customers of BIAS providers and other telecommunications services. Given the growth in interconnected VoIP and the extent to which it increasingly is viewed as a substitute for traditional telephone service, telecommunications carriers could be disadvantaged if they were subject to these requirements but other interconnected VoIP providers were not. Consumers' privacy interests could benefit to the extent that providers of competitive services are subject to the same obligations. Furthermore, in light of Congress's amendment of the Act, including Section 222, to apply E-911 obligations to interconnected VoIP, the 911 system could be disrupted to the extent that our harmonized Section 222 regime were no longer to apply to interconnected VoIP.

[1118] *2007 CPNI Order*, 22 FCC Rcd at 6956, para. 56.

Furthermore, "extending Section 222's protections to interconnected VoIP service customers is necessary to protect the privacy of wireline or wireless customers that place calls to or receive calls from interconnected VoIP providers."[1119] These rationales hold equally true today. In addition, in 2008, Congress ratified the Commission's decision to apply Section 222's requirements to interconnected VoIP by adding language to Section 222 that expressly covers "IP-enabled voice service,"[1120] defined expressly to incorporate the Commission's definition of "interconnected VoIP service."[1121]

374. We believe that the rules we adopt today are no less suitable for interconnected VoIP service, and are in fact better tailored to that service, than the rules adopted in 2007. As explained above, we have adopted a harmonized set of rules for voice services and BIAS. There is considerable flexibility built into these rules to permit providers of different services and with different business models to adopt privacy practices appropriate for their businesses.[1122] Moreover, while the Order expands on existing obligations in some respects, it also streamlines or removes several of the more prescriptive requirements codified in the existing rules.[1123] We have also broadened the enterprise customer exemption[1124] and taken measures to address the potential for disproportionate impacts on smaller providers, including those that provide interconnected VoIP service.[1125] We therefore are not persuaded that our rules will overburden interconnected VoIP providers in particular with "expand[ed] privacy obligations" that would "forestall competition."[1126]

### F. Constitutional Considerations

#### 1. Our Sensitivity-Based Choice Framework Is Supported by the Constitution

375. In adopting section 222, Congress identified a substantial government interest in protecting the privacy of customers of telecommunications services. In adopting and revising rules pursuant to section 222 we have recognized and honored that same substantial interest. Nonetheless, because our rules require carries to provide their customers with tools to grant or deny the carriers approval to use customer information for marketing and other purposes, they can be said to restrict certain types of commercial speech by telecommunications carriers, and therefore must be narrowly tailored to further that substantial government interest.[1127] In the *Central Hudson* case, the Supreme Court found that in order to meet the requirement that rules implicating commercial speech are narrowly tailored to meet a substantial government interest, the government must conduct a threshold inquiry regarding whether the commercial speech concerns lawful activity and is not misleading.[1128] If this threshold requirement is met, as it is here, the government may restrict the speech only if (1) the government interest advanced by the regulation is substantial; (2) the regulation directly and materially advances that interest; and (3) the regulation is not more extensive than necessary to serve the interest.[1129] By adopting a sensitivity-based

[1119] *Id*. at 6956, para. 57.

[1120] *See* NET 911 Act; *see also* 47 U.S.C. § 222(d)(4), (f)(1), (g).

[1121] 47 U.S.C. § 222(d)(4), (f)(1), (g) (applying provisions of section 222 to "IP-enabled voice service"); § 615b(8) (defining "IP-enabled voice service" as having "the meaning given the term 'interconnected VoIP service' by section 9.3 of the Federal Communications Commission's regulations (47 CFR 9.3)").

[1122] *See, e.g.*, *supra* para. 242.

[1123] *See, e.g.*, *supra* para. 234 (removal of annual certifications requirement); para. 253 (customer authentication).

[1124] *See supra* Part III.H.2. *But see* Voice on the Net Coalition Comments at 6.

[1125] *See infra* Appx. B.

[1126] *But see* Voice on the Net Coalition Comments at 4.

[1127] *Central Hudson Gas & Electric Corp. v. Pub. Serv. Comm'n of N. Y.*, 447 U.S. 557 (1980).

[1128] *Central Hudson*, 447 U.S. at 566; *see also U.S. West*, 182 F.3d at 1233.

[1129] *Central Hudson*, 447 U.S. at 566; *NCTA v. FCC*, 555 F.3d at 1000; *U.S. West*, 182 F.3d at 1233.

framework for giving customers tools to make decisions about their telecommunications carriers' use and sharing of their information, the rules we adopt today meet that three part test.

### a. Substantial Government Interest

376. We agree with the D.C. Circuit that Section 222 seeks to promote a substantial public interest in protecting consumer privacy.[1130] The record indicates broad agreement on this point,[1131] which is further reinforced by the wealth of case law reiterating the substantial state interest in protecting privacy.[1132] Section 222 is designed to protect the interest of telecommunications consumers in limiting unexpected and unwanted use and disclosure of their personal information by carriers that must collect such information in order to provide the telecommunications service,[1133] and the record further indicates that customers' ability to know and control the information gathered by virtue of their relationships with their telecommunications providers also comprises a substantial government interest.[1134]

377. The failure to adequately protect customer PI can have myriad negative consequences for customers and society at large. Revelations of private facts have been recognized as harms since at least the time of Justices Warren and Brandeis.[1135] Failure to protect the privacy of consumer information can, of course create a risk of financial harm, identity theft and physical threat.[1136] The Commission has also found that emotional and dignitary harms are privacy harms, in other contexts.[1137] The FTC similarly recognized that harms beyond the economic, physical, and intrusive are nonetheless real and

[1130] *NCTA v. FCC*, 555 F.3d at 1001 (2009) (internal citations omitted) ("The Tenth Circuit supposed that § 222 sought to promote a governmental interest in protecting against the disclosure of 'information [that] could prove embarrassing,' and it doubted whether this interest could be deemed 'substantial.' We do not share the Tenth Circuit's doubt. For one thing, we have already held, in an analogous context, that 'protecting the privacy of consumer credit information' is a 'substantial' government interest. For another thing, we do not agree that the interest in protecting customer privacy is confined to preventing embarrassment as the Tenth Circuit thought. There is a good deal more to privacy than that. . . . The Supreme Court knows this as well Congress: 'both the common law and the literal understanding of privacy encompass the individual's control of information concerning his or her person.'").

[1131] CTIA Comments at 81-82 (recognizing substantial interest in customers' control of their personal information); CTIA Sept. 16, 2016 *Ex Parte* at 18-19 (conceding substantial privacy interest in online ecosystem while questioning the breadth of the proposed rules); Consumer Federation of California Reply at 8-9 (enumerating state interests in privacy found throughout federal and state law).

[1132] *See, e.g.*, *NCTA v. FCC*, 555 F.3d at 1001; *Ohio v. Akron Ctr. for Reprod. Health*, 497 U.S. 502, 529 (1990); *Carey v. Population Servs., Intern.*, 431 U.S. 678, 684 (1977); *Whalen v. Roe*, 429 U.S. 589, 599 (1977); *Griswold v. Connecticut*, 381 U.S. 479, 483 (1965); *Florida Bar v. Went For It, Inc.*, 515 U.S. 618, 625 (1995); *Edenfield v. Fane*, 507 U.S. 761, 766 (1993). *US West v. FCC*, frequently cited in opposition to the constitutionality of this Order, acknowledges the "substantial state interest" in privacy, and that Section 222, in particular, has a "specific and dominant purpose" of protecting consumer privacy. 182 F.3d at 1234, 1236.

[1133] *See, e.g.*, *2002 CPNI Order*, 17 FCC Rcd at 14875, para. 33.

[1134] *See supra* note 1131.

[1135] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 213 (1890) ("If the invasion of privacy constitutes a legal *injuria*, the elements for demanding redress exist, since already the value of mental suffering, caused by an act wrongful in itself, is recognized as a basis for compensation."); *see also* William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383, 389 (1960) (enumerating privacy torts, including "[p]ublic disclosure of embarrassing private facts about the plaintiff").

[1136] *See, e.g.*, *supra* note 696 (acknowledging potential for financial or physical harm).

[1137] In implementing the Truth in Caller ID Act, the Commission found that "harm" was a broad concept encompassing financial, physical, and emotional harm. *See Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, WC Docket No. 11-39, Report and Order, 26 FCC Rcd 9114, 9122, para. 22 (2011).

cognizable,[1138] and the Administration's CPBR defines "privacy risk" to include the potential to cause "emotional distress, or physical, financial, professional, or other harm to an individual."[1139]

378. Some commenters argue that the Commission can only demonstrate an interest in addressing the *disclosure* of customer PI and not in how carriers' *use* customer PI.[1140] We disagree. The Supreme Court has recognized that an important part of privacy is the right to know and have an effective voice in how one's information is being used, holding that "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."[1141] The D.C. Circuit has similarly held that "it is widely accepted that privacy deals with determining for oneself when, how, and to whom personal information will be disclosed to others."[1142] This conception of privacy is embedded within the history of the Fair Information Practice Principles[1143] (which form the broadly-supported[1144] basis for our privacy rules), and within the long history of communications privacy as well.[1145] Scholarly literature on privacy also finds that misuse by the collecting entity can harm individuals' privacy, even apart from disclosure.[1146]

379. Direct surveys confirm consumers' recognition of these harms. According to the 2016 Consumer Privacy Index by TRUSTe and the National Cybersecurity Alliance, 68 percent of consumers were more concerned about not knowing how personal information was collected online than losing their principal income.[1147] The Consumer Privacy Index also indicated that large numbers of consumers want control over who has access to personal information (45 percent), how that information is used (42 percent), and the type of information collected (41 percent).[1148] Consumers also object to their data being

[1138] 2012 FTC Privacy Report at 7-9.

[1139] 2015 Administration CPBR Discussion Draft, § 4(g).

[1140] *See, e.g.*, Comments of Laurence Tribe on behalf of CTIA, NCTA and USTelecom at 27-29 (Tribe Comments).

[1141] *U.S. Dept. of Justice v. Reporters Comm. For Freedom of Press*, 489 U.S. 749, 763 (1989) (cited in *NCTA v. FCC*, 555 F.3d at 1001); *see* OTI Reply at 18-19.

[1142] *NCTA v. FCC*, 555 F.3d at 1001; *see* OTI Reply at 20.

[1143] From their inception, FIPPs have recognized privacy as an individual's right to control *uses* of information about him—not merely to control their disclosures. *See* HEW Report at 40-41 (finding that privacy is affected by the recording, disclosure, and use of identifiable information).

[1144] *See, e.g.*, 2012 FTC Privacy Report at i; 2012 White House Privacy Blueprint; Online Interest-Based Advertising Accountability Comments at 2; EPIC Comments at 2-3; Privacy Rights Clearinghouse at 2-3; McDonald Reply at 1; Charter Comments at 6-7; Internet Association Comments at 6-7; ITIC Comments at 4; USTelecom Comments at 11-12.

[1145] The Federal Radio Act of 1927, and the original language of the Communications Act of 1934, prohibited carriers not only from publishing or divulging information relevant to communications, but also from making uses of the information solely to benefit themselves. *See* Max D. Paglin, A Legislative History of the Communications Act of 1934, 721 (1989); Communications Act of 1934 § 605, 48 Stat. 1103 (now codified at 47 U.S.C. § 605(a)); Public Knowledge Reply at 4.

[1146] *See* Daniel Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477 (2006); M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 Ind. L.J. 11131, 1133 (2011) (noting the existence of both subjective and objective privacy harms); OTI Reply at 20, 27.

[1147] Consumer Privacy Index 2016; OTI Reply at 22.

[1148] Consumer Privacy Index 2016. A Bain & Company survey of over 900 consumers found that two-thirds of them felt it should be "illegal for companies to collect or use . . . data without getting prior consent." Bain & Company Press Release, *How can companies acquire customer data while building customer loyalty at the same time? Ask permission*, Bain & Company (May 11, 2015), http://bain.com/about/press/press-releases/Digital-privacy-survey-2015-press-release.aspx; OTI Reply at 23.

used, and not only disclosed, in the service of targeted advertising.[1149] These studies demonstrate empirically that consumers find loss of control over their information harmful, even apart from potential monetary loss.

380. The risk of privacy harms directly affects behavior and activity by eroding trust in and use of communications networks. As the Commission has found, if "consumers have concerns about the privacy of their personal information, such concerns may restrain them from making full use of broadband Internet access services and the Internet, thereby lowering the likelihood of broadband adoption and decreasing consumer demand."[1150] There is evidence that unexpected uses of private customer information can increase fear, uncertainty, powerlessness, and vulnerability.[1151] This is not a purely academic concern; the National Telecommunications and Information Administration (NTIA) recently found that fear of privacy violations chills online activity, to the point where privacy concerns prevented 45 percent of online households from conducting financial transactions, buying goods or services, or posting on social networks.[1152] The Consumer Privacy Index found that 74 percent of respondents limited their activity in the past year due to privacy concerns, including 36 percent who stopped using certain websites and 29 percent stopped using an app.[1153] In contrast, when companies protect consumers' privacy, consumers' adoption of their products, services, and technologies increases.[1154]

381. We therefore conclude that the government's interest in protecting customer privacy is a substantial one—a fact recognized widely by consumers, the courts, and the Communications Act.

**b. Direct and Material Advancement**

382. The choice framework that we adopt directly and materially advances the substantial government interests discussed above.[1155] We find that requiring customer approval for use and disclosure of customer PI prevents information uniquely collected and collated by telecommunications carriers from being used or disclosed against a customer's wishes, consistent with customer expectations, and as such directly and materially advances the government's substantial government interest in protecting customers' privacy.[1156] Customers have an important interest in ensuring that their personal

[1149] Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities that Enable It* 8, 13 (2009); OTI Reply at 23-24, n.69

[1150] *2015 Open Internet Order*, 30 FCC Rcd at 5821, para. 464.

[1151] Solove at 520; OTI Reply at 29.

[1152] Rafi Goldberg, NTIA, Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

[1153] Consumer Privacy Index 2016; OTI Reply at 25.

[1154] 2012 FTC Privacy Report at 8-9.

[1155] *U.S. West*, 182 F.3d at 1237.

[1156] While we recognize that adopting these rules cannot protect customers from privacy violations that originate from entities that are not telecommunications providers, the fact that the rules do not create universal privacy protection does not mean that customers' privacy interests are not advanced. *See, e.g.*, *Williams-Yulee v. Florida Bar Ass'n*, 135 S. Ct 1656, 1668 (2015) (citing *R.A.V. v. St. Paul*, 505 U.S. 377, 387 (1992)) ("Although a law's underinclusivity raises a red flag, the First Amendment imposes no freestanding 'underinclusiveness limitation.'"); *id.* ("A State need not address all aspects of a problem in one fell swoop; policymakers may focus on their most pressing concerns. We have accordingly upheld laws—even under strict scrutiny—that conceivably could have restricted even greater amounts of speech in service of their stated interests."); *see also Trans Union Corp. v. F.T.C.*, 267 F.3d 1138, 1143 (D.C. Cir. 2001) (citing *Blount v. SEC*, 61 F.3d 938, 946 (1995))("A regulation is not fatally underinclusive simply because an alternative regulation, which would restrict more speech or the speech of more

(continued….)

information is not used by their BIAS providers or other telecommunications carrier without their prior approval in a way that the customers do not or cannot reasonably expect.[1157]

383. In addition, requiring telecommunications carriers to obtain opt-in approval for the use and sharing of sensitive customer PI materially advances the government's interest in protecting telecommunications customers' privacy and in enabling customer to avoid unwanted and unexpected use and disclosure of sensitive customer PI. The opt-in requirements we adopt today provide telecommunications customers control over how their sensitive customer PI can be used for purposes besides those essential to the delivery of service. Likewise, we conclude that opt-out directly and materially advances the government's interest that a customer be given an opportunity to approve (or disapprove) uses of his non-sensitive customer PI by mandating that carriers provide prior notice to customers along with an opportunity to decline the carriers' requested use.

#### c. The Rules Are No More Burdensome than Necessary to Advance the Government's Substantial Interest

384. *Central Hudson* requires that regulations on commercial speech be no more extensive than necessary to advance the substantial interest.[1158] This does not mean that a regulation must be as narrow as possible, however. The Supreme Court has held that "[t]he government is not required to employ the least restrictive means conceivable . . . a fit that is not necessarily perfect, but reasonable; that represents not necessarily the single best disposition but one whose scope is in proportion to the interest served."[1159] As explained below, our framework satisfies this test.

385. *Non-Sensitive Customer PI.* In most cases involving what we categorize as non-sensitive customer PI, we find opt-in approval unnecessary to ensure adequate customer choice. We therefore find that the opt-out framework for use and sharing of non-sensitive customer PI is a narrowly tailored means to directly and materially advance the government's interest in protecting consumers from unapproved use of non-sensitive customer PI by telecommunications carriers. The record reflects that non-sensitive information naturally generates fewer privacy concerns for customers, and as such does not require the same level of customer approval as for sensitive customer PI.[1160] Further, the record reflects that customers expect their providers to use their non-sensitive information to market improved services, lower-priced service offerings, promotional discounts for new services, and other offers of value from telecommunications carriers and their affiliates. The record also demonstrates that customers can reap significant benefits in the form of more personalized service offerings and possible cost saving from their carriers providing services based on the non-sensitive customer PI that carriers collect.[1161] Requiring carriers to obtain opt-out consent from customers to use and share their non-sensitive information grants carriers flexibility to make improvements and innovations based on customer PI, while still ensuring that customers can control the use and sharing of their non-sensitive customer PI.

386. *Sensitive Customer PI.* We require opt-in approval only for the most important

(Continued from previous page)
people, could be more effective . . . a rule is struck for *under*inclusiveness only if it cannot fairly be said to advance any genuinely substantial government interest."). *But see* Tribe Comments at 22.

[1157] *See supra* para. 87.

[1158] *Central Hudson*, 447 U.S. at 569-70.

[1159] *Greater New Orleans Broad. Ass'n v. United States*, 527 U.S. 173, 188 (1999) (internal quotation marks omitted).

[1160] *See supra* para. 198.

[1161] The Commission has previously found, in the context of its voice CPNI rules, that "telecommunications consumers expect to receive targeted notices from their carriers about innovative telecommunications offerings that may bundle desired telecommunications services and/or products, save the consumer money, and provide other consumer benefits." *2002 CPNI Order*, 17 FCC Rcd at 14877, para. 36.

information to customers—sensitive customer PI. We find that requiring opt-in approval for the use and sharing of sensitive customer PI is a narrowly-tailored means of advancing the Commission's interests in protecting the privacy of sensitive customer PI, and in enabling customers meaningful choice on the use and sharing of such sensitive customer PI. As discussed above in detail, the record reflects that customers reasonably expect that their sensitive information will not be shared without their affirmative consent.[1162] Furthermore, it has been our experience implementing Section 222 that sensitive information, being more likely to lead to more serious customer harm, requires additional protection,[1163] and the record here supports that view .[1164] Commenters nearly unanimously argue that use and sharing of sensitive customer information be subject to customer opt-in approval.[1165] Although we recognize that opt-in imposes additional costs, we find that opt-in is warranted to maximize opportunities for informed choice about sensitive information.

387. In contrast, we find that opt-out consent would be insufficient to protect the privacy of sensitive customer PI.[1166] As we explain above, research has shown that default choices can be "sticky," meaning that consumers will remain in the default position, even if they would not have actively chosen it.[1167] From this, we conclude that an opt-out regime for use and sharing of sensitive customer PI would not materially and directly advance the government's interest in protecting customer privacy because it would not adequately address customers' expectations that their sensitive customer PI is not used without their affirmative consent.

### 2. Other First Amendment Arguments

388. *Strict Scrutiny Under* Sorrell. The customer choice rules we adopt today do not impermissibly target particular speech or speakers, and thus a strict scrutiny analysis under *Sorrell v. IMS Health Inc.*[1168] is unwarranted. In *Sorrell*, the state of Vermont specifically targeted "drug detailers" and their marketing speech, which the state disfavored, in a framework that otherwise permitted communications about medical prescriptions.[1169] By contrast, the rules adopted here do not disfavor any particular activity. While a large number of commenters are particularly concerned with the limitations that the rules may place upon marketing, customers' privacy interests reach far beyond targeted marketing, to include for instance risk of identity theft or other fraud, stalking, and revelations of private communications, as well as the harms inherent in lacking control over the uses of their proprietary information.

389. The fact that Section 222 and our rules thereunder apply to certain types of information and certain providers is a function of their tailoring, not indications that they are content-based. As explained above, our rules are tailored to address unique characteristics of telecommunications services and of the relationship between telecommunications carriers and their customers.[1170] Were we to interpret *Sorrell* to hold sector-specific privacy laws such as Section 222 and our rules to be content-based simply

[1162] *See supra* para. 193, note 553.

[1163] *See, e.g.*, *2007 CPNI Order*, 22 FCC Rcd at 6949-52, paras. 44-46.

[1164] *See supra* para. 193.

[1165] *See supra* para. 193.

[1166] As a functional matter, while opt-out consent has been described as the least restrictive form of obtaining customer approval, it is only "marginally less intrusive than opt-in for First Amendment purposes." *See* CDT Reply at 9, citing *NCTA v. FCC*, 555 F.3d at 1002.

[1167] *See supra* para. 194.

[1168] 564 U.S. 552 (2011).

[1169] *Sorrell*, 564 U.S. at 565.

[1170] *See supra* Part. III.A.

because they do not apply to all entities equally, it would stand to invalidate nearly every federal privacy law, considering the sectoral nature of our federal privacy statutes.[1171] However, *Sorrell* stands for no such thing, itself citing HIPAA—limited to covering certain specific entities and types of information—as an example of a constitutionally sound privacy protection.[1172]

390. *Compelled Speech*. Some commenters argue that the notice requirements unconstitutionally compel speech from carriers.[1173] We disagree. Requirements to include purely factual and uncontroversial information in commercial speech are constitutional so long as they are reasonably related to the government's substantial interest in protecting consumers.[1174] The notice requirements we adopt here, just like the notice requirements in the CPNI rules before them and like numerous notice and labeling requirements before,[1175] require only that companies provide factual and uncontroversial information to consumers.

391. *Constitutional Avoidance*. Some commenters raise arguments citing the canon of constitutional avoidance.[1176] We do not believe this is applicable. Constitutional avoidance is a canon of statutory interpretation that states that a court should not resolve a case "by deciding a constitutional question if it can be resolved in some other fashion."[1177] As the Supreme Court has held, "[t]he so-called canon of constitutional avoidance is an interpretive tool, counseling that ambiguous statutory language be construed to avoid serious constitutional doubts." [1178] The Court further found "no precedent for applying it to limit the scope of authorized executive action."[1179] The canon of constitutional avoidance therefore does not apply to this proceeding, does not require that we adopt an opt-out framework, and does not mandate that we avoid regulating in this space.

392. Finally, to the extent that parties argue that today's rules deny carriers a First Amendment right of editorial control or impose prior restraints that implicate the First Amendment,[1180] we note that it is well established that common carriers transmitting speech through communications networks are not speakers for First Amendment purposes.[1181]

---

[1171] Indeed, if laws impacting expression were considered content-based for not being universal, nearly every privacy and intellectual property law would need to pass strict scrutiny.

[1172] *Sorrell*, 564 U.S. at 573; ACLU Reply at 5. Similarly, use-based exceptions to Section 222 and our rules do not render the statute or rules content-based any more than purpose-based exceptions in HIPAA. *Cf.* OTI Reply at 11-12.

[1173] T-Mobile Comments at 42-44; Washington Legal Foundation Comments at 14-15.

[1174] *See Zauderer v. Office of Disc. Counsel*, 471 U.S. 626, 651 (1985); *see also, e.g.*, *Am. Meat Inst. v. U.S. Dep't of Agriculture*, 760 F.3d 18, 22 (D.C. Cir. 2014) (holding that country-of-origin labeling requirements were not unconstitutionally compelled speech); *N.Y. State Rest. Ass'n v. N.Y. City Bd. of Health*, 556 F.3d 114, 133 (2d Cir. 2009); *Nat'l Elec. Mfrs. Ass'n v. Sorrell*, 272 F.3d 104, 113-15 (2d Cir. 2001).

[1175] *Id.*

[1176] *See, e.g.*, Tribe Comments at 38-39.

[1177] Black's Law Dictionary, 377 (10th ed. 2014).

[1178] *FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 516 (2009) (citing *Edward J. DeBartolo Corp. v. Florida Gulf Coast Building & Constr. Trades Council*, 485 U.S. 568, 575 (1988)).

[1179] *Id.*

[1180] *See* Letter from Mike Wendy, President, MediaFreedom to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, at 1 (filed Oct. 18, 2016).

[1181] *See U.S. Telecom Ass'n v. FCC*, 825 F.3d at 742 ("[T]he communicative intent of the individual speakers who use such transmission networks does not transform the networks themselves into speakers."); *U.S. v. Western Elec. Co.*, 673 F. Supp. 525, 586 n. (D.D.C. 1987) (Greene, J.).

### G. Severability

393. In this Report and Order, we adopt a unified scheme of privacy protections for customers of BIAS and other telecommunications services. While the unity and comprehensiveness of this scheme maximizes its utility, we clarify that its constituent elements each operate independently to protect consumers. Were any element of this scheme stayed or invalidated by a reviewing court, the elements that remained in effect would continue to provide vital consumer protections. For instance, telecommunications customers have long benefitted from Commission rules governing the treatment CPNI. The rules we adopt today would continue to ensure that such information is protected even if they did not extend to all of the information we define as customer PI. Similarly, the different forms of conduct regulated under Section 222—use, disclosure, and permission of access—each pose distinct threats to the confidentiality of customer PI. Finally, the benefit of the rules for customers of any particular telecommunications service does not hinge on the same rules applying to other telecommunications services. Accordingly, we consider each of the rules adopted in this Report and Order to be severable, both internally and from the remaining rules. In the event of a stay or invalidation of any part of any rule, or of any rule as it applies as to certain services, providers, forms of conduct, or categories of information, the Commission's intent is to otherwise preserve the rule to the fullest possible extent.

## V. PROCEDURAL MATTERS

### A. Regulatory Flexibility Analysis

394. As required by the Regulatory Flexibility Act of 1980 (RFA),[1182] an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *Broadband Privacy NPRM*.[1183] The Commission sought written public comment on the possible significant economic impact on small entities regarding the proposals address in the *2016 Broadband Privacy NPRM*, including comments on the IRFA. Pursuant to the RFA, a Final Regulatory Flexibility Analysis is set forth in Appendix B.

### B. Paperwork Reduction Act

395. This document contains new information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. It will be submitted to the Office of Management and Budget (OMB) for review under Section 3507(d) of the PRA. OMB, the general public, and other federal agencies are invited to comment on the new information collection requirements contained in this proceeding. In addition, we note that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, see 44 U.S.C. 3506(c)(4), we previously sought specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees.

396. In this present document, we require telecommunications carriers to: 1) disclose their privacy practices to customers; 2) provide customers a mechanism for opting in or out of the use or sharing of their customer PI; 3) notify customers of any unauthorized disclosure or use of their customer PI; and 4) provide customers clear and conspicuous notice regarding any financial incentive programs related to the use or disclosure of their customer PI. We have assessed the effects of these changes and find that the burdens on small businesses will be addressed through the implementation plan adopted in this Order, as well as accommodations made in response to small carriers concerns on the record. The privacy policy notice rules, for example, afford carriers significant flexibility on how to comply with the notice requirement. They mandate neither a specific format nor specific content to be contained in the notice. We have also directed the Commission's Consumer Advisory Committee to develop a standardized notice format that will serve as a safe harbor once adopted. Similarly, the choice rules do

[1182] *See* 5 U.S.C. § 603.

[1183] *Broadband Privacy NPRM*, Appx. B.

not prescribe a specific format for accepting a customer's privacy choices. The choice rules are also significantly harmonized with existing rules, with which most small providers currently comply. Additionally, the heightened requirements for financial incentive programs allow all providers considerable latitude to develop their programs within the parameters of the rule. Finally, the data breach notification rules incorporate both a harm trigger and notification timeline that significantly lessen the implementation requirements for small providers.

### C. Congressional Review Act

397. The Commission will send a copy of this Report and Order in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act (CRA), see 5 U.S.C. § 801(a)(1)(A).

### D. Accessible Formats

398. To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an email to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (tty).

## VI. ORDERING CLAUSES

399. Accordingly, IT IS ORDERED that, pursuant to Sections 1, 2, 4(i)-(j), 201, 202, 222, 303(b), 303(r), 316, 338(i), 631, and 705 of the Communications Act of 1934, as amended, and Section 706 of the Telecommunications Act of 1996, as amended, 47 U.S.C. §§ 151, 152, 154(i)-(j), 201, 202, 222, 303(b), 303(r), 316, 338(i), 551, 605, 1302, this Report and Order IS ADOPTED.

400. IT IS FURTHER ORDERED that part 64 of the Commission's rules IS AMENDED as set forth in Appendix A.

401. IT IS FURTHER ORDERED that the data security requirements set forth in new 47 CFR § 64.2005 SHALL BE effective 90 days after publication in the Federal Register.

402. IT IS FURTHER ORDERED that, except as set forth in the prior paragraph, this Report and Order SHALL BE effective 30 days after publication of a summary in the Federal Register, except that the amendments to 47 CFR §§ 64.2003, 64.2004, 64.2006, and 64.2011(b), which contain new or modified information collection requirements that require approval by the Office of Management and Budget under the Paperwork Reduction Act, WILL BECOME EFFECTIVE after the Commission publishes a notice in the Federal Register announcing such approval and the relevant effective date. It is our intention in adopting the foregoing Report and Order that, if any provision of the Report and Order or the rules, or the application thereof to any person or circumstance, is held to be unlawful, the remaining portions of such Report and Order and the rules not deemed unlawful, and the application of such Report and Order and the rules to other person or circumstances, shall remain in effect to the fullest extent permitted by law.

403. IT IS FURTHER ORDERED that the Commission's Consumer & Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this Report and Order to Congress and the Government Accountability Office pursuant to the Congressional Review Act, see 5 U.S.C. § 801(a)(1)(A).

404. IT IS FURTHER ORDERED that the Commission's Consumer & Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this Report and Order, including the Final Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

## APPENDIX A

## Final Rules

The Federal Communications Commission proposes to amend 47 CFR part 64 to read as follows:

PART 64 – MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

1. The authority citation for Part 64 is revised to read as follows:

AUTHORITY: 47 U.S.C. 154, 254(k), 403, Pub. L. 104–104, 110 Stat. 56. Interpret or apply 47 U.S.C. 201, 202, 218, 222, 225, 226, 227, 228, 254(k), 301, 303, 332, 338, 551, 616, 620, 705, 1302, and the Middle Class Tax Relief and Job Creation Act of 2012, Pub. L. 112-96, unless otherwise noted.

2. Revise Subpart U to read as follows:

Subpart U – Protecting Customer Information

**§ 64.2001 Basis and Purpose**.

(a) *Basis*. The rules in this subpart are issued pursuant to the Communications Act of 1934, as amended.

(b) *Purpose*. The purpose of the rules in this subpart is to implement section 222 of the Communications Act of 1934, as amended, 47 U.S.C. 222.

**§ 64.2002 Definitions.**

(a) Broadband Internet access service (BIAS). The term "broadband Internet access service" or "BIAS" has the same meaning given to such term in section 8.2(a) of this chapter.

(b) Broadband Internet Access service provider. The term "broadband Internet access service provider" or "BIAS provider" means a person engaged in the provision of BIAS.

(c) Breach of security. The terms "breach of security," "breach," or "data breach," mean any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information.

(d) Call detail information. Any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

(e) Customer. A customer of a telecommunications carrier is (1) a current or former subscriber to a telecommunications service; or (2) an applicant for a telecommunications service.

(f) Customer proprietary information. The term "customer proprietary information" or "customer PI" means any of the following a carrier acquires in connection with its provision of telecommunications service:

(1) Individually identifiable customer proprietary network information (CPNI);

(2) Personally identifiable information (PII); and

(3) Content of communications.

(g) Customer proprietary network information (CPNI). The term "customer proprietary network information" or "CPNI" has the same meaning given to such term in section 222(h)(1) of the Communications Act of 1934, as amended, 47 U.S.C. 222(h)(1).

(h) Interconnected Voice over Internet Protocol (VoIP) Service. The term "interconnected VoIP service" has the same meaning given to such term in subsection (h) of this section.

(i) Material change. The term "material change" means any change that a customer, acting reasonably under the circumstances, would consider important to his or her decisions regarding his or her privacy, including any change to information required by the privacy notice described in section 64.2003.

(j) Opt-in approval. A method for obtaining customer consent to use, disclose, or permit access to the customer's proprietary information. This approval method requires that the carrier obtain from the customer affirmative, express consent allowing the requested usage, disclosure, or access to the customer proprietary information after the customer is provided appropriate notification of the carrier's request consistent with the requirements set forth in this subpart.

(k) Opt-out approval. A method for obtaining customer consent to use, disclose, or permit access to the customer's proprietary information. Under this approval method, a customer is deemed to have consented to the use, disclosure, or access to the customer's proprietary information if the customer has failed to object thereto after the customer is provided appropriate notification of the carrier's request for consent consistent with the requirements set forth in this subpart.

(l) Person. The term "person" has the same meaning given such term in section 3 of the Communications Act of 1934, as amended, 47 U.S.C. 153.

(m) Personally identifiable information (PII). The term "personally identifiable information" or "PII" means any information that is linked or reasonably linkable to an individual or device.

(n) Sensitive customer proprietary information. The terms "sensitive customer proprietary information" or "sensitive customer PI" include:

(1) financial information;
(2) health information;
(3) information pertaining to children;
(4) Social Security numbers;
(5) precise geo-location information;
(6) content of communications;
(7) call detail information; and
(8) web browsing history, application usage history, and the functional equivalents of either.

(o) Telecommunications carrier or carrier. The terms "telecommunications carrier" or "carrier" shall have the same meaning as set forth in section 3 of the Communications Act of 1934, as amended, 47 U.S.C. 153. For the purposes of this subpart, the term "telecommunications carrier" or "carrier" shall include a person engaged in the provision of interconnected VoIP service, as that term is defined in subsection (h) of this section.

(p) Telecommunications service. The term "telecommunications service" has the same meaning given to such term in section 3 of the Communications Act of 1934, as amended, 47 U.S.C. 153. For the purposes of this subpart, the term "telecommunications service" shall include interconnected VoIP service, as that term is defined in subsection (h) of this section.

**§ 64.2003 Notice Requirements for Telecommunications Carriers.**

(a) A telecommunications carrier must notify its customers of its privacy policies. Such notice must be clear and conspicuous, and in language that is comprehensible and not misleading.

(b) *Contents.* A telecommunications carrier's notice of its privacy policies under subsection (a) must:

(1) Specify and describe the types of customer proprietary information that the telecommunications carrier collects by virtue of its provision of telecommunications service and how it uses that information;

(2) Specify and describe under what circumstances the telecommunications carrier discloses or permits access to each type of customer proprietary information that it collects;

(3) Specify and describe the categories of entities to which the carrier discloses or permits access to customer proprietary information and the purposes for which the customer proprietary information will be used by each category of entities;

(4) Specify and describe customers' opt-in approval and/or opt-out approval rights with respect to their customer proprietary information, including:

(i) That a customer's denial or withdrawal of approval to use, disclose, or permit access to customer proprietary information will not affect the provision of any telecommunications services of which he or she is a customer; and

(ii) That any grant, denial, or withdrawal of approval for the use, disclosure, or permission of access to the customer proprietary information is valid until the customer affirmatively revokes such grant, denial, or withdrawal, and inform the customer of his or her right to deny or withdraw access to such proprietary information at any time.

(5) Provide access to a mechanism for customers to grant, deny, or withdraw approval for the telecommunications carrier to use, disclose, or provide access to customer proprietary information as required by section 64.2004 of this subpart;

(6) Be completely translated into a language other than English if the telecommunications carrier transacts business with the customer in that language.

(c) *Timing.* Notice required under subsection (a) must:

(1) Be made available to prospective customers at the point of sale, prior to the purchase of service, whether such point of sale is in person, online, over the telephone, or via another means; and

(2) Be made persistently available through: a clear and conspicuous link on the telecommunications carrier's homepage; the carrier's application (app), if it provides one for account management purposes; and any functional equivalent to the carrier's homepage or app. If a carrier does not have a website, it must provide notice to customers in paper form or another format agreed upon by the customer.

(d) *Material changes to a telecommunications carrier's privacy policies.* A telecommunications carrier must provide existing customers with advance notice of one or more material changes to the carrier's privacy policies. Such notice must be clear and conspicuous, and in language that is comprehensible and not misleading, and must:

(1) Be provided through email or another means of active communication agreed upon by the customer;

(2) Specify and describe:

(i) The changes made to the telecommunications carrier's privacy policies, including any changes to what customer proprietary information the carrier collects, and how it uses, discloses, or permits access to such information, the categories of entities to which it discloses or permits access to customer proprietary information, and which, if any, changes are retroactive; and

(ii) Customers' opt-in approval and/or opt-out approval rights with respect to their customer proprietary information, including the material specified in subsection (b)(4) of this section;

(3) Provide access to a mechanism for customers to grant, deny, or withdraw approval for the telecommunications carrier to use, disclose, or permit access to customer proprietary information as required by section 64.2004 of this subpart; and

(4) Be completely translated into a language other than English if the telecommunications carrier transacts business with the customer in that language.

**§ 64.2004 Customer Approval.**

Except as described in subsection (a), a telecommunications carrier may not use, disclose, or permit access to customer proprietary information except with the opt-out or opt-in approval of a customer as described in this section.

(a) *Limitations and Exceptions.* A telecommunications carrier may use, disclose, or permit access to customer proprietary information without customer approval for the following purposes:

(1) In its provision of the telecommunications service from which such information is derived, or in its provision of services necessary to, or used in, the provision of such service.

(2) To initiate, render, bill, and collect for telecommunications service.

(3) To protect the rights or property of the telecommunications carrier, or to protect users of the telecommunications service and other providers from fraudulent, abusive, or unlawful use of the service.

(4) To provide any inbound marketing, referral, or administrative services to the customer for the duration of a real-time interaction, if such interaction was initiated by the customer.

(5) To provide location information and/or non-sensitive customer proprietary information to:

(i) A public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's request for emergency services;

(ii) Inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or

(iii) Providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.

(6) As otherwise required or authorized by law.

(b) *Opt-Out Approval Required.* Except as otherwise provided in this section, a telecommunications carrier must obtain opt-out approval from a customer to use, disclose, or permit access to any of the customer's non-sensitive customer proprietary information. If it so chooses, a telecommunications carrier may instead obtain opt-in approval from a customer to use, disclose, or permit access to any of the customer's non-sensitive customer proprietary information.

(c) *Opt-In Approval Required.* Except as otherwise provided in this section, a telecommunications carrier must obtain opt-in approval from a customer to:

(1) use, disclose, or permit access to any of the customer's sensitive customer proprietary information; or

(2) make any material retroactive change—i.e., a material change that would result in a use, disclosure, or permission of access to any of the customer's proprietary information previously collected by the carrier for which the customer did not previously grant approval, either through opt-in or opt-out consent, as required by subsections (b) and (c) of this section.

(d) *Notice and Solicitation Required.*

(1) Except as described in subsection (a) of this section, a telecommunications carrier must at a minimum solicit customer approval pursuant to subsection (b) and/or (c), as applicable, at the point of sale and when making one or more material changes to privacy policies. Such solicitation may be part of, or the same communication as, a notice required by section 64.2003 of these rules.

(2) A telecommunications carrier's solicitation of customer approval must be clear and conspicuous, and in language that is comprehensible and not misleading. Such solicitation must disclose:

(i) The types of customer proprietary information for which the carrier is seeking customer approval to use, disclose, or permit access to;

(ii) The purposes for which such customer proprietary information will be used;

(iii) The categories of entities to which the carrier intends to disclose or permit access to such customer proprietary information; and

(iv) A means to easily access the notice required by section 64.2003(a) of this subpart and a means to access the mechanism required by subsection (e).

(3) A telecommunications carrier's solicitation of customer approval must be completely translated into a language other than English if the telecommunications carrier transacts business with the customer in that language.

(e) *Mechanism for Exercising Customer Approval.* A telecommunications carrier must make available a simple, easy-to-use mechanism for customers to grant, deny, or withdraw opt-in approval and/or opt-out approval at any time. Such mechanism must be clear and conspicuous, in language that is comprehensible and not misleading, and made available at no additional cost to the customer. Such mechanism must be persistently available on or through the carrier's website; the carrier's application (app), if it provides one for account management purposes; and any functional equivalent to the carrier's homepage or app. If a carrier does not have a website, it must provide a persistently available mechanism by another means such as a toll-free telephone number. The customer's grant, denial, or withdrawal of approval must be given effect promptly and remain in effect until the customer revokes or limits such grant, denial, or withdrawal of approval.

**§ 64.2005 Data Security.**

(a) A telecommunications carrier must take reasonable measures to protect customer PI from unauthorized use, disclosure, or access.

(b) The security measures taken by a telecommunications carrier to implement the requirement set forth in this section must appropriately take into account each of the following factors:

(1) The nature and scope of the telecommunications carrier's activities;

(2) The sensitivity of the data it collects;

(3) The size of the telecommunications carrier; and

(4) Technical feasibility.

(c) A telecommunications carrier may employ any lawful security measures that allow it to implement the requirement set forth in this section.

**§ 64.2006 Data Breach Notification.**

(a) *Customer Notification.* A telecommunications carrier shall notify affected customers of any breach without unreasonable delay and in any event no later than 30 calendar days after the carrier reasonably determines that a breach has occurred, subject to law enforcement needs, unless the telecommunications carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach.

(1) A telecommunications carrier required to provide notification to a customer under this subsection must provide such notice by one or more of the following methods:

(i) Written notification sent to either the customer's email address or the postal address of record of the customer, or, for former customers, to the last postal address ascertainable after reasonable investigation using commonly available sources; or

(ii) Other electronic means of active communications agreed upon by the customer for contacting that customer for data breach notification purposes.

(2) The customer notification required to be provided under this subsection must include:

(i) The date, estimated date, or estimated date range of the breach of security;

(ii) A description of the customer PI that was breached or reasonably believed to have been breached;

(iii) Information the customer can use to contact the telecommunications carrier to inquire about the breach of security and the customer PI that the telecommunications carrier maintains about that customer;

(iv) Information about how to contact the Federal Communications Commission and any state regulatory agencies relevant to the customer and the service; and

(v) If the breach creates a risk of financial harm, information about the national credit-reporting agencies and the steps customers can take to guard against identity theft, including any credit monitoring, credit reporting, credit freezes, or other consumer protections the telecommunications carrier is offering customers affected by the breach of security.

(b) *Commission Notification.* A telecommunications carrier must notify the Commission of any breach affecting 5,000 or more customers no later than seven business days after the carrier reasonably determines that a breach has occurred and at least three business days before notification to the affected customers, unless the telecommunications carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. A telecommunications carrier must notify the Commission of any breach affecting fewer than 5,000 customers without unreasonable delay and no later than thirty (30) calendar days after the carrier reasonably determines that a breach has occurred, unless the telecommunications carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. Such notification shall be made through a central reporting system made available by the Commission.

(c) *Federal Law Enforcement Notification.* A telecommunications carrier must notify the Federal Bureau of Investigation (FBI) and the U.S. Secret Service (Secret Service) of a breach that affects 5,000 or more customers no later than seven business days after the carrier reasonably determines that such a breach has occurred and at least three business days before notification to the affected customers, unless the telecommunications carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. Such notification shall be made through a central reporting system made available by the Commission.

(d) *Recordkeeping.* A telecommunications carrier shall maintain a record, electronically or in some

other manner, of any breaches and notifications made to customers, unless the telecommunications carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. The record must include the dates on which the carrier determines that a reportable breach has occurred and the dates of customer notification. The record must include a written copy of all customer notifications. Carriers shall retain the record for a minimum of two years from the date on which the carrier determines that a reportable breach has occurred.

**§ 64.2010 Business Customer Exemption for Provision of Telecommunications Services other than BIAS.**

Telecommunications carriers may bind themselves contractually to privacy and data security regimes other than those described in this subpart for the provision of telecommunications services other than BIAS to enterprise customers if the carrier's contract with that customer specifically addresses the issues of transparency, choice, data security, and data breach and provides a mechanism for the customer to communicate with the carriers about privacy and data security concerns.

**§ 64.2011 BIAS Offers Conditioned on Waiver of Privacy Rights.**

(a) A BIAS provider must not condition, or effectively condition, provision of BIAS on a customer's agreement to waive privacy rights guaranteed by law or regulation, including this subpart. A BIAS provider must not terminate service or otherwise refuse to provide BIAS as a direct or indirect consequence of a customer's refusal to waive any such privacy rights.

(b) A BIAS provider that offers a financial incentive, such as lower monthly rates, in exchange for a customer's approval to use, disclose, and/or permit access to the customer's proprietary information must do all of the following:

(1) Provide notice explaining the terms of any financial incentive program that is clear and conspicuous, and in language that is comprehensible and not misleading. Such notice must be provided both at the time the program is offered and at the time a customer elects to participate in the program. Such notice must:

(i) Explain that the program requires opt-in approval to use, disclose, and/or permit access to customer PI;

(ii) Include information about what customer PI the provider will collect, how it will be used, and with what categories of entities it will be shared and for what purposes;

(iii) Be easily accessible and separate from any other privacy notifications, including but not limited to any privacy notifications required by this subpart;

(iv) Be completely translated into a language other than English if the BIAS provider transacts business with the customer in that language; and

(v) Provide at least as prominent information to customers about the equivalent service plan that does not necessitate the use, disclosure, or access to customer PI beyond that required or permitted by law or regulation, including under this subpart.

(2) Obtain customer opt-in approval in accordance with section 64.2004(c) of this subpart for participation in any financial incentive program.

(3) If customer opt-in approval is given, the BIAS provider must make available a simple, easy-to-use mechanism for customers to withdraw approval for participation in such financial incentive program at any time. Such mechanism must be clear and conspicuous, in language that is comprehensible and not misleading, and must be persistently available on or through the carrier's website; the carrier's application (app), if it provides one for account management purposes; and any functional equivalent to the carrier's homepage or app. If a carrier does not have a website, it must provide a persistently available mechanism by another means such as a toll-free telephone number.

**§ 64.2012 Effect on State Law.**

The rules set forth in this subpart shall preempt any State law only to the extent that such law is inconsistent with the rules set forth herein and only if the Commission has affirmatively determined that the State law is preempted on a case-by-case basis. The Commission shall not presume that more restrictive State laws are inconsistent with the rules set forth herein.

## APPENDIX B

### Final Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *Broadband Privacy NPRM* for this proceeding.[2] The Commission sought written public comment on the proposals in the *Broadband Privacy NPRM*, including comment on the IRFA. The Commission received comments on the IRFA, which are discussed below.[3] This present Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA.[4]

#### A. Need for, and Objectives of, the Rules

2. In the Order, we adopt privacy requirements for providers of broadband Internet access service (BIAS) and other telecommunications services.[5] In doing so, we build upon the Commission's long history of protecting customer privacy in the telecommunications sector. Section 222 of the Communications Act provides statutory protections to the privacy of the data that all telecommunications carriers collect from their customers. Section 222(a) imposes a duty on all telecommunications carriers to protect the confidentiality of their customers' "proprietary information," or PI. Section 222(c) imposes restrictions on telecommunications carriers' use and sharing of customer proprietary network information (CPNI) without customer approval, subject to certain exceptions, including as necessary to provide the telecommunications service (or services necessary to or used in providing that telecommunications service), and as required by law.[6]

3. Over the last two decades, the Commission has promulgated, revised, and enforced privacy rules for telecommunications carriers that are focused on implementing the CPNI requirements of Section 222. As practices have changed, the Commission has refined its Section 222 rules. The current Section 222 rules focus on transparency, choice, data security, and data breach notification.

4. Prior to 2015, BIAS was classified as an information service, which excluded such services from the ambit of Title II of the Act, including Section 222, and the Commission's CPNI rules. Instead, broadband providers were subject to the FTC's unfair and deceptive acts and practices authority. In the *2015 Open Internet Order*, we reclassified BIAS as a telecommunications service subject to Title II of the Act, an action upheld by the D.C. Circuit in *United States Telecom Ass'n v. FCC*. While we granted BIAS forbearance from many Title II provisions, we concluded that application and enforcement of the privacy protections in Section 222 to BIAS is in the public interest and necessary for the protection of consumers. However, we questioned "whether the Commission's current rules implementing section 222 necessarily would be well suited to broadband Internet access service," and forbore from the application of these rules to broadband service, "pending the adoption of rules to govern broadband Internet access service in a separate rulemaking proceeding."[7]

5. In March 2016, we adopted the *Broadband Privacy NPRM*, which proposed a framework

[1] *See* 5 U.S.C. § 603. The RFA, *see* 5 U.S.C. §§ 601-612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[2] *Broadband Privacy NPRM*, 31 FCC Rcd at 2611-32, Appx. B.

[3] *See* Alaska Telephone Association Reply at 1-2; CCA Reply at 6; NTCA Reply at 15-16; RWA Comments at 2-13; WISPA Comments at 4-5, 31-33; WISPA Reply at 1-3, 31-43; U.S. Small Business Administration Reply.

[4] *See* 5 U.S.C. § 604.

[5] *See supra* note 68.

[6] *See supra* Part III.A.

[7] *2015 Open Internet Order*, 30 FCC Rcd at 5820-22, paras. 462-64; *see also supra* Part III.A.

for applying the longstanding privacy requirements of the Act to BIAS.[8] In the *NPRM*, we proposed rules protecting customer privacy using the three foundations of privacy—transparency, choice, and security—and also sought comment on, among other things, whether we should update rules that govern the application of Section 222 to traditional telephone service and interconnected VoIP service in order to harmonize them with the results of this proceeding.[9]

6. Based on the record gathered in this proceeding, today we adopt a harmonized set of rules applicable to BIAS providers and other telecommunications carriers. The privacy framework we adopt focuses on transparency, choice, and data security, and provides heighted protection for sensitive customer information, consistent with customer expectations. Our need to extend such privacy requirements to BIAS providers is based, in part, on their particular role as network providers and the context of the consumer/BIAS provider relationship. Based on our review of the record, we reaffirm our earlier finding that a broadband provider "sits at a privileged place in the network, the bottleneck between the customer and the rest of the Internet"[10]—a position that we have referred to as a gatekeeper.[11] As such, BIAS providers can collect "an unprecedented breadth" of electronic personal information.[12]

7. In adopting these rules we honor customers' privacy rights and implement the statutory requirement that carriers protect the confidentiality of customer proprietary information. These rules do not prohibit carriers from using or sharing customer information, but rather are designed to protect consumer choice while giving carriers the flexibility they need to continue to innovate. 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.

### B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA

8. In response to the *Broadband Privacy NPRM*, five entities filed comments, reply comments, and/or *ex parte* letters that specifically addressed the IRFA to some degree: Alaska Telephone Association, Competitive Carriers Association, NTCA, Rural Wireless Association, and Wireless Internet

[8] *See generally Broadband Privacy NPRM*, 31 FCC Rcd at 2500.

[9] *See, e.g.*, *Broadband Privacy NPRM*, 31 FCC Rcd at 2510, para. 24.

[10] *See* Letter from Paul Ohm, Professor, Georgetown University Law Center, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 16-106 Attach., Testimony Before the Subcommittee on Communications and Technology, Committee on Energy and Commerce, U.S. House of Representatives at 3 (filed June 19, 2016) (Paul Ohm Testimony).

[11] *See 2015 Open Internet Order*, 30 FCC Rcd at 5629, para. 80 (noting that "once a consumer chooses a broadband provider, that provider has a monopoly on access to the subscriber").

[12] Letter from Kathleen McGee, Bureau Chief, Bureau of Internet and Technology, New York State Attorney General, to Tom Wheeler, Chairman, FCC, GC Docket No. 16-106 at 2 (filed June 30, 2016) (NY Attorney General June 30, 2016 *Ex Parte* Letter) (also claiming that BIAS providers can collect "not only a consumer's name, address and financial information but also every website he or she visited, the links clicked on those websites, geo-location information, and the content of electronic communications"); *see also, e.g.*, Letter from Christopher N. Olsen, Counsel to Ghostery, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 16-106, Attach. at 3-5 (Ghostery Apr. 29, 2016 *Ex Parte* Letter); Consumer Action Comments at 1; Consumer Watchdog Comments at 4 ("The ISP is in a unique position to amass deeply revealing personal profiles, share the data with third parties or use it for its own purposes."); Public Knowledge et al. Comments, Attach. Public Knowledge White Paper, Protecting Privacy, Promoting Competition: A framework for Updating the Federal Communications Commission Privacy Rules for the Digital World at 51-52, 55-56 (Public Knowledge White Paper); AAJ Comments at 8 (explaining that "BIAS providers are now privy to an extensive amount of personal information about their customers"); EFF Comments at 1.

Service Providers Association (WISPA).[13] Some of these, as well as other entities, filed comments, reply comments, and/or *ex parte* letters that more generally considered the small business impact of our proposals.[14]

9. Some commenters recommend that the Commission adopt specific exemptions or provisions to alleviate burdens on small carriers. In particular, commenters recommend that the Commission (1) exempt small carriers from some or all of the rules based on their size and/or practices;[15] (2) give small carriers additional time to comply with the rules;[16] (3) harmonize notice and choice requirements with the preexisting voice CPNI rules;[17] (4) exempt small carriers from any privacy dashboard requirements and otherwise give them flexibility in the structure of their privacy notices;[18] (5) grandfather existing customer approvals for use and disclosure of customer information;[19] (6) exempt small carriers from any opt-in approval requirements;[20] (6) not impose specific data security requirements on small providers;[21] (7) not impose specific data breach reporting deadlines on small providers, and instead allow them to report breaches as soon as practicable;[22] and (8) not hold small carriers liable for misuse of customer PI by third parties with whom they share the information.[23] We considered these proposals and concerns when composing the Order and the accompanying rules.[24]

### C. Response to Comments by the Chief Counsel for Advocacy of the Small Business Administration

10. Pursuant to the Small Business Jobs Act of 2010, which amended the RFA, the Commission is required to respond to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration (SBA), and to provide a detailed statement of any change made to the proposed rules as a result of those comments.[25]

11. The SBA filed comments in response to the IRFA encouraging the Commission to examine measures, exemptions, and alternatives that would ease compliance by small

[13] *See* Alaska Telephone Association Reply at 1-2; CCA Reply at 6; NTCA Reply at 15-16; RWA Comments at 2-13; WISPA Comments at 4-5, 31-33; WISPA Reply at 1-3, 31-43.

[14] *See, e.g.*, ACA Comments at 38-39, 46-51, 57-58; ACA Reply at 4, 14-20; CCA Reply at 12-13, 25-26, 35, 40-41; Education & Research Consortium et al. Comments at 5, 8-10; NTCA Comments at 18, 41-43, 49-51, 55; Rural Wireless Association Comments at 2-14; USTelecom Comments at 19; WISPA Comments at 4-5, 28-29, 31-33; WISPA Reply at 31-43; WTA Comments at 2-3, 10-17; WTA Reply at 5-10, 13; WTA & Nex-Tech Apr. 25, 2016 *Ex Parte* at 1.

[15] *See* ACA Reply at 4; Alaska Telephone Association Reply at 1-2; WISPA Reply at 41; WTA Comments at 2-3; WTA Reply at 5-6.

[16] *See* ACA Comments at 46-49; CCA Reply at 40-41; WISPA Comments at 28-29.

[17] *See* ACA Comments at 57-58; RWA Comments at 6-7; WTA Comments at 12.

[18] *See* ACA Comments at 38-39, 46; ACA Reply at 4; CCA Reply at 25-26, 35; NTCA Comments at 41-43; WTA Comments at 14-17; WTA Reply at 8-10. *But see* ACA Reply at 14-15 (asking for standardized notices with a safe harbor); NTCA Comments at 41-42 (same).

[19] *See* USTelecom Comments at 19; NTCA Comments at 55; WISPA Comments at 31; WTA Comments at 10, 16.

[20] *See* NTCA Comments at 49-51.

[21] *See* CCA Reply at 12-13; WISPA Comments at 31-33; WISPA Reply at 31-43; WTA Reply at 13.

[22] *See* ACA Reply at 4; WISPA Comments at 31-33; WISPA Reply at 31-43.

[23] Education & Research Consortium et al. Comments at 8-10.

[24] *See infra* Appx. B, Part VI.F.

[25] 5 U.S.C. § 604(a)(3).

telecommunications carriers with our rules.[26] SBA observed that compliance costs to small providers may include "consulting fees, attorney's fees, hiring or training in-house privacy personnel, customer notification costs, and opportunity costs."[27] In particular, SBA recommends giving small providers more time to comply with the rules and it supports granting small providers an exemption from the rules "wherever practicable."[28]

12. As explained in detail below, we have taken numerous measures in this Order to alleviate burdens for small providers, consistent with the comments of the SBA. In particular, we have adopted SBA's proposal that we give small providers additional time to comply.[29] Also, while we do not exempt small providers from any of our rules, we have taken alternative measures to address several of the concerns with specific rule proposals that the SBA identifies. For instance, the data security rule we adopt focuses on the "reasonableness" of a carrier's security practices and does not prescribe any minimum required practices a provider must undertake to achieve compliance.[30] The rule also specifically recognizes that the size of the provider is one of the factors to be considered in determining whether a provider has engaged in reasonable data security practices. By formulating the rule in this way, we have addressed small provider concerns regarding the costs of implementing prescriptive requirements.[31] We also note that among other accommodations directly responsive to small provider concerns, we decline to require a consumer-facing dashboard.

### D. Description and Estimate of the Number of Small Entities to Which the Rules Will Apply

13. The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the rules.[32] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[33] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[34] A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.[35]

14. For the purposes of these rules, we define small providers as providers with 100,000 or fewer broadband connections as reported on their most recent Form 477, aggregated over all the providers' affiliates. We decline to count based on the number of customers from whom carriers collect

[26] Letter from Darryl L. DePriest, Chief Counsel for Advocacy, and Jamie Belcore Saloom, Assistant Chief Counsel, Office of Advocacy, U.S. Small Business Administration, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 (filed June 27, 2016) (SBA Comments).

[27] U.S. Small Business Administration Reply at 3.

[28] U.S. Small Business Administration Reply at 4.

[29] *See supra* Part III.I.4.

[30] *See supra* Part III.E.

[31] *See supra* Part III.E.1.

[32] 5 U.S.C. § 604.

[33] 5 U.S.C. § 601(6).

[34] 5 U.S.C. § 601(3) (incorporating by reference the definition of "small-business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

[35] 15 U.S.C. § 632.

data, as we recognize that some data collection is necessary to the provisions of service. Cabining the scope of small providers to those serving 100,000 or fewer subscribers is consistent with the *2015 Open Internet Order*.[36]

15. The rules apply to all telecommunications carriers, including providers of BIAS. Below, we describe the types of small entities that might provide these services.

### 1. Total Small Entities

16. Our rules may, over time, affect small entities that are not easily categorized at present. We therefore describe here, at the outset, three comprehensive, statutory small entity size standards.[37] First, as of 2013, the SBA estimates there are an estimated 28.8 million small businesses nationwide—comprising some 99.9% of all businesses.[38] In addition, a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field."[39] Nationwide, as of 2007, there were approximately 1,621,315 small organizations.[40] Finally, the term "small governmental jurisdiction" is defined generally as "governments of cities, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."[41] Census Bureau data for 2011 indicate that there were 90,056 local governmental jurisdictions in the United States.[42] We estimate that, of this total, as many as 89,327 entities may qualify as "small governmental jurisdictions."[43] Thus, we estimate that most governmental jurisdictions are small.

### 2. Broadband Internet Access Service Providers

17. The Economic Census places BIAS providers, whose services might include Voice over Internet Protocol (VoIP), in either of two categories, depending on whether the service is provided over the provider's own telecommunications facilities (e.g., cable and DSL ISPs), or over client-supplied telecommunications connections (e.g., dial-up ISPs). The former are within the category of Wired Telecommunications Carriers,[44] which has an SBA small business size standard of 1,500 or fewer

[36] *See supra* Part III.I.4.

[37] *See* 5 U.S.C. §§ 601(3)-(6).

[38] *See* Small Bus. Admin., Office of Advocacy, *Frequently Asked Questions about Small Business* 1 (2016), https://www.sba.gov/sites/default/files/advocacy/SB-FAQ-2016_WEB.pdf.

[39] 5 U.S.C. § 601(4).

[40] Indep. Sector, The New Nonprofit Almanac and Desk Reference (2010).

[41] 5 U.S.C. § 601(5).

[42] U.S. Census Bureau, Statistical Abstract of the United States: 2012, Section 8, page 267, tbl. 429, https://www.census.gov/compendia/statab/2012/tables/12s0429.pdf/ (data cited therein are from 2007).

[43] The 2007 U.S. Census data for small governmental organizations are not presented based on the size of the population in each such organization. There were 89,476 local governmental organizations in 2007. If we assume that county, municipal, township, and school district organizations are more likely than larger governmental organizations to have populations of 50,000 or less, the total of these organizations is 52,095. As a basis of estimating how many of these 89,476 local government organizations were small, in 2011, we note that there were a total of 715 cities and towns (incorporated places and minor civil divisions) with populations over 50,000. U.S. Census Bureau, City and Town Totals Vintage: 2011, http://www.census.gov/popest/data/cities/totals/2011/index.html. If we subtract the 715 cities and towns that meet or exceed the 50,000 population threshold, we conclude that approximately 88,761 are small. U.S. Census Bureau, Statistical Abstract of the United States: 2012, Section 8, page 267, tbl. 429, https://www.census.gov/compendia/statab/2012/tables/12s0429.pdf/ (data cited therein are from 2007).

[44] U.S. Census Bureau, 2012 NAICS Definitions, "517110 Wired Telecommunications Carriers," http://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517110&search=2012%20NAICS%20Search.

employees.[45] These are also labeled "broadband." The latter are within the category of All Other Telecommunications,[46] which has a size standard of annual receipts of $32.5 million or less.[47] These are labeled non-broadband. According to Census Bureau data for 2012, there were 3,117 firms in the first category, total, that operated for the entire year.[48] Of this total, 3,083 firms had employment of 999 or fewer employees.[49] For the second category, the data show that 1,442 firms operated for the entire year.[50] Of those, 1,400 had annual receipts below $25 million per year. Consequently, we estimate that the majority of broadband Internet access service provider firms are small entities.

18. The broadband Internet access service provider industry has changed since this definition was introduced in 2007. The data cited above may therefore include entities that no longer provide broadband Internet access service, and may exclude entities that now provide such service. To ensure that this FRFA describes the universe of small entities that our action affects, we discuss in turn several different types of entities that might be providing broadband Internet access service, which also overlap with entities providing other telecommunications services. We note that, although we have no specific information on the number of small entities that provide broadband Internet access service over unlicensed spectrum, we include these entities in our Final Regulatory Flexibility Analysis.

### 3. Wireline Providers

19. *Wired Telecommunications Carriers*. The U.S. Census Bureau defines this industry as "establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry."[51] The SBA has developed a small business size standard for Wired Telecommunications Carriers, which consists of all such companies having 1,500 or fewer employees.[52] Census data for 2012 shows that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000 employees.[53] Thus, under this size standard, the majority of firms in this industry can be considered small.

20. *Local Exchange Carriers (LECs)*. Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. The closest applicable NAICS Code category is Wired Telecommunications Carriers as defined in this FRFA. Under

[45] 13 CFR § 121.201, NAICS code 517110.

[46] U.S. Census Bureau, 2012 NAICS Definitions, "517919 All Other Telecommunications,", http://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517919&search=2012%20NAICS%20Search.

[47] 13 CFR § 121.201, NAICS code 517919.

[48] U.S. Census Bureau, 2007 Economic Census, Subject Series: Information, Table 5, "Establishment and Firm Size: Employment Size of Firms for the United States: 2007 NAICS Code 517110" (2010).

[49] *See id.*

[50] U.S. Census Bureau, 2007 Economic Census, Subject Series: Information, "Establishment and Firm Size," NAICS code 5179191 (2010) (receipts size).

[51] http://www.census.gov/cgi-bin/sssd/naics/naicsrch.

[52] *See* 13 CFR § 120.201, NAICS Code 517110.

[53] http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

the applicable SBA size standard, such a business is small if it has 1,500 or fewer employees.[54] According to Commission data, census data for 2012 shows that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000 employees.[55] The Commission therefore estimates that most providers of local exchange carrier service are small entities that may be affected by the rules adopted.

21. *Incumbent Local Exchange Carriers* (*Incumbent LECs*). Neither the Commission nor the SBA has developed a small business size standard specifically for incumbent local exchange services. The closest applicable NAICS Code category is Wired Telecommunications Carriers as defined in this FRFA. Under that size standard, such a business is small if it has 1,500 or fewer employees.[56] According to Commission data, 3,117 firms operated in that year. Of this total, 3,083 operated with fewer than 1,000 employees.[57] Consequently, the Commission estimates that most providers of incumbent local exchange service are small businesses that may be affected by the rules and policies adopted. Three hundred and seven (307) Incumbent Local Exchange Carriers reported that they were incumbent local exchange service providers.[58] Of this total, an estimated 1,006 have 1,500 or fewer employees.[59]

22. *Competitive Local Exchange Carriers (Competitive LECs), Competitive Access Providers (CAPs), Shared-Tenant Service Providers, and Other Local Service Providers*. Neither the Commission nor the SBA has developed a small business size standard specifically for these service providers. The appropriate NAICS Code category is Wired Telecommunications Carriers, as defined in this FRFA. Under that size standard, such a business is small if it has 1,500 or fewer employees.[60] U.S. Census data for 2012 indicate that 3,117 firms operated during that year. Of that number, 3,083 operated with fewer than 1,000 employees.[61] Based on this data, the Commission concludes that the majority of Competitive LECS, CAPs, Shared-Tenant Service Providers, and Other Local Service Providers, are small entities. According to Commission data, 1,442 carriers reported that they were engaged in the provision of either competitive local exchange services or competitive access provider services.[62] Of these 1,442 carriers, an estimated 1,256 have 1,500 or fewer employees.[63] In addition, 17 carriers have reported that they are Shared-Tenant Service Providers, and all 17 are estimated to have 1,500 or fewer employees.[64] Also, 72 carriers have reported that they are Other Local Service Providers.[65] Of this total, 70 have 1,500 or fewer employees.[66] Consequently, based on internally researched FCC data, the Commission estimates that

[54] 13 CFR § 121.201, NAICS code 517110.

[55] http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

[56] 13 CFR § 121.201, NAICS code 517110.

[57] http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

[58] *See Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*).

[59] *Id.*

[60] 13 CFR § 121.201, NAICS code 517110.

[61] http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

[62] *See Trends in Telephone Service,* at tbl. 5.3.

[63] *Id.*

[64] *Id.*

[65] *Id.*

[66] *Id.*

most providers of competitive local exchange service, competitive access providers, Shared-Tenant Service Providers, and Other Local Service Providers are small entities.

23. We have included small incumbent LECs in this present RFA analysis. As noted above, a "small business" under the RFA is one that, *inter alia*, meets the pertinent small business size standard (e.g., a telephone communications business having 1,500 or fewer employees), and "is not dominant in its field of operation."[67] The SBA's Office of Advocacy contends that, for RFA purposes, small incumbent LECs are not dominant in their field of operation because any such dominance is not "national" in scope.[68] We have therefore included small incumbent LECs in this RFA analysis, although we emphasize that this RFA action has no effect on Commission analyses and determinations in other, non-RFA contexts.

24. *Interexchange Carriers.* Neither the Commission nor the SBA has developed a definition for Interexchange Carriers. The closest NAICS Code category is Wired Telecommunications Carriers as defined in this FRFA. The applicable size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees.[69] U.S. Census data for 2012 indicates that 3,117 firms operated during that year. Of that number, 3,083 operated with fewer than 1,000 employees.[70] According to internally developed Commission data, 359 companies reported that their primary telecommunications service activity was the provision of interexchange services.[71] Of this total, an estimated 317 have 1,500 or fewer employees.[72] Consequently, the Commission estimates that the majority of interexchange service providers are small entities that may be affected by the rules adopted.

25. *Operator Service Providers* (*OSPs*). Neither the Commission nor the SBA has developed a small business size standard specifically for operator service providers. The appropriate size standard under SBA rules is for the category Wired Telecommunications Carriers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[73] According to Commission data, 33 carriers have reported that they are engaged in the provision of operator services. Of these, an estimated 31 have 1,500 or fewer employees and two have more than 1,500 employees.[74] Consequently, the Commission estimates that the majority of OSPs are small entities that may be affected by these rules.

26. *Prepaid Calling Card Providers.* Neither the Commission nor the SBA has developed a small business definition specifically for prepaid calling card providers. The most appropriate NAICS code-based category for defining prepaid calling card providers is Telecommunications Resellers. This industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual

[67] 5 U.S.C. § 601(3).

[68] Letter from Jere W. Glover, Chief Counsel for Advocacy, SBA, to William E. Kennard, Chairman, Federal Communications Commission (filed May 27, 1999). The Small Business Act contains a definition of "small business concern," which the RFA incorporates into its own definition of "small business." 15 U.S.C. § 632(a); 5 U.S.C. § 601(3). SBA regulations interpret "small business concern" to include the concept of dominance on a national basis. 13 CFR § 121.102(b).

[69] 13 CFR § 121.201, NAICS code 517110.

[70] http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

[71] *See Trends in Telephone Service,* at tbl. 5.3.

[72] *Id.*

[73] 13 CFR § 121.201, NAICS code 517110.

[74] *Trends in Telephone Service*, tbl. 5.3.

networks operators (MVNOs) are included in this industry.[75] Under the applicable SBA size standard, such a business is small if it has 1,500 or fewer employees.[76] U.S. Census data for 2012 show that 1,341 firms provided resale services during that year. Of that number, 1,341 operated with fewer than 1,000 employees.[77] Thus, under this category and the associated small business size standard, the majority of these prepaid calling card providers can be considered small entities. According to Commission data, 193 carriers have reported that they are engaged in the provision of prepaid calling cards.[78] All 193 carriers have 1,500 or fewer employees.[79] Consequently, the Commission estimates that the majority of prepaid calling card providers are small entities that may be affected by the rules adopted.

27. *Local Resellers.* Neither the Commission nor the SBA has developed a small business size standard specifically for Local Resellers. The SBA has developed a small business size standard for the category of Telecommunications Resellers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[80] Census data for 2012 show that 1,341 firms provided resale services during that year. Of that number, 1,341 operated with fewer than 1,000 employees.[81] Under this category and the associated small business size standard, the majority of these local resellers can be considered small entities. According to Commission data, 213 carriers have reported that they are engaged in the provision of local resale services.[82] Of this total, an estimated 211 have 1,500 or fewer employees.[83] Consequently, the Commission estimates that the majority of local resellers are small entities that may be affected by the rules adopted.

28. *Toll Resellers.* The Commission has not developed a definition for Toll Resellers. The closest NAICS Code Category is Telecommunications Resellers, and the SBA has developed a small business size standard for the category of Telecommunications Resellers.[84] Under that size standard, such a business is small if it has 1,500 or fewer employees.[85] Census data for 2012 show that 1,341 firms provided resale services during that year. Of that number, 1,341 operated with fewer than 1,000 employees.[86] Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 881 carriers have reported that they are engaged in the provision of toll resale services.[87] Of this total, an estimated 857 have 1,500 or fewer employees.[88] Consequently, the Commission estimates that the majority of toll resellers are small entities.

---

[75] http://www.census.gov/cgi-bin/ssd/naics/naicsrch.

[76] 13 CFR § 121.201, NAICS code 517911.

[77] http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

[78] *See Trends in Telephone Service,* at tbl. 5.3.

[79] *Id.*

[80] 13 CFR § 121.201, NAICS code 517911.

[81] http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

[82] *See Trends in Telephone Service,* at tbl. 5.3.

[83] *Id.*

[84] 13 CFR § 121.201, NAICS code 517911.

[85] http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

[86] *Id*.

[87] *Trends in Telephone Service*, at tbl. 5.3.

[88] *Id.*

29. *Other Toll Carriers*. Neither the Commission nor the SBA has developed a definition for small businesses specifically applicable to Other Toll Carriers. This category includes toll carriers that do not fall within the categories of interexchange carriers, operator service providers, prepaid calling card providers, satellite service carriers, or toll resellers. The closest applicable NAICS Code category is for Wired Telecommunications Carriers as defined in paragraph 6 of this FRFA. Under the applicable SBA size standard, such a business is small if it has 1,500 or fewer employees.[89] Census data for 2012 shows that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000 employees.[90] Thus, under this category and the associated small business size standard, the majority of Other Toll Carriers can be considered small. According to internally developed Commission data, 284 companies reported that their primary telecommunications service activity was the provision of other toll carriage.[91] Of these, an estimated 279 have 1,500 or fewer employees.[92] Consequently, the Commission estimates that most Other Toll Carriers are small entities.

#### 4. Wireless Providers – Fixed and Mobile

30. The telecommunications services category covered by these rules may cover multiple wireless firms and categories of regulated wireless services. In addition, for those services subject to auctions, we note that, as a general matter, the number of winning bidders that claim to qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. Also, the Commission does not generally track subsequent business size unless, in the context of assignments and transfers or reportable eligibility events, unjust enrichment issues are implicated.

31. *Wireless Telecommunications Carriers (except Satellite*). This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless internet access, and wireless video services.[93] The appropriate size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees. For this industry, Census data for 2012 show that there were 967 firms that operated for the entire year. Of this total, 955 firms had fewer than 1,000 employees. Thus under this category and the associated size standard, the Commission estimates that the majority of wireless telecommunications carriers (except satellite) are small entities. Similarly, according to internally developed Commission data, 413 carriers reported that they were engaged in the provision of wireless telephony, including cellular service, Personal Communications Service (PCS), and Specialized Mobile Radio (SMR) services.[94] Of this total, an estimated 261 have 1,500 or fewer employees.[95] Thus, using available data, we estimate that the majority of wireless firms can be considered small.

32. *Wireless Communications Services*. This service can be used for fixed, mobile, radiolocation, and digital audio broadcasting satellite uses. The Commission defined "small business" for the wireless communications services (WCS) auction as an entity with average gross revenues of $40 million for each of the three preceding years, and a "very small business" as an entity with average gross

[89] 13 CFR § 121.201, NAICS code 517110.

[90] http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ5&prodType=table.

[91] *Trends in Telephone Service*, at tbl. 5.3.

[92] *Id.*

[93] NAICS Code 517210. *See* http://www.census.gov/cgi-bin/ssd/naics/naicsrch.

[94] *Trends in Telephone Service*, at tbl. 5.3.

[95] *Id.*

revenues of $15 million for each of the three preceding years.[96] The SBA has approved these definitions.[97]

33. *1670–1675 MHz Services*. This service can be used for fixed and mobile uses, except aeronautical mobile.[98] An auction for one license in the 1670–1675 MHz band was conducted in 2003. One license was awarded. The winning bidder was not a small entity.

34. *Wireless Telephony*. Wireless telephony includes cellular, personal communications services, and specialized mobile radio telephony carriers. As noted, the SBA has developed a small business size standard for Wireless Telecommunications Carriers (except Satellite).[99] Under the SBA small business size standard, a business is small if it has 1,500 or fewer employees.[100] According to Commission data, 413 carriers reported that they were engaged in wireless telephony.[101] Of these, an estimated 261 have 1,500 or fewer employees and 152 have more than 1,500 employees.[102] Therefore, a little less than one third of these entities can be considered small.

35. *Broadband Personal Communications Service.* The broadband personal communications services (PCS) spectrum is divided into six frequency blocks designated A through F, and the Commission has held auctions for each block. The Commission initially defined a "small business" for C- and F-Block licenses as an entity that has average gross revenues of $40 million or less in the three previous calendar years.[103] For F-Block licenses, an additional small business size standard for "very small business" was added and is defined as an entity that, together with its affiliates, has average gross revenues of not more than $15 million for the preceding three calendar years.[104] These small business size standards, in the context of broadband PCS auctions, have been approved by the SBA.[105] No small businesses within the SBA-approved small business size standards bid successfully for licenses in Blocks A and B. There were 90 winning bidders that claimed small business status in the first two C-Block auctions. A total of 93 bidders that claimed small business status won approximately 40 percent of the 1,479 licenses in the first auction for the D, E, and F Blocks.[106] On April 15, 1999, the Commission completed the reauction of 347 C-, D-, E-, and F-Block licenses in Auction No. 22.[107] Of the 57 winning bidders in that auction, 48 claimed small business status and won 277 licenses.

---

[96] *Amendment of the Commission's Rules to Establish Part 27*, *the Wireless Communications Service (WCS)*, Report and Order, 12 FCC Rcd 10785, 10879, para. 194 (1997).

[97] *See* Letter from Aida Alvarez, Administrator, SBA, to Amy Zoslov, Chief, Auctions and Industry Analysis Division, Wireless Telecommunications Bureau, FCC (filed Dec. 2, 1998) (*Alvarez Letter 1998*).

[98] 47 CFR § 2.106; *see generally* 47 CFR §§ 27.1-27.70.

[99] 13 CFR § 121.201, NAICS code 517210.

[100] *Id*.

[101] *Trends in Telephone Service*, tbl. 5.3.

[102] *Id.*

[103] *See Amendment of Parts 20 and 24 of the Commission's Rules – Broadband PCS Competitive Bidding and the Commercial Mobile Radio Service Spectrum Cap; Amendment of the Commission's Cellular/PCS Cross-Ownership Rule*, Report and Order, 11 FCC Rcd 7824, 7850-52, paras. 57-60 (1996) (*PCS Report and Order*); *see also* 47 CFR § 24.720(b).

[104] *See PCS Report and Order*, 11 FCC Rcd at 7852, para. 60.

[105] *See Alvarez Letter 1998*.

[106] *See Broadband PCS*, *D*, *E and F Block Auction Closes*, Public Notice, Doc. No. 89838 (rel. Jan. 14, 1997).

[107] *See C*, *D*, *E*, *and F Block Broadband PCS Auction Closes*, Public Notice, 14 FCC Rcd 6688 (WTB 1999). Before Auction No. 22, the Commission established a very small standard for the C Block to match the standard

(continued….)

36. On January 26, 2001, the Commission completed the auction of 422 C and F Block Broadband PCS licenses in Auction No. 35. Of the 35 winning bidders in that auction, 29 claimed small business status.[108] Subsequent events concerning Auction 35, including judicial and agency determinations, resulted in a total of 163 C and F Block licenses being available for grant. On February 15, 2005, the Commission completed an auction of 242 C-, D-, E-, and F-Block licenses in Auction No. 58. Of the 24 winning bidders in that auction, 16 claimed small business status and won 156 licenses.[109] On May 21, 2007, the Commission completed an auction of 33 licenses in the A, C, and F Blocks in Auction No. 71.[110] Of the 12 winning bidders in that auction, five claimed small business status and won 18 licenses.[111] On August 20, 2008, the Commission completed the auction of 20 C-, D-, E-, and F-Block Broadband PCS licenses in Auction No. 78.[112] Of the eight winning bidders for Broadband PCS licenses in that auction, six claimed small business status and won 14 licenses.[113]

37. *Specialized Mobile Radio Licenses.* The Commission awards "small entity" bidding credits in auctions for Specialized Mobile Radio (SMR) geographic area licenses in the 800 MHz and 900 MHz bands to firms that had revenues of no more than $15 million in each of the three previous calendar years.[114] The Commission awards "very small entity" bidding credits to firms that had revenues of no more than $3 million in each of the three previous calendar years.[115] The SBA has approved these small business size standards for the 900 MHz Service.[116] The Commission has held auctions for geographic area licenses in the 800 MHz and 900 MHz bands. The 900 MHz SMR auction began on December 5, 1995, and closed on April 15, 1996. Sixty bidders claiming that they qualified as small businesses under the $15 million size standard won 263 geographic area licenses in the 900 MHz SMR band. The 800 MHz SMR auction for the upper 200 channels began on October 28, 1997, and was completed on December 8, 1997. Ten bidders claiming that they qualified as small businesses under the $15 million size standard won 38 geographic area licenses for the upper 200 channels in the 800 MHz SMR band.[117] A second auction for the 800 MHz band was held on January 10, 2002 and closed on January 17, 2002 and included 23 BEA licenses. One bidder claiming small business status won five licenses.[118]

(Continued from previous page)
used for F Block. *Amendment of the Commission's Rules Regarding Installment Payment Financing for Personal Communications Services (PCS) Licensees*, Fourth Report and Order, 13 FCC Rcd 15743, 15768, para. 46 (1998).

[108] *See C and F Block Broadband PCS Auction Closes; Winning Bidders Announced*, Public Notice, 16 FCC Rcd 2339 (2001).

[109] *See Broadband PCS Spectrum Auction Closes; Winning Bidders Announced for Auction No. 58*, Public Notice, 20 FCC Rcd 3703 (2005).

[110] *See Auction of Broadband PCS Spectrum Licenses Closes; Winning Bidders Announced for Auction No. 71*, Public Notice, 22 FCC Rcd 9247 (2007).

[111] *Id*.

[112] *See Auction of AWS-1 and Broadband PCS Licenses Closes; Winning Bidders Announced for Auction 78*, Public Notice, 23 FCC Rcd 12749 (WTB 2008).

[113] *Id.*

[114] 47 CFR § 90.814(b)(1).

[115] *Id*.

[116] *See* Letter from Aida Alvarez, Administrator, SBA, to Thomas Sugrue, Chief, Wireless Telecommunications Bureau, Federal Communications Commission (filed Aug. 10, 1999) (*Alvarez Letter 1999*).

[117] *See Correction to Public Notice DA 96-586 "FCC Announces Winning Bidders in the Auction of 1020 Licenses to Provide 900 MHz SMR in Major Trading Areas,"* Public Notice, 18 FCC Rcd 18367 (WTB 1996).

[118] *See Multi-Radio Service Auction Closes*, Public Notice, 17 FCC Rcd 1446 (WTB 2002).

38. The auction of the 1,053 800 MHz SMR geographic area licenses for the General Category channels began on August 16, 2000, and was completed on September 1, 2000. Eleven bidders won 108 geographic area licenses for the General Category channels in the 800 MHz SMR band and qualified as small businesses under the $15 million size standard.[119] In an auction completed on December 5, 2000, a total of 2,800 Economic Area licenses in the lower 80 channels of the 800 MHz SMR service were awarded.[120] Of the 22 winning bidders, 19 claimed small business status and won 129 licenses. Thus, combining all four auctions, 41 winning bidders for geographic licenses in the 800 MHz SMR band claimed status as small businesses.

39. In addition, there are numerous incumbent site-by-site SMR licenses and licensees with extended implementation authorizations in the 800 and 900 MHz bands. We do not know how many firms provide 800 MHz or 900 MHz geographic area SMR service pursuant to extended implementation authorizations, nor how many of these providers have annual revenues of no more than $15 million. One firm has over $15 million in revenues. In addition, we do not know how many of these firms have 1,500 or fewer employees, which is the SBA-determined size standard.[121] We assume, for purposes of this analysis, that all of the remaining extended implementation authorizations are held by small entities, as defined by the SBA.

40. *Lower 700 MHz Band Licenses*. The Commission previously adopted criteria for defining three groups of small businesses for purposes of determining their eligibility for special provisions such as bidding credits.[122] The Commission defined a "small business" as an entity that, together with its affiliates and controlling principals, has average gross revenues not exceeding $40 million for the preceding three years.[123] A "very small business" is defined as an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $15 million for the preceding three years.[124] Additionally, the lower 700 MHz Service had a third category of small business status for Metropolitan/Rural Service Area (MSA/RSA) licenses—"entrepreneur"—which is defined as an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $3 million for the preceding three years.[125] The SBA approved these small size standards.[126] An auction of 740 licenses (one license in each of the 734 MSAs/RSAs and one license in each of the six Economic Area Groupings (EAGs)) commenced on August 27, 2002, and closed on September 18, 2002. Of the 740 licenses available for auction, 484 licenses were won by 102 winning bidders. Seventy-two of the winning bidders claimed small business, very small business or entrepreneur status and won a total of 329 licenses.[127] A second auction commenced on May 28, 2003, closed on June 13, 2003, and included 256 licenses: 5 EAG licenses and 476 Cellular Market Area licenses.[128] Seventeen winning bidders claimed small or very small business status and won 60 licenses, and nine

[119] *See 800 MHz Specialized Mobile Radio (SMR) Service General Category (851–854 MHz) and Upper Band (861–865 MHz) Auction Closes; Winning Bidders Announced*, Public Notice, 15 FCC Rcd 17162 (2000).

[120] *See 800 MHz SMR Service Lower 80 Channels Auction Closes; Winning Bidders Announced*, Public Notice, 16 FCC Rcd 1736 (2000).

[121] *See generally* 13 CFR § 121.201, NAICS code 517210.

[122] *See Reallocation and Service Rules for the 698–746 MHz Spectrum Band (Television Channels 52–59)*, Report and Order, 17 FCC Rcd 1022 (2002) (*Channels 52–59 Report and Order*).

[123] *See id.* At 1087-88, para. 172.

[124] *See id*.

[125] *See id.*, at 1088, para. 173.

[126] *See Alvarez Letter 1999*.

[127] *See Lower 700 MHz Band Auction Closes*, Public Notice, 17 FCC Rcd 17272 (WTB 2002).

[128] *See id.*

winning bidders claimed entrepreneur status and won 154 licenses.[129] On July 26, 2005, the Commission completed an auction of 5 licenses in the Lower 700 MHz band (Auction No. 60). There were three winning bidders for five licenses. All three winning bidders claimed small business status.

41. In 2007, the Commission reexamined its rules governing the 700 MHz band in the *700 MHz Second Report and Order*.[130] An auction of 700 MHz licenses commenced January 24, 2008 and closed on March 18, 2008, which included, 176 Economic Area licenses in the A Block, 734 Cellular Market Area licenses in the B Block, and 176 EA licenses in the E Block.[131] Twenty winning bidders, claiming small business status (those with attributable average annual gross revenues that exceed $15 million and do not exceed $40 million for the preceding three years) won 49 licenses. Thirty three winning bidders claiming very small business status (those with attributable average annual gross revenues that do not exceed $15 million for the preceding three years) won 325 licenses.

42. *Upper 700 MHz Band Licenses*. In the *700 MHz Second Report and Order*, the Commission revised its rules regarding Upper 700 MHz licenses.[132] On January 24, 2008, the Commission commenced Auction 73 in which several licenses in the Upper 700 MHz band were available for licensing: 12 Regional Economic Area Grouping licenses in the C Block, and one nationwide license in the D Block.[133] The auction concluded on March 18, 2008, with 3 winning bidders claiming very small business status (those with attributable average annual gross revenues that do not exceed $15 million for the preceding three years) and winning five licenses.

43. *700 MHz Guard Band Licensees*. In 2000, in the 700 MHz Guard Band Order, the Commission adopted size standards for "small businesses" and "very small businesses" for purposes of determining their eligibility for special provisions such as bidding credits and installment payments.[134] A small business in this service is an entity that, together with its affiliates and controlling principals, has average gross revenues not exceeding $40 million for the preceding three years.[135] Additionally, a very small business is an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $15 million for the preceding three years.[136] SBA approval of these definitions is not required.[137] An auction of 52 Major Economic Area licenses commenced on September

[129] *See id.*

[130] *Service Rules for the 698–746*, *747–762 and 777–792 MHz Band; Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems; Section 68.4(a) of the Commission's Rules Governing Hearing Aid-Compatible Telephones; Biennial Regulatory Review—Amendment of Parts 1*, *22*, *24*, *27*, *and 90 to Streamline and Harmonize Various Rules Affecting Wireless Radio Services; Former Nextel Communications*, *Inc. Upper 700 MHz Guard Band Licenses and Revisions to Part 27 of the Commission's Rules; Implementing a Nationwide*, *Broadband*, *Interoperable Public Safety Network in the 700 MHz Band; Development of Operational*, *Technical and Spectrum Requirements for Meeting Federal*, *State and Local Public Safety Communications Requirements Through the Year 2010; Declaratory Ruling on Reporting Requirement under Commission's Part 1 Anti-Collusion Rule*, Second Report and Order, 22 FCC Rcd 15289, 15359 n. 434 (2007) (*700 MHz Second Report and Order*).

[131] *See Auction of 700 MHz Band Licenses Closes*, Public Notice, 23 FCC Rcd 4572 (WTB 2008).

[132] *700 MHz Second Report and Order*, 22 FCC Rcd 15289.

[133] *See Auction of 700 MHz Band Licenses Closes*, Public Notice, 23 FCC Rcd 4572 (WTB 2008).

[134] *See Service Rules for the 746–764 MHz Bands*, *and Revisions to Part 27 of the Commission's Rules*, Second Report and Order, 15 FCC Rcd 5299 (2000) (*746–764 MHz Band Second Report and Order*).

[135] *See id.* at 5343, para. 108.

[136] *See id.*

[137] *See id.* at 5343, para. 108 n.246 (for the 746–764 MHz and 776–794 MHz bands, the Commission is exempt from 15 U.S.C. § 632, which requires Federal agencies to obtain SBA approval before adopting small business size standards).

6, 2000, and closed on September 21, 2000.[138] Of the 104 licenses auctioned, 96 licenses were sold to nine bidders. Five of these bidders were small businesses that won a total of 26 licenses. A second auction of 700 MHz Guard Band licenses commenced on February 13, 2001, and closed on February 21, 2001. All eight of the licenses auctioned were sold to three bidders. One of these bidders was a small business that won a total of two licenses.[139]

44. *Air-Ground Radiotelephone Service*. The Commission has previously used the SBA's small business size standard applicable to Wireless Telecommunications Carriers (except Satellite), i.e., an entity employing no more than 1,500 persons.[140] There are approximately 100 licensees in the Air-Ground Radiotelephone Service, and under that definition, we estimate that almost all of them qualify as small entities under the SBA definition. For purposes of assigning Air-Ground Radiotelephone Service licenses through competitive bidding, the Commission has defined "small business" as an entity that, together with controlling interests and affiliates, has average annual gross revenues for the preceding three years not exceeding $40 million.[141] A "very small business" is defined as an entity that, together with controlling interests and affiliates, has average annual gross revenues for the preceding three years not exceeding $15 million.[142] These definitions were approved by the SBA.[143] In May 2006, the Commission completed an auction of nationwide commercial Air-Ground Radiotelephone Service licenses in the 800 MHz band (Auction No. 65). On June 2, 2006, the auction closed with two winning bidders winning two Air-Ground Radiotelephone Services licenses. Neither of the winning bidders claimed small business status.

45. *AWS Services (1710–1755 MHz and 2110–2155 MHz bands (AWS-1); 1915–1920 MHz, 1995–2000 MHz, 2020–2025 MHz and 2175–2180 MHz bands (AWS-2); 2155–2175 MHz band (AWS-3))*. For the AWS-1 bands,[144] the Commission has defined a "small business" as an entity with average annual gross revenues for the preceding three years not exceeding $40 million, and a "very small business" as an entity with average annual gross revenues for the preceding three years not exceeding $15 million. For AWS-2 and AWS-3, although we do not know for certain which entities are likely to apply for these frequencies, we note that the AWS-1 bands are comparable to those used for cellular service and personal communications service. The Commission has not yet adopted size standards for the AWS-2 or AWS-3 bands but proposes to treat both AWS-2 and AWS-3 similarly to broadband PCS service and AWS-1 service due to the comparable capital requirements and other factors, such as issues involved in relocating incumbents and developing markets, technologies, and services.[145]

---

[138] *See 700 MHz Guard Bands Auction Closes: Winning Bidders Announced*, Public Notice, 15 FCC Rcd 18026 (WTB 2000).

[139] *See 700 MHz Guard Bands Auction Closes: Winning Bidders Announced*, Public Notice, 16 FCC Rcd 4590 (WTB 2001).

[140] 13 CFR § 121.201, NAICS codes 517210.

[141] *Amendment of Part 22 of the Commission's Rules to Benefit the Consumers of Air-Ground Telecommunications Services*, *Biennial Regulatory Review—Amendment of Parts 1*, *22*, *and 90 of the Commission's Rules*, *Amendment of Parts 1 and 22 of the Commission's Rules to Adopt Competitive Bidding Rules for Commercial and General Aviation Air-Ground Radiotelephone Service*, Order on Reconsideration and Report and Order, 20 FCC Rcd 19663, paras. 28-42 (2005).

[142] *Id.*

[143] *See* Letter from Hector V. Barreto, Administrator, SBA, to Gary D. Michaels, Deputy Chief, Auctions and Spectrum Access Division, Wireless Telecommunications Bureau, Federal Communications Commission (filed Sept. 19, 2005).

[144] The service is defined in section 90.1301 *et seq*. of the Commission's Rules, 47 CFR § 90.1301 *et seq*.

[145] *See Service Rules for Advanced Wireless Services in the 1.7 GHz and 2.1 GHz Bands*, Report and Order, 18 FCC Rcd 25162, Appx. B (2003), *modified by Service Rules for Advanced Wireless Services in the 1.7 GHz and 2.1 GHz*

(continued….)

46. *3650–3700 MHz band*. In March 2005, the Commission released a *Report and Order and Memorandum Opinion and Order* that provides for nationwide, non-exclusive licensing of terrestrial operations, utilizing contention-based technologies, in the 3650 MHz band (i.e., 3650–3700 MHz). As of April 2010, more than 1270 licenses have been granted and more than 7433 sites have been registered. The Commission has not developed a definition of small entities applicable to 3650–3700 MHz band nationwide, non-exclusive licensees. However, we estimate that the majority of these licensees are Internet Access Service Providers (ISPs) and that most of those licensees are small businesses.

47. *Fixed Microwave Services.* Microwave services include common carrier,[146] private-operational fixed,[147] and broadcast auxiliary radio services.[148] They also include the Local Multipoint Distribution Service (LMDS),[149] the Digital Electronic Message Service (DEMS),[150] and the 24 GHz Service,[151] where licensees can choose between common carrier and non-common carrier status.[152] At present, there are approximately 36,708 common carrier fixed licensees and 59,291 private operational-fixed licensees and broadcast auxiliary radio licensees in the microwave services. There are approximately 135 LMDS licensees, three DEMS licensees, and three 24 GHz licensees. The Commission has not yet defined a small business with respect to microwave services. For purposes of the IRFA, we will use the SBA's definition applicable to Wireless Telecommunications Carriers (except satellite)—i.e., an entity with no more than 1,500 persons.[153] Under the present and prior categories, the SBA has deemed a wireless business to be small if it has 1,500 or fewer employees.[154] The Commission does not have data specifying the number of these licensees that have more than 1,500 employees, and thus is unable at this time to estimate with greater precision the number of fixed microwave service licensees that would qualify as small business concerns under the SBA's small business size standard. Consequently, the Commission estimates that there are up to 36,708 common carrier fixed licensees and up to 59,291 private operational-fixed licensees and broadcast auxiliary radio licensees in the microwave services that may be small and may be affected by the rules and policies adopted herein. We note, however, that the common carrier microwave fixed licensee category includes some large entities.

48. *Broadband Radio Service and Educational Broadband Service.* Broadband Radio Service systems, previously referred to as Multipoint Distribution Service (MDS) and Multichannel

(Continued from previous page)
*Bands*, Order on Reconsideration, 20 FCC Rcd 14058, Appx. C (2005); *Service Rules for Advanced Wireless Services in the 1915–1920 MHz*, *1995–2000 MHz*, *2020–2025 MHz and 2175–2180 MHz Bands; Service Rules for Advanced Wireless Services in the 1.7 GHz and 2.1 GHz Bands*, Notice of Proposed Rulemaking, 19 FCC Rcd 19263, Appx. B (2005); *Service Rules for Advanced Wireless Services in the 2155–2175 MHz Band*, Notice of Proposed Rulemaking, 22 FCC Rcd 17035, Appx. (2007).

[146] *See* 47 CFR Part 101, Subparts C and I.

[147] *See* 47 CFR Part 101, Subparts C and H.

[148] Auxiliary Microwave Service is governed by Part 74 of Title 47 of the Commission's Rules. *See* 47 CFR Part 74. Available to licensees of broadcast stations and to broadcast and cable network entities, broadcast auxiliary microwave stations are used for relaying broadcast television signals from the studio to the transmitter, or between two points such as a main studio and an auxiliary studio. The service also includes mobile TV pickups, which relay signals from a remote location back to the studio.

[149] *See* 47 CFR Part 101, Subpart L.

[150] *See* 47 CFR Part 101, Subpart G.

[151] *See id.*

[152] *See* 47 CFR §§ 101.533, 101.1017.

[153] 13 CFR § 121.201, NAICS code 517210.

[154] 13 CFR § 121.201, NAICS code 517210 (2007 NAICS). The now-superseded, pre-2007 CFR citations were 13 CFR § 121.201, NAICS codes 517211 and 517212 (referring to the 2002 NAICS).

Multipoint Distribution Service (MMDS) systems, and "wireless cable," transmit video programming to subscribers and provide two-way high speed data operations using the microwave frequencies of the Broadband Radio Service (BRS) and Educational Broadband Service (EBS) (previously referred to as the Instructional Television Fixed Service (ITFS)).[155] In connection with the 1996 BRS auction, the Commission established a small business size standard as an entity that had annual average gross revenues of no more than $40 million in the previous three calendar years.[156] The BRS auctions resulted in 67 successful bidders obtaining licensing opportunities for 493 Basic Trading Areas (BTAs). Of the 67 auction winners, 61 met the definition of a small business. BRS also includes licensees of stations authorized prior to the auction. At this time, we estimate that of the 61 small business BRS auction winners, 48 remain small business licensees. In addition to the 48 small businesses that hold BTA authorizations, there are approximately 392 incumbent BRS licensees that are considered small entities.[157] After adding the number of small business auction licensees to the number of incumbent licensees not already counted, we find that there are currently approximately 440 BRS licensees that are defined as small businesses under either the SBA or the Commission's rules.

49. In 2009, the Commission conducted Auction 86, the sale of 78 licenses in the BRS areas.[158] The Commission offered three levels of bidding credits: (i) a bidder with attributed average annual gross revenues that exceed $15 million and do not exceed $40 million for the preceding three years (small business) received a 15 percent discount on its winning bid; (ii) a bidder with attributed average annual gross revenues that exceed $3 million and do not exceed $15 million for the preceding three years (very small business) received a 25 percent discount on its winning bid; and (iii) a bidder with attributed average annual gross revenues that do not exceed $3 million for the preceding three years (entrepreneur) received a 35 percent discount on its winning bid.[159] Auction 86 concluded in 2009 with the sale of 61 licenses.[160] Of the ten winning bidders, two bidders that claimed small business status won 4 licenses; one bidder that claimed very small business status won three licenses; and two bidders that claimed entrepreneur status won six licenses.

50. In addition, the SBA's Cable Television Distribution Services small business size standard is applicable to EBS. There are presently 2,436 EBS licensees. All but 100 of these licenses are held by educational institutions. Educational institutions are included in this analysis as small entities.[161] Thus, we estimate that at least 2,336 licensees are small businesses. Since 2007, Cable Television Distribution Services have been defined within the broad economic census category of Wired Telecommunications Carriers; that category is defined as follows: "This industry comprises

[155] *Amendment of Parts 21 and 74 of the Commission's Rules with Regard to Filing Procedures in the Multipoint Distribution Service and in the Instructional Television Fixed Service and Implementation of Section 309(j) of the Communications Act—Competitive Bidding*, Report and Order, 10 FCC Rcd 9589, 9593, para. 7 (1995).

[156] 47 CFR § 21.961(b)(1).

[157] 47 U.S.C. § 309(j). Hundreds of stations were licensed to incumbent MDS licensees prior to implementation of Section 309(j) of the Communications Act of 1934, 47 U.S.C. § 309(j). For these pre-auction licenses, the applicable standard is SBA's small business size standard of 1500 or fewer employees.

[158] *Auction of Broadband Radio Service (BRS) Licenses, Scheduled for October 27, 2009, Notice and Filing Requirements, Minimum Opening Bids, Upfront Payments, and Other Procedures for Auction 86*, Public Notice, 24 FCC Rcd 8277 (2009).

[159] *Id.* at 8296 para. 73.

[160] *Auction of Broadband Radio Service Licenses Closes, Winning Bidders Announced for Auction 86, Down Payments Due November 23, 2009, Final Payments Due December 8, 2009, Ten-Day Petition to Deny Period*, Public Notice, 24 FCC Rcd 13572 (2009).

[161] The term "small entity" within SBREFA applies to small organizations (nonprofits) and to small governmental jurisdictions (cities, counties, towns, townships, villages, school districts, and special districts with populations of less than 50,000). 5 U.S.C. §§ 601(4)-(6). We do not collect annual revenue data on EBS licensees.

establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired telecommunications networks. Transmission facilities may be based on a single technology or a combination of technologies."[162] The SBA has developed a small business size standard for this category, which is: all such firms having 1,500 or fewer employees. To gauge small business prevalence for these cable services we must, however, use the most current census data that are based on the previous category of Cable and Other Program Distribution and its associated size standard; that size standard was: all such firms having $13.5 million or less in annual receipts.[163] According to Census Bureau data for 2007, there were a total of 996 firms in this category that operated for the entire year.[164] Of this total, 948 firms had annual receipts of under $10 million, and 48 firms had receipts of $10 million or more but less than $25 million.[165] Thus, the majority of these firms can be considered small.

### 5. Satellite Service Providers

51. *Satellite Telecommunications Providers.* Two economic census categories address the satellite industry. The first category has a small business size standard of $30 million or less in average annual receipts, under SBA rules.[166] The second has a size standard of $30 million or less in annual receipts.[167]

52. The category of Satellite Telecommunications "comprises establishments primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications."[168] For this category, Census Bureau data for 2012 show that there were a total of 333 firms that operated for the entire year.[169] Of this total, 299 firms had annual receipts of under $25 million.[170] Consequently, we estimate that the majority of Satellite Telecommunications firms are small entities that might be affected by our action.

53. The second category of Other Telecommunications comprises, *inter alia*, "establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation. This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems."[171] For this category, census data for 2012 show that there

[162] U.S. Census Bureau, 2012 NAICS Definitions, "517110 Wired Telecommunications Carriers," (partial definition), http://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517110&search=2012.

[163] 13 CFR § 121.201, NAICS code 517110.

[164] U.S. Census Bureau, 2007 Economic Census, Subject Series: Information, Receipts by Enterprise Employment Size for the United States: 2007, NAICS code 517510 (rel. Nov. 19, 2010).

[165] *Id*.

[166] 13 CFR § 121.201, NAICS Code 517410.

[167] 13 CFR § 121.201, NAICS Code 517919.

[168] U.S. Census Bureau, 2012 NAICS Definitions, "517410 Satellite Telecommunications," http://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517410&search=2012.

[169] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1251SSSZ4, Information: Subject Series - Estab and Firm Size: Receipts Size of Firms for the United States: 2012, NAICS code 517410 http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ4&prodType=table.

[170] *Id*.

[171] U.S. Census Bureau, 2012 NAICS Definitions, "517919 All Other Telecommunications," http://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517919&search=2012.

were 1,442 firms that operated for the entire year. Of these firms, a total of 1,400 had gross annual receipts of less than $25 million.[172] Thus, a majority of "All Other Telecommunications" firms potentially affected by the rules adopted can be considered small.

### 6. Cable Service Providers

54. *Cable and Other Program Distributors*. Since 2007, these services have been defined within the broad economic census category of Wired Telecommunications Carriers; that category is defined as follows: "This industry comprises establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired telecommunications networks. Transmission facilities may be based on a single technology or a combination of technologies."[173] The SBA has developed a small business size standard for this category, which is: all such firms having 1,500 or fewer employees. To gauge small business prevalence for these cable services we must, however, use current census data that are based on the previous category of Cable and Other Program Distribution and its associated size standard; that size standard was: all such firms having $13.5 million or less in annual receipts.[174] According to Census Bureau data for 2007, there were a total of 2,048 firms in this category that operated for the entire year.[175] Of this total, 1,393 firms had annual receipts of under $10 million, and 655 firms had receipts of $10 million or more.[176] Thus, the majority of these firms can be considered small.

55. *Cable Companies and Systems*. The Commission has also developed its own small business size standards, for the purpose of cable rate regulation. Under the Commission's rules, a "small cable company" is one serving 400,000 or fewer subscribers, nationwide.[177] Industry data shows that there were 1,141 cable companies at the end of June 2012.[178] Of this total, all but ten cable operators nationwide are small under this size standard.[179] In addition, under the Commission's rules, a "small

[172] http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ4&prodType=table.

[173] U.S. Census Bureau, 2012 NAICS Definitions, "517110 Wired Telecommunications Carriers," (partial definition), http://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517110&search=2012.

[174] 13 CFR § 121.201, NAICS code 517110.

[175] U.S. Census Bureau, 2007 Economic Census, Subject Series: Information, "Establishment and Firm Size," NAICS code 517110 (rel. Nov. 19, 2010).

[176] *Id*.

[177] 47 CFR § 76.901(e). The Commission determined that this size standard equates approximately to a size standard of $100 million or less in annual revenues. *Implementation of Sections of the 1992 Cable Act: Rate Regulation*, Sixth Report and Order and Eleventh Order on Reconsideration, 10 FCC Rcd 7393, 7408 (1995).

[178] NCTA, Industry Data, Number of Cable Operating Companies (June 2012), http://www.ncta.com/Statistics.aspx (visited Sept. 28, 2012). Depending upon the number of homes and the size of the geographic area served, cable operators use one or more cable systems to provide video service. *See Annual Assessment of the Status of Competition in the Market for Delivery of Video Programming*, Fifteenth Report, 28 FCC Rcd 10496, 10505-06, para. 24 (2013) (*15th Annual Competition Report)*.

[179] *See* SNL Kagan, "Top Cable MSOs – 12/12 Q", http://www.snl.com/InteractiveX/TopCableMSOs.aspx?period=2012Q4&sortcol=subscribersbasic&sortorder=desc. We note that, when applied to an MVPD operator, under this size standard (i.e., 400,000 or fewer subscribers) all but 14 MVPD operators would be considered small. *See* NCTA, Industry Data, Top 25 Multichannel Video Service Customers (2012), http://www.ncta.com/industry-data. The Commission applied this size standard to MVPD operators in its implementation of the CALM Act. *See Implementation of the Commercial Advertisement Loudness Mitigation (CALM) Act*, Report and Order, 26 FCC Rcd 17222, 17245-46, para. 37 (2011) (*CALM Act Report and Order*) (defining a smaller MVPD operator as one serving 400,000 or fewer subscribers nationwide, as of December 31, 2011).

system" is a cable system serving 15,000 or fewer subscribers.[180] Current Commission records show 4,945 cable systems nationwide.[181] Of this total, 4,380 cable systems have less than 20,000 subscribers, and 565 systems have 20,000 or more subscribers, based on the same records. Thus, under this standard, we estimate that most cable systems are small entities.

56. *Cable System Operators*. The Communications Act also contains a size standard for small cable system operators, which is "a cable operator that, directly or through an affiliate, serves in the aggregate fewer than 1 percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000."[182] There are approximately 52,403,705 cable video subscribers in the United States today.[183] Accordingly, an operator serving fewer than 524,037 subscribers shall be deemed a small operator if its annual revenues, when combined with the total annual revenues of all its affiliates, do not exceed $250 million in the aggregate.[184] Based on available data, we find that all but nine incumbent cable operators are small entities under this size standard.[185] We note that the Commission neither requests nor collects information on whether cable system operators are affiliated with entities whose gross annual revenues exceed $250 million.[186] Although it seems certain that some of these cable system operators are affiliated with entities whose gross annual revenues exceed $250 million, we are unable at this time to estimate with greater precision the number of cable system operators that would qualify as small cable operators under the definition in the Communications Act.

### 7. All Other Telecommunications

57. **"**All Other Telecommunications" is defined as follows: This U.S. industry is comprised of establishments that are primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation. This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems. Establishments providing Internet services or voice over Internet protocol (VoIP) services via client-supplied telecommunications connections are also included in this industry.[187] The SBA has developed a small business size standard for "All Other Telecommunications," which consists of all such firms with gross annual receipts of $32.5 million or less.[188] For this category, census data for 2012 show that there were 1,442 firms that operated for the entire year. Of these firms, a total of 1,400 had gross annual receipts of less than $25 million.[189] Thus, a majority of "All Other Telecommunications" firms potentially affected by the rules adopted can be considered small.

---

[180] 47 CFR § 76.901(c).

[181] The number of active, registered cable systems comes from the Commission's Cable Operations and Licensing System (COALS) database on Aug. 28, 2013. A cable system is a physical system integrated to a principal headend.

[182] 47 CFR § 76.901 (f) and notes ff. 1, 2, and 3.

[183] *See* SNL KAGAN at www.snl.com/interactivex/MultichannelIndustryBenchmarks.aspx.

[184] 47 CFR § 76.901(f) and notes ff. 1, 2, and 3.

[185] *See* SNL KAGAN at www.snl.com/interactivex/TopCable MSOs.aspx.

[186] The Commission does receive such information on a case-by-case basis if a cable operator appeals a local franchise authority's finding that the operator does not qualify as a small cable operator pursuant to section 76.901(f) of the Commission's rules. *See* 47 CFR § 76.901(f).

[187] http://www.census.gov/cgi-bin/ssssd/naics/naicsrch.

[188] 13 CFR § 121.201; NAICS Code 517919

[189] http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ4&prodType=table.

### E. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

58. The Order adopts requirements concerning (1) the provision of meaningful notice of privacy policies; (2) customer approval for the use and disclosure of customer PI; (3) reasonable data security; (4) data breach notification; and (5) particular practices that raise privacy concerns. The rules we adopt in the Order will apply to all telecommunications carriers, including BIAS and voice service providers.

59. *Providing Meaningful Notice of Privacy Policies.* We adopt privacy policy notice requirements for all telecommunications carriers, including small providers. We require telecommunications carriers to provide notices of privacy policies at the point of sale prior to the purchase of service, and also to make notices clearly, conspicuously, and persistently available on carriers' websites and via carriers' apps that are used to manage service, if any. These notices must clearly inform customers about what customer proprietary information the providers collect, how they use it, and under what circumstances they share it. We also require that providers inform their customers about customers' rights to opt in to or out (as the case may be) of the use or sharing of their proprietary information. We require that privacy notices be clear, conspicuous, comprehensible, and not misleading; and written in the language with which the carrier transacts business with the customer; but we do not require that they be formatted in any specific manner. Finally, we require providers to give their customers advance notice of material changes to their privacy policies.[190] We have declined to require periodic notice on an annual or bi-annual basis, similar to what the preexisting CPNI rules require.

60. *Customer Approval Requirements for the Use and Disclosure of Customer PI.* We require carriers to obtain express, informed customer consent (i.e., opt-in approval) for the use and sharing of sensitive customer PI. With respect to non-sensitive customer PI, carriers must, at a minimum, provide their customers the ability to opt out of the carrier's use or sharing of that non-sensitive customer information. Carriers must also provide customers with easy access to a choice mechanism that is simple, easy-to-use, clearly and conspicuously disclosed, persistently available, and made available at no additional cost to the customer.[191] We require telecommunications carriers to solicit customer approval at the point of sale, and permit further solicitations after the point of sale. We also require that carriers actively contact their customers in these subsequent solicitations, to ensure that customers are adequately informed. Finally, we require the solicitations to be clear and conspicuous, comprehensible, not misleading, and to contain the information necessary for a customer to make an informed choice. This means the solicitations must inform customers of the types of customer proprietary information that the carrier is seeking to use, disclose, or permit access to, how those types of information will be used or shared, and the categories of entities with which that information is shared. In order to maintain flexibility, we do not require particular formats or methods by which a carrier must communicate its solicitation of consent to customers.[192]

61. Our rules allow providers to use and disclose customer data without approval if the data is properly de-identified. This option gives providers carriers, including small providers, a way to use customer information that avoids both the risks associated with identifiable information and any compliance costs associated with obtaining customer approval.[193]

62. *Reasonable Data Security*. We require telecommunications carriers to take reasonable measures to secure customer PI. We decline to mandate specific activities that providers must undertake in order to meet this reasonableness requirement. We do, however, offer guidance on the types of data

[190] *See supra* Part III.C.

[191] *See supra* Part III.D.

[192] *See id.*

[193] *See supra* Part III.B.4.

security practices we recommend carriers strongly consider as they seek to comply with our data security requirement, while recognizing that what constitutes "reasonable" data security is an evolving concept. When considering whether a carrier's data security practices are reasonable, we will weigh the nature and scope of the carrier's activities, the sensitivity of the underlying data, the size of the carrier, and technical feasibility. We recognize that the resources and data practices of small carriers are likely to be different from large carriers, and therefore what constitutes "reasonable" data security for a small carrier and a large carrier may differ. The totality of the circumstances, and not any individual factor, is determinative of whether a carrier's practices are reasonable. By requiring providers to take reasonable data security measures, we make clear that providers will not be held strictly liable for all data breaches.[194]

63. *Data Breach Notification Requirements.* We require BIAS providers and other telecommunications carriers to notify affected customers, the Commission—and, when a breach affects 5,000 or more customers, the FBI and Secret Service—of data breaches that meet a harm-based trigger. In particular, a carrier must report the breach unless it reasonably determines that no harm to customers is reasonably likely to occur. Customer breach notifications must include the date, estimated date, or estimated date range of the breach; a description of the customer PI that was breached; contact information for the carrier; contact information for the FCC and any relevant state agencies; and information about credit-reporting agencies and steps customers can take to avoid identity theft.[195] We also require providers to keep records, for two years, of the dates of breaches and the dates when customers are notified.

64. When a reportable breach affects 5,000 or more customers, a provider must notify the Commission and the FBI and Secret Service within seven (7) business days of when the carrier reasonably determines that such a breach has occurred, and at least three (3) business days before notifying customers. The Commission will create a centralized portal for reporting breaches to the Commission and other federal law enforcement agencies.[196] Carriers must notify affected customers without unreasonable delay, and no later than 30 calendar days following the carriers' reasonable determination that a breach has occurred, unless the FBI or Secret Service requests a further delay. When a reportable breach does not meet the 5,000-customer threshold for reporting to the FBI and Secret Service, the Commission may be notified of the breach within the same no-more-than-30-days timeframe as affected customers.

65. *Particular Practices That Raise Privacy Concerns.* The Order prohibits BIAS providers from conditioning the provision of service on a customer's consenting to use or sharing of the customer's proprietary information over which our rules provide the consumer with a right of approval.[197] However, the Order does not prohibit BIAS providers from offering financial incentives to permit the use or disclosure of such information.[198] The Order requires BIAS providers offering such incentives to provide clear notice explaining the terms of any financial incentive program and to obtain opt-in consent. The notice must be clear and conspicuous and explained in a way that is comprehensible and not misleading. The explanation must include information about what customer PI the provider will collect, how it will be used, with what types of entities it will be shared, and for what purposes.[199] BIAS providers must make financial incentive notices easily accessible and separate from any other privacy notifications.[200] When a

[194] *See supra* Part III.E.

[195] *See supra* Part III.F.

[196] *See id.*

[197] *See supra* Part III.G.2.

[198] *See id.*

[199] *See id.*

[200] *See id.*

BIAS provider markets a service plan that involves an exchange of personal information for reduced pricing or other benefits, it must also provide at least as prominent information to customers about an equivalent plan that does not include such an exchange. BIAS providers must also comply with all notice requirements of our rules when providing a financial incentive notice.[201]

### F. Steps Take to Minimize the Significant Economic Impact on Small Entities and Significant Alternatives Considered

66. The RFA requires an agency to describe any significant, specifically small business, alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rule for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities."[202]

67. The Commission considered the economic impact on small providers, as identified in comments filed in response to the *NPRM* and IRFA, in reaching its final conclusions and taking action in this proceeding. Moreover, in formulating these rules, we have sought to provide flexibility for small providers whenever possible, including by avoiding prescription of the specific practices carriers must follow to achieve compliance.[203] Additionally, harmonizing our rules across all telecommunications services will reduce and streamline compliance costs for small carriers.[204] We have also adopted a phased-in implementation schedule, under which small providers are given an extra twelve months to come into compliance with the notice and approval requirements we adopt today. As discussed below, we have designed the rules we adopt today with the goal of minimizing burdens on all carriers, and particularly on small carriers.

68. *Providing Meaningful Notice of Privacy Policies*. Recognizing the importance of flexibility in finding successful ways to communicate privacy policies to consumers, we decline to adopt any specific form or format for privacy notices. We adopt rules that require providers to disclose their privacy practices, but decline 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 this requirement. In the interest of further minimizing the burden of transparency, particularly for small providers, we also direct the Consumer Advisory Committee to develop a model privacy policy notice that will serve as a safe harbor for our notice requirements.[205] We also decline to adopt specific notice requirements in mobile formats and we decline to require periodic notices of privacy practices.[206]

69. *Customer Approval Requirements for the Use and Disclosure of Customer PI*. In formulating customer approval requirements we have taken specific actions to reduce burdens on small carriers. First, as requested by small carriers and other commenters, we harmonize the voice and BIAS customer approval regimes into one set of rules.[207] Second, we do not require carriers to provide a "privacy dashboard" for customer approvals; carriers may use any choice mechanism that is easy to use, persistently available, and clearly and conspicuously provided. This reduces the need for small carriers to

[201] *See supra* Part III.C.

[202] 5 U.S.C. § 603(c)(1)–(c)(4).

[203] *See supra, e.g.*, Parts III.E.1; III.F.1.

[204] *See, e.g.*, ACA Comments at 57-58; WTA-NexTech Ex Parte at 1-2.

[205] *See supra* paras. 153-155.

[206] *See supra* paras. 143, 152.

[207] *See supra* para. 171.

develop specific customer service architecture.[208] Third, we decline to require a specific format for accepting customer privacy choices and therefore allow carriers, particularly small carriers, that lack sophisticated websites or apps to accept customer choices through other means, such as by email or phone, so long as these means are persistently available. Fourth, we eliminate the periodic compliance documentation and reporting requirements that create recordkeeping burdens in our pre-existing CPNI rules.[209] To further reduce compliance burdens, we have clarified that choice solicitations may be combined a carrier's other privacy policy notices.

70. *Reasonable Data Security*. In the *NPRM* we proposed rules that included an overarching data security expectation and specified particular types of practices that carriers would need to implement to comply with that standard, while allowing carriers flexibility in implementing the proposed requirements. Based on the record in this proceeding, we have modified the overarching data security standard to more directly focus on reasonableness of the carriers' data security practices based on the particulars of the carrier's situation. Also based on the record, we decline to mandate specific activities that carriers must undertake in order to meet the reasonable data security requirement. We do, however, offer guidance on the types of data security practices we recommend carriers strongly consider as they seek to comply with our data security requirement—recognizing, of course, that what constitutes "reasonable" data security is an evolving concept.[210] This guidance should be of particular benefit to smaller providers that may have less established data security programs. Also, our rule directs all providers—including small providers—to adopt contextually appropriate security practices. Contextual factors specified in the rule include the size of the provider and nature and scope of its activities. In including such factors, we take into account small providers' concerns that certain security measures that may be appropriate for larger carriers, such as having a dedicated official to oversee data security implementation, are likely beyond the needs and resources of the smallest carriers.

71. *Data Breach Notification Requirements*. In formulating our data breach rules, we specifically considered their impact on small carriers and crafted rules designed to balance the burdens on small carriers with the privacy and information security needs of those carriers' customers. First, our adoption of a harm-based trigger substantially reduces compliance burdens on small carriers by not requiring excessive notifications and by granting carriers the flexibility to focus their limited resources on preventing and ameliorating breaches, rather than issuing notifications for inconsequential events. The record shows that because small carriers tend to collect and use customer data far less extensively than larger carriers, they are less likely to have breaches that would trigger the notification requirements of our rules.[211] Second, our customer notification timeline also provides small carriers with greater flexibility; allowing up to 30 days to notify customers of a breach allows small carriers with fewer resources more time to investigate than the 10 days originally proposed. Third, we are creating a centralized portal for reporting data breaches to the Commission and law enforcement. This will streamline the notification process, which particularly reduces burdens on small carriers with fewer staff dedicated to breach mitigation.[212] Finally, for breaches affecting fewer than 5,000 customers, we extend the Commission notification deadline from seven (7) business days to thirty (30) calendar days. This provision will significantly reduce compliance burdens for small carriers, many of whom have fewer than 5,000 customers.[213]

72. *Implementation*. To provide certainty to customers and carriers alike, we establish a

[208] *See supra* Part III.D.4.

[209] *See supra* Part III.D.5.

[210] *See supra* Part III.E.2.

[211] *See supra* Part III.F.1.

[212] *See supra* Part III.F.2.

[213] *See supra* Part III.F.3.

timeline by which carriers must implement the privacy rules we adopt today. Carriers that have complied with FTC and industry best practices will be well-positioned to achieve prompt compliance with our privacy rules. We recognize, however, that carriers, especially small carriers, will need some time to update their internal business processes as well as their customer-facing privacy policies and choice mechanisms in order to come into compliance with some of our rules.[214]

73. The notice and choice rules we adopt today will become effective the later of (1) eight weeks after announcement PRA approval, or (12) twelve months after the Commission publishes a summary of the Order in the Federal Register. Carriers will need to analyze the new, harmonized privacy rules as well as coordinate with various business segments and vendors, and update programs and policies. Carriers will also need to engage in consumer outreach and education. These implementation steps will take time and we find, as supported in the record, that twelve months after publication of the Order in the Federal Register is an adequate minimum implementation period to implement the new notice and approval rules.[215] In order to minimize disruption to carriers' business practices, we do not require carriers to obtain new consent from all their customers. Rather, we treat as valid or "grandfather" any customer consent that was obtained prior to the effective date of our rules and thus is consistent with our new requirements. We decline to more broadly grandfather preexisting consents obtained by small carriers because we find that the parameters set forth in our rules create the appropriate balance to limit compliance costs while providing customers the privacy protections they need.[216]

74. The data breach rule we adopt today will become effective the later of (1) eight weeks after announcement PRA approval, or (2) six months after the Commission publishes a summary of the Order in the Federal Register. Although we recognize that carriers may have to modify practices and policies to implement our new rule, we find the harm trigger we adopt and timeline for notifying customers lessen the implementation requirements. Moreover, harmonization of our data breach rule for BIAS and voice services enable providers to streamline their notification processes, which should also lessen carriers' need for implementation time. Given these steps to minimize compliance burdens, we find six months is an adequate minimum timeframe.[217]

75. The data security requirements we adopt today will become effective 90 days after publication of a summary of the Order in the Federal Register. We find this to be an appropriate implementation period for the data security requirements because carriers should already be largely in compliance with these requirements because the reasonableness standard adopted in this Order provides carriers flexibility in how to approach data security and resembles the obligation to which they were previously subject pursuant to Section 5 of the FTC Act. We therefore do not think the numerous steps outlined by commenters that would have been necessary to comply with the data security proposals in the *NPRM* apply to the data security rules we adopt.[218]

76. The prohibition on conditioning offers to provider BIAS on a customer's agreement to waive privacy rights will become effective 30 days after publication of a summary of the Order in the Federal Register. We find that unlike other privacy rules, consumers should benefit from this prohibition promptly. We find no basis for any delay in the effective date of this important protection. All other privacy rules adopted in the Order will be effective 30 days after publication of a summary of the Order in

[214] *See supra* Part III.I.

[215] *See supra* Part III.I.1.

[216] *See supra* Part III.I.3.

[217] *See supra* Part III.I.1.

[218] *See id.*

the Federal Register.[219] We also adopt a uniform implementation timetable for both BIAS and other telecommunications services.[220]

77. To provide additional flexibility to small carriers, we give small carriers an additional twelve months to implement the notice and customer approval rules we adopt today.[221] We find that an additional one-year phase-in will allow small providers time to make the necessary investments to implement these rules. The record reflects that small providers have comparatively limited resources and rely extensively on vendors over which they have limited leverage to compel adoption of new requirements. We recognize our notice and choice framework may entail upfront costs for small carriers. As such, we find that this limited extension is appropriate.[222]

78. We have considered, but opt against, providing small providers with even longer or broader extension periods, or with exemptions from the rules, as some commenters suggest.[223] In part, this is because the measures we have taken to reduce burdens for small providers have in many cases mitigated commenters' specific concerns. For instance, we find that we have addressed small provider concerns about the adoption of specific security requirements, such as annual risk assessments, by adopting a data security rule that does not prescribe any such requirements.[224] Moreover, as advocated by small providers, we adopt a customer choice framework that distinguishes between sensitive and non-sensitive customer information, as well as decline to mandate a customer-facing dashboard to help manage their implementation and compliance costs. Furthermore, we find that our data breach notification requirements and "take-it-or-leave-it" prohibition do not require implementation extension for small providers as compliance with these protections should not be costly for small carriers that generally collect less customer information and use customer information for narrower purposes.

79. **Report to Congress:** The Commission will send a copy of the Order, including this FRFA, in a report to be sent to Congress pursuant to the Congressional Review Act.[225] In addition, the Commission will send a copy of the Order, including this FRFA, to the Chief Counsel for Advocacy of the SBA. A copy of the Order and FRFA (or summaries thereof) will also be published in the Federal Register.[226]

[219] *See id*.

[220] *See supra* Part III.I.2.

[221] *See supra* Part III.I.4.

[222] *See id.*

[223] *See supra* Appx. B, Part VI.B.

[224] *See supra* Part III.E.1.

[225] *See* 5 U.S.C. § 801(a)(1)(A).

[226] *See* 5 U.S.C. § 604(b).

**STATEMENT OF**
**CHAIRMAN TOM WHEELER**

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106.

Last week, I visited Consumer Reports' headquarters in Yonkers, New York, where I toured their product testing facility and met with senior leadership. When looking at a smart refrigerator that collects and shares data over the Internet, the discussion turned to privacy. Who would have ever imagined that what you have in your refrigerator would be information available to AT&T, Comcast, or whoever your network provider is?

The more our economy and our lives move online, the more information about us goes over our Internet Service Provider (ISP) – and the more consumers want to know how to protect their personal information in the digital age.

Today, the Commission takes a significant step to safeguard consumer privacy in this time of rapid technological change, as we adopt rules that will allow consumers to choose how their Internet Service Provider (ISP) uses and shares their personal data.

The bottom line is that it's your data. How it's used and shared should be your choice.

Over the past six months, we've engaged with consumer and public interest groups, fixed and mobile ISPs, advertisers, app and software developers, academics, other government actors including the FTC, and individual consumers, to figure out the best approach. Based on the extensive feedback we've received, we crafted today's rules to provide consumers increased choice, transparency and security online.

The time has also come to address the harmful impacts of mandatory arbitration requirements on consumers of communications services. To address this issue comprehensively, we have begun an internal process designed to produce a Notice of Proposed Rulemaking on this important topic by February 2017.

I want to thank the FTC and the Administration for leading the way with the FTC's privacy framework, and the Administration's Consumer Privacy Bill of Rights.

I'd like to acknowledge the companies who believe consumers care about privacy, and came to the table with constructive feedback.

To the consumer and public interest groups who have for years fought for consumer privacy protections in a digital age, thank you.

To our incredibly talented wireline bureau team lead by Matt DelNero and Lisa Hone, your hard work and dedication is inspiring.

And to the Chairman's Office team, led by Ruth Milkman and Stephanie Weiner. Thank you.

**STATEMENT OF**
**COMMISSIONER MIGNON L. CLYBURN**
**APPROVING IN PART AND CONCURRING IN PART**

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106.

Why has this Commission, received more than a quarter of a million filings, of which the vast majority show support for the adoption of strong privacy rules? Because consumers care deeply about their privacy—and so should we.

Ninety-one percent of Americans believe, consumers have lost control of how their personal information is collected, and used by companies. That's ninety-one percent. With news seemingly breaking every week, about a cyberattack, massive data breaches, and companies collecting and selling customer data to government agencies, that number should come as no surprise to anyone.

So when faced with the question, of should I support requiring companies to give consumers more notice, more choice, and more transparency, you hear no double speak from me. Simply put, additional consent here means, that consumers will have more of a say, in how their personal information is used—and I for one, think that is a good thing.

Today, we substantially adopt the FTC's framework on privacy, with some tweaks to account for the current era, and unique position broadband providers occupy in our everyday lives. Where we deviate, we do so with the protection of consumers in mind. This *Order,* I am proud to say, adopts strong privacy protections, and provides robust choice for those who consent to the use, or sharing of their information, as a means of receiving new products, more targeted advertising, or other innovative offerings made possible by big data.

I am grateful to the Chairman and Commissioner Rosenworcel, who agreed to many of my edits. In particular, this item incorporates my suggestions to account for people with disabilities and strengthens protections for protected classes under our national civil rights laws. It also toughens our pay-for-privacy safeguards, and improves the abilities of businesses to contract for their own privacy protections.

But what it does not do, is address the issue of mandatory arbitration, an issue I outlined in my remarks at the #Solutions2020 Forum last week. Mandatory arbitration, put simply, forces consumers with grievances against a company, out of the court system, and into a private dispute resolution system. In other words, their options are limited.

In an op-ed appearing in TIME earlier this week, Senator Franken and I described in detail, why mandatory arbitration is a consumer un-friendly practice.

For those who take exception, I must remind them that in this privacy proceeding, we did provide notice, we developed a record, and had an opportunity to give relief to millions of consumers nationwide, including the 99.9% of mobile wireless customers, who are forced to give up their day in court when they sign up for connectivity. In a rulemaking about transparent notice and choice to consumers for their privacy, I believe it is a natural fit to ensure transparent notice and choice, in the context of dispute resolution.

Public justice systems, discipline private conduct. But private justice systems are "an oxymoron," according to one appeals court judge, and he is not alone in that thought. The Consumer Financial Protection Bureau, has found that limiting forced arbitration clauses, have a powerful deterrent effect, resulting in companies changing business practices in more consumer-friendly ways. An inscrutable, unfairly levied below-the-line fee on a bill, may be disputed by a thousand consumers, but a provider can collect that fee from a million customers who may never notice that line item as they pay their monthly bill.

Without the watchful eye of the court system, a company can limit its losses to those thousand who do take notice, while keeping the proceeds from the millions who did not. And as one arbitrator put it, "why would an arbitrator cater to a person they will never see again," over a corporation who is repeatedly footing the bill?

Several agencies have stepped up and declared these provisions unlawful in other contexts, and yes, I am disappointed that we did not join this vanguard, in ensuring that consumers are not unwittingly giving up their day in court, when they sign up for communications services. And because of this, I respectfully concur in part. Nevertheless, I am heartened, Mr. Chairman, that we are committed to addressing this issue, in a separate proceeding, with a firm timeline.

To the Wireline Competition Bureau and Office of General Counsel staff, who have wrestled through these difficult issues for years, and somewhat frenetically over the past few days, I thank you. You have further empowered the American consumer through this item, and for that, and more, I am grateful.

**STATEMENT OF**
**COMMISSIONER JESSICA ROSENWORCEL**

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106.

To understand the future of privacy, I think it is important to begin by focusing on the forces shaping our new digital world. I see three.

First, we live in an era of always-on connectivity. Connection is no longer just convenient. It fuels every aspect of modern civic and commercial life. Sitting outside this connectivity is consigning yourself to the wrong side of the digital divide—and that has a cost because it hampers any shot at 21st century success.

Second, it used to be that the communications relationship was primarily between a customer and his or her carrier. But the number of third parties participating in our digital age connections and transactions has multiplied exponentially. Dial a call, write an e-mail, make a purchase, update a profile, peruse a news site, store photographs in the cloud, and you should assume that service providers, advertising networks, and companies specializing in analytics have access to your personal information. Lots of it. For a long time. Our digital footprints are no longer in sand; they are in wet cement.

Third, the monetization of data is big business. The cost of data storage has declined dramatically. The market incentives to keep our data and slice and dice it to inform commercial activity are enormous—and they are going to grow.

Today these forces collide for all of us in our lives lived online, where what we download, post, say and do says so much about who we are to the world.

But the truth is we are just getting started. Because the future will feature a whole new world of the Internet of Things, where the connectivity we have today will look quaint. Every piece of machinery, pallet of equipment, thermostat, smoke detector, street light, garbage pail, parking meter—you name it—will be a connected device. This creates powerful opportunities that will make us more effective and more efficient, our cities smarter and our communities more connected. But these benefits come with big security challenges. We had an object lesson in these challenges last weekend, with one of the largest Distributed Denial of Service attacks in history, with botnets taking control of insecure connected devices, and compromising them by flooding servers and sites with overwhelming traffic.

So when consumers survey this new digital landscape they wonder what privacy means. They do not want the digital age to decimate their fabled right to be left alone. They want privacy—but more importantly they want control. They want to control the whiplash from these new digital forces—and take some ownership of what is done with their personal information.

Today, the Commission provides consumers with the tools to do just that. We update—for the first time in nearly a decade—our privacy policies under Section 222 of the Communications Act. We establish new rules protecting the privacy of broadband customers. We adopt an opt-in regime for use and sharing of sensitive customer personal information and an opt-out regime for use and sharing of non-sensitive customer personal information. We put in place data security and breach notification policies so every consumer has confidence that efforts are in place to prevent harm from unlawful access to their data.

This is real privacy control for consumers. It helps in the here and now. But with respect to the future of privacy, I think we still have work to do.

Our domestic privacy policies largely rest on a foundation of old sector-specific laws. So continuing work to harmonize our privacy frameworks is hard—but deserves time and attention. To this end, the policies we adopt today are in many ways in sync with the approach taken by our colleagues at the Federal Trade Commission under Section 5 of the Federal Trade Commission Act. To the extent

they are not, let's face the facts—we are dealing with old laws, new technologies, and hard choices about existing regulatory schemes.

Privacy policy discussion, including ours here today, frequently focuses on three values—transparency, choice, and security. But I think it is time to introduce a fourth—simplicity. The forces at work in the digital world today are only going to make privacy more complex for all of us to control. But consumers should not have to be network engineers to understand who is collecting their data and they should not have to be lawyers to understand if their information is protected. So it is incumbent on every policymaker with privacy authority to think about how to make our policies more simple and more consistent. In fact, I think it is time for a 21st century inter-agency privacy council, where this Commission and our colleagues across government can do a better job of aligning privacy policies across the board. That won't be easy. But for the future of privacy, future of consumer control, and future of the digital economy—it will be worth the effort.

**DISSENTING STATEMENT OF COMMISSIONER AJIT PAI**

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106.

For the last two decades, the United States has embraced a technology-neutral framework for online privacy. Administered by the Federal Trade Commission, this framework applied across all sectors of the online ecosystem. It reflected the uniform expectation of privacy that consumers have when they go online. It didn't matter whether an edge provider or ISP obtained your data. And it certainly didn't matter whether, as a consumer, you understood what those regulatory classifications meant—let alone the technical and legal intricacies that dictate when a single online company is operating in its capacity as an edge provider as opposed to an ISP. Regardless of all of that, the FTC's unified approach meant that you could rest assured knowing that a single and robust regulatory approach protected your online data.[1]

That's why since the beginning of this proceeding, I have pushed for the Federal Communications Commission to parallel the FTC's framework as closely as possible. I agreed with my colleague that consumers have a "uniform expectation of privacy" and that the FCC thus "will not be regulating the edge providers differently" from ISPs.[2] I agreed that "consumers should not have to be network engineers to understand who is collecting their data and they should not have to be lawyers to determine if their information is protected."[3] I agreed that "harmonizing FCC policies with other federal authorities with responsibilities for privacy is a responsible course of action."[4] And I agreed with the FTC when it said that an approach that imposes unique rules on ISPs that do not apply to all online actors that collect and use consumer data is "not optimal."[5] These are the core principles that I have held throughout this proceeding.

I was disappointed—but not surprised—when FCC leadership circulated an *Order* that departed so dramatically from those principles. Over the past three weeks, my office diligently pursued a compromise framework that would have minimized the vast differences between the *Order*'s approach and the FTC's regime—one that would have protected consumer privacy while also allowing for more competition in the online advertising market, where edge providers are currently dominant.

For example, I asked my colleagues to acknowledge that persistent online identifiers (like static IP addresses) pose a larger privacy issue than more transitive identifiers. Distinguishing between the two in our de-identification standard would incentivize ISPs to compete with edge providers for online ads and do so through more privacy-protective technologies. Unfortunately, my colleagues were unwilling to compromise on this—or in any other meaningful respect.

[1] Indeed, the Obama Administration itself told the European Union that the FTC framework was strong and that nothing more, from a regulatory perspective, was needed to protect online consumers against predatory practices.

[2] Statement of Chairman Tom Wheeler, Hearing before the U.S. House of Representatives Subcommittee on Communications and Technology, "Oversight of the Federal Communications Commission," Preliminary Transcript at 141 (Nov. 17, 2015).

[3] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Notice of Proposed Rulemaking, 31 FCC Rcd 2500, 2637 (2016) (Statement of Commissioner Jessica Rosenworcel).

[4] Commissioner Jessica Rosenworcel Responses to Questions for the Record Submitted to the House Energy and Commerce Subcommittee on Communications and Technology's Hearing on "Oversight of the Federal Communications Commission" at 3 (July 12, 2016), *available at* http://bit.ly/2eOhvkg.

[5] Federal Trade Commission Bureau of Consumer Protection Staff Comments at 8.

That leaves us with rules that radically depart from the FTC framework. And that leaves us with rules that apply very different regulatory regimes based on the identity of the online actor. As my colleagues' earlier comments make clear, as the FTC has made plain, this makes no sense.

Now, today's *Order* tries to justify this new and complex approach by arguing that ISPs and edge providers see vastly different amounts of your online data. It recounts what it says is a vast sea of data that ISPs obtain. It then says that "By contrast, edge providers only see a slice of any given consumers Internet traffic."[6] A "slice." Really? The era of Big Data is here. The volume and extent of personal data that edge providers collect on a daily basis is staggering. But because the *Order* wants to treat ISPs differently from edge providers, it asserts that the latter only sees a "slice" of consumers' online data. This is not data-driven decision-making, but corporate favoritism.

The reality—something today's *Order* does not acknowledge—is that edge providers do not just see a slice of your online data. Consider what the Electronic Privacy Information Center told us:

> The FCC describes ISPs as the most significant component of online communications that poses the greatest threat to consumer privacy. This description is inconsistent with the reality of the online communications ecosystem. Internet users routinely shift from one ISP to another, as they move between home, office, mobile, and open WiFi services. However, all pathways lead to essentially one Internet search company and one social network company. Privacy rules for ISPs are important and necessary, but it is obvious that the more substantial threats for consumers are not the ISPs.[7]

Indeed, any review of the headlines rebuts the FCC's assertion that edge providers only see a fraction of your data. Consider these stories, almost all from just the past few weeks: "Google quietly updates privacy policy to drop ban on personally identifiable web tracking."[8] "Privacy Debate Flares With Report About Yahoo Scanning Emails."[9] "Apple keeps track of all the phone numbers you contact using iMessage."[10] "Twitter location data reveals users' homes, workplaces."[11] "Amnesty International rates Microsoft's Skype among worst in privacy."[12]

But due to the FCC's action today, those who have more insight into consumer behavior (edge providers) will be subject to more lenient regulation than those who have less insight (ISPs). This doesn't make sense. And when you get past the headlines, slogans, and self-congratulations, this is the reality that Americans should remember: Nothing in these rules will stop edge providers from harvesting and monetizing your data, whether it's the websites you visit or the YouTube videos you watch or the emails you send or the search terms you enter on any of your devices.

---

[6] *Order* at para. 30.

[7] EPIC Comments at 15.

[8] Anmol Sachdeva, Google quietly updates privacy policy to drop ban on personally identifiable web tracking, *The Tech Portal* (Oct. 21, 2016), *available at* http://bit.ly/2dIvcmY.

[9] Robert McMillan & Damian Paletta, Privacy Debate Flares With Report About Yahoo Scanning Emails, *Wall Street Journal* (Oct. 5, 2016), *available at* http://on.wsj.com/2dI7ovW.

[10] Oscar Raymundo, Apple keeps track of all the phone numbers you contact using iMessage, *MacWorld* (Sept. 28, 2016), *available at* http://bit.ly/2ev8QVi.

[11] Patrick Nelson, Twitter location data reveals users' homes, workplaces, *NetworkWorld* (May 18, 2016), *available at* http://bit.ly/1XmHAYf.

[12] Dennis Bednarz, Amnesty International rates Microsoft's Skype among worst in privacy, *WinBeta* (Oct. 23, 2016), *available at* http://bit.ly/2f8RnDv.

So if the FCC truly believes that these new rules are necessary to protect consumer privacy, then the government now must move forward to ensure uniform regulation of all companies in the Internet ecosystem at the new baseline the FCC has set.

That means the ball is now squarely in the FTC's court. The FTC could return us to a level playing field by changing its sensitivity-based approach to privacy to mirror the FCC's. No congressional action would be needed in order for the FTC to establish regulatory consistency and prevent consumer confusion.

Were it up to me, the FCC would have chosen a different path—one far less prescriptive and one consistent with two decades of privacy law and practice. The FCC should have restored the level playing field that once prevailed for all online actors using the FTC's framework. After all, as everyone acknowledges, consumers have a uniform expectation of privacy. They shouldn't have to be network engineers to understand who is collecting their data. And they shouldn't need law degrees to determine whether their information is protected.

But the agency has rejected that approach. Instead, it has adopted one-sided rules that will cement edge providers' dominance in the online advertising market and lead to consumer confusion about which online companies can and cannot use their data. I dissent.

**DISSENTING STATEMENT OF**
**COMMISSIONER MICHAEL O'RIELLY**

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106.

Today, the Commission attempts to solve a problem of its own making and, in the process, creates a host of new ones. Having reclassified broadband Internet access service as a telecommunications service, the FCC usurped part of the FTC's role in overseeing broadband privacy. Not content to inherit a system that, by almost all accounts, was working quite well to protect consumers, the FCC quickly embarked on an expansionist mission, seeking to impose situationally-defective new requirements that are stricter than most consumers would ever want or expect and that exceed the Commission's authority. Finding itself out of its depth, the FCC was forced to rein in some of the most extreme proposals and align itself better with the FTC framework. Landing in a less bad spot, however, should not be confused with setting sound policy. I must dissent for a number of reasons.

Beginning with legal authority, the Commission's attempt to fit broadband into section 222 is fundamentally flawed. The plain language of the statute speaks in terms of telephone service.[1] Accordingly, in its effort to shoehorn broadband into this regime, the Commission is forced to ignore or explain away language that clearly contradicts its position, regulate by analogy, or simply create new obligations out of thin air.[2]

To start, there is no independent authority in section 222(a) to regulate privacy or data security, regardless of the technology. As I have said before, the purpose of section 222(a) was to set forth the general parameters of *who* would be covered by the new rules contained in the other subsections. Before the 1996 Act, the rules only applied to AT&T, the BOCs, and GTE. Section 222(a) changed that by extending the general duty to protect proprietary information to *all* telecommunications carriers, while sections 222(b) and (c) detail *when and how* that duty is to be exercised. Specifically, section 222(b) protects other carriers from anti-competitive practices by requiring the confidentiality of carrier proprietary information, while section 222(c) protects the privacy expectations of consumers with respect to their call records by requiring the confidentiality of "customer proprietary network information", or CPNI. Given this three-part structure, it is not surprising that section 222(a) employs a term – proprietary information – that encompasses both the carrier proprietary information used in 222(b) as well as the CPNI used in section 222(c). It does not give the Commission license to ignore its own history and read section 222(a) and its terminology out of context.

Additionally, the use of "equipment manufacturers" in subsection (a) does not provide or authenticate any independent authority to act under the subsection, as the Commission tries to imagine in this item. Instead, it merely functions to cross reference overall concerns that some believed that equipment procurement by old-school Bell Operating Companies would lead to sharing of improper information from manufacturers. To the extent that concern existed, it was addressed directly in various places in section 273 with specific authority to act provided to the Commission in subsection (g) and, thus, it is inappropriate to read such authority into section 222(a).

[1] *See, e.g.,* CTIA Comments at 16-23; Comcast Comments at 67.

[2] Interestingly, when deciding that the section 222(e) exception for subscriber list information does not apply to broadband subscriber information, the order takes pains to examine the intent of Congress regarding the exception and analyzes the publishing technologies and information sharing practices that were in place at the time of enactment. In deciding that the rest of section 222 applies to broadband, however, the order breezes right past Congressional intent. Accordingly, section 222(e) is focused on "telephone books" or "direct equivalents" (no "functional equivalents" here) but somehow section 222(c) covers applications.

Commenters supplied additional reasons that refute the FCC's interpretation. They point out that the FCC's expansive interpretation of section 222(a) cannot stand because it would nullify other provisions of section 222.[3] And they show that Congress carefully crafted Section 222 to regulate CPNI and deliberately chose not to use the broader category of "personally identifiable information," or PII, unlike elsewhere in the Act.[4] These arguments further demonstrate that the order's interpretation of section 222(a) is not a permissible or reasonable one. Only a court intent on ignoring its obligations could not understand what the Commission is attempting to do here.

Since there is no independent authority in section 222(a), the categories of information that the FCC made up within section 222(a) – "customer proprietary information" and its subset "personally identifiable information" – are outside the scope of the provision. Yet even if the Commission attempted to ground its rules solely in section 222(c), which I do not concede applies to broadband either, it would still face significant legal problems. Many of the elements that the Commission wants to capture within its rules are not "customer proprietary network information".

First, proprietary information is "information that a person or entity owns to the exclusion of others," and thus it is not proprietary "if other individuals or entities can access the information and use it for their own commercial purposes."[5] That is why, in defining CPNI in section 222(h), Congress specified that it is limited to information that is made available to carriers "solely by virtue of the carrier-customer relationship."[6] Unlike traditional voice calls where the only parties that had access to call records were those already subject to section 222(c) – the local exchange carrier and in some instances the interexchange carrier – multiple parties that are unregulated by section 222 have access to an end user's online activities.[7] Indeed, "an ISP need not rely on its own relationship with its customers to collect information about their online activities because it could obtain the same information independently (at a price) from data brokers or other unregulated third parties."[8] Accordingly, this information would fall outside the scope of section 222(c).[9]

The order responds that proprietary information can't mean information kept secret from everyone else, because other personal information would not be protected by the CPNI rules. And it resorts to platitudes that adhering to the law as it is drafted would "undermine the privacy protective purpose of the statute." But those arguments misunderstand the limited purpose of section 222. It was never intended to cover all information about a person. It defines and protects a specific set of call record information, and until just recently, that has been the Commission's interpretation as well.[10] Far from

[3] *See, e.g.,* CTIA Comments at 27; AT&T Comments at 105-107; Verizon Comments at 57-58.

[4] Verizon Comments at 58-59 (citing Whitman v. American Trucking Ass'ns, Inc., 531 U.S. 457, 468 (2001); Dole Food Co. v. Patrickson, 538 U.S. 468, 476 (2003)).

[5] CTIA Comments at 34.

[6] 47 U.S.C. § 222(h).

[7] AT&T Comments at 101.

[8] *Id*. at 102.

[9] Even under the Commission's erroneous theory, to which I do not subscribe, that section 222(a) provides independent authority, this type of information would have to be excluded because section 222(a) likewise uses the term proprietary. Accordingly, section 222(a) also does not cover PII. Verizon also makes the point that, at most, section 222(a) requires "that carriers 'protect the confidentiality' of information; it does not govern permissible *uses* of information" and, therefore, "is far too thin a reed to authorize the entire regulatory apparatus the Commission proposes to erect for PII that is not CPNI." Verizon Comments at 59.

[10] *See, e.g.,* Verizon Comments at 56 ("The fact that the Commission has only now — after 18 years — claimed to discover new authority within Section 222 over all PII held by all telecommunications carriers, rather than only CPNI, belies that novel statutory interpretation. As the Supreme Court has cautioned, '[w]hen an agency claims to discover in a long-extant statute an unheralded power to regulate a significant portion of the American economy, we (continued….)

creating a gap, as the order claims, Congress made an intentional allocation of responsibility. Section 222 directs the Commission to protect a discrete category of information and, to the extent Congress is concerned about other types of information, it has enacted other laws covering them, and it can enact additional laws going forward. The FCC is not empowered to supplement its own authority, even if it believes it has policy reasons to do so.[11]

At times, the order runs circles around itself. For instance, the order takes the position that "proprietary information" covers "information that should not be exposed widely to the public." But when confronted with the fact that IP addresses are necessarily disclosed on the open Internet to make the service work, the order responds that "whether information is available to third parties does not affect whether it meets the statutory definition of CPNI."[12]

Second, section 222(c)(1) is limited to "individually identifiable" CPNI. Therefore, the order's inclusion of information that is reasonably linked or linkable to a person *or device* is impermissibly broad.[13] If a device "cannot be linked to a specific individual[,] . . . information that may be linked to the device would fall outside the scope of the statute and should not be subject to these rules."[14]

As a backstop, the order also lists a number of other provisions that provide absolutely no authority for these rules.[15] As I've said before, those provisions were never intended to regulate privacy or data security. In addition, by specifically enacting section 222, Congress made clear that the authority to regulate privacy is found in that provision. Any other reading would render section 222 superfluous.

While the FCC has no authority to adopt broadband privacy rules, I am compelled to comment on the serious deficiencies in the rules themselves in the event that somehow a court erroneously, irresponsibly and lawlessly finds that there is authority for them. In particular, the order fails to adequately justify the rules, including why it takes a different approach from the FTC in several key respects, leaving ISPs with substantially greater burdens than other Internet companies. The order falls back on the tired refrain that broadband providers are "gatekeepers" and that, in that role, they are able to see more information about their customers than edge providers. This ridiculous notion has been thoroughly debunked in the record.[16] The fact that consumers use multiple platforms to access the

(Continued from previous page)
typically greet its announcement with a measure of skepticism. We expect Congress to speak clearly if it wishes to assign to an agency decisions of vast economic and political significance.'") (citing Utility Air Regulatory Grp. v. EPA, 134 S. Ct. 2427, 2444 (2014) (citation and internal quotation marks omitted)).

[11] For example, the order now claims that a broad definition of protected information is required to better align FCC rules with the FTC approach. Putting aside for a moment the fact that the FCC does not actually line up with the FTC approach in several key respects, the FCC cannot exceed the limits of the authority delegated to it by Congress. As one commenter noted: "The law is clear that an agency cannot 'use its definitional authority to expand its own jurisdiction.'" Comcast Comments at 68 (citing Am. Bankers Ass'n v. SEC, 804 F.2d 739, 754-55 (D.C. Cir. 1986)).

[12] Of course, IP addresses do not qualify as CPNI in any event, as commenters have demonstrated. *See, e.g.,* Comcast Comments at 77-81.

[13] *See, e.g.,* AT&T Oct. 17, 2016 *Ex Parte* at 4.

[14] *Id*.

[15] *See also* AT&T Comments at 108-113; CTIA Comments at 59-73.

[16] *See, e.g.*, Peter Swire, Associate Director, The Institute for Information Security & Privacy at Georgia Tech, et al., Working Paper, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others* at 24-25 (filed May 27, 2016); EPIC Comments at 16 ("The FCC describes ISPs as the most significant component of online communications that poses the greatest threat to consumer privacy. This description is inconsistent with the reality of the online communications ecosystem. Internet users routinely shift from one ISP to another, as they move between home, office, mobile, and open WiFi services. However, all pathways lead to essentially one Internet search company and one social network company."); Comcast Comments at 26-34; Verizon Comments at 16-24.

Internet, coupled with the increasing prevalence of encryption, significantly undermines the order's claims that broadband providers have unique or unparalleled access to customers and their information. The Commission's lame attempt at discounting the traffic subject to encryption does a disservice to common sense and ignores the plain fact that consumer traffic from the most popular Internet sites is already encrypted with more to come. Accordingly, to the extent that the rules rely on the faulty gatekeeper proposition, the Commission should be overturned for that reason alone.

The FCC claims that, in moving to a sensitivity-based framework, the rules will be "more properly calibrated to customer and business expectations." But requiring opt-in notice for web browsing history and application usage data is a significant departure from the FTC approach, which is the basis for current expectations.[17] Under the FTC approach, those categories have not been treated as sensitive. While this approach has been in effect, there has been no evidence of any privacy harms, and businesses have been able to "provide great value to consumers in the form of discounts, convenient features, and other new and innovative services."[18] Requiring opt-in consent for these categories will destroy that value and upend years of settled expectations, burdening rather than benefitting most users.[19]

It will also create confusion. Consumers will receive notices from the broadband providers asking them to opt in. If they do not opt in, but continue to see advertisements based on their web browsing and application usage, some will understandably assume that their broadband providers are violating their privacy policies when, in fact, the ads originate from third parties not subject to FCC rules.[20]

It is also unnecessary. As commenters pointed out, to the extent that web browsing history and application usage data concerns sensitive information, such as health or financial records, it is already covered by the other categories that the FTC, and now the FCC, consider to be sensitive.[21] Commenters also submitted documentation into the record showing how broadband providers and other Internet companies currently differentiate and avoid the use of sensitive web browsing and application usage information under the current FTC framework.[22] Therefore, there is no reason to adopt an added layer of sensitivity that sweeps too broadly.

---

[17] *See, e.g.,* ITTA Oct. 21, 2016 *Ex Parte* at 2-3 (noting that "Web browsing and app usage history are not considered sensitive by the FTC" that "the FTC's Privacy Report endorsed an opt-out approach towards web browsing data used for behavioral advertising" and that "[a]gainst the backdrop of the longstanding, embedded commercial practice of consumers benefiting from targeted advertising based on web browsing history, consumers do not have the same expectations of privacy in this context as they do with other categories of information.").

[18] T-Mobile Oct. 14, 2016 *Ex Parte* at 2. *See also, e.g.,* Comcast Comments at 26-34; Verizon Comments at 17-24.

[19] *See, e.g.,* Comcast Comments at 44-52; T-Mobile Oct. 14, 2016 *Ex Parte* at 1-2.

[20] *See, e.g.,* Comcast Comments at 43; ITTA Oct. 21, 2016 *Ex Parte* at 3.

[21] Comcast Comments at 43.

[22] *See, e.g.,* Internet Commerce Coalition Oct. 18, 2016 *Ex Parte* at 2-3 (describing how ISPs and Internet companies use a combination of "white lists" and "black lists" that "isolate and exclude data categorized as sensitive by the FTC"); AT&T Oct. 17 *Ex Parte* at 3 ("Like any other Internet company, a broadband provider can avoid the use of sensitive information by categorizing website and app usage based on standard industry interest categories established by the Interactive Advertising Bureau ('IAB') and other leading industry associations. This process involves correlating non-content web address or app information (e.g., visit to a sports website) with a pre-established "white list" of permissible interest categories (e.g., sports lover) available from the IAB. The list of interest categories can be refined as needed to exclude any sensitive categories."); American Association of Advertising Agencies et. al Oct. 21, 2016 *Ex Parte* at 2 ("[C]ompanies across the Internet, including ISPs, have for decades used a combination of administrative and technical controls to limit the use of sensitive data for marketing and advertising purposes, absent consumer consent. These practices were developed to comply with the FTC's privacy framework and the self-regulatory program administered by the DAA."); Future of Privacy Forum Reply at

(continued….)

The order responds that it is better to be overinclusive because what is non-sensitive to most people could be sensitive to some. But, again, given that there has been no evidence of harm while this approach has been in effect at the FTC, there is no reason to re-draw the line in a way that will burden most consumers. That is not to say that privacy conscious consumers should have no remedy at all. Rather, they should be presented with clear notice of how their providers differentiate sensitive information and have the ability to opt out if they do not think methods are sufficient to protect them.[23]

The Commission must realize that an overly broad opt-in regime has significant consequences for consumers because "[i]t is well understood that an opt-in consent mechanism results in far fewer individuals conveying their consent than is the case under an opt-out consent mechanism" even when substantial benefits are at stake.[24] As one commenter noted: "In the marketing context, a rough rule of thumb is that opt-out consent mechanisms may yield approximately 82% or much higher of individuals preserving their consent, whereas an opt-in consent model may yield only approximately 18% or much lower of individuals consenting."[25] While the Commission anticipates that, in an opt-in regime, many consumers will wish to affirmatively exercise choice options, the "statistics on opt-in consent rates cited above show that this is not the case, and that many individuals will simply not pay attention to the choice or skip past it to get to the service."[26] This isn't consumer choice, it's recognition of consumer apathy.

Perhaps most troubling is that the order explicitly contemplates that it will apply to the Internet of Things. And, it makes this sweeping power grab without explaining how it has authority to do so. When I first cautioned that reclassifying broadband would lead to the FCC regulating edge providers and applications, some scoffed. Then it happened and now it is front and center again. Here, the FCC is refreshingly honest about its ambitions in this item, and I have every reason to expect that the Commission will make good on this vast new stake it has claimed. Those in the edge community should reconsider their belief that the FCC will never venture into their business models: The Commission is intentionally setting itself on a collision course with the FTC's definition with the intention to up the burdens on edge providers and all technology companies, either here or at the FTC.

The ultimate absurdity of these rules is that broadband providers remain free to purchase and use the information they need from those other Internet companies, including edge providers, because these other companies, not covered by the rules, will continue to operate under the FTC's opt-out regime. The rules prohibit a broadband provider from using sensitive "customer proprietary information" without opt-in consent, but "customer proprietary information" is limited to information that the provider "acquires in

(Continued from previous page)
8; Google Oct. 3, 2016 *Ex Parte* at 1; NCTA Oct. 20, 2016 *Ex Parte* at 3-5; INCOMPAS Oct. 21, 2016 *Ex Parte* at 3.

[23] ITIF Oct. 20, 2016 *Ex Parte* at 2.

[24] Comcast Comments at 48; Technology Policy Institute Oct. 17, 2016 *Ex Parte* at 2 ("All available research suggests that opt-in consent dramatically reduces participation. Any data classified under opt-in is less likely to be available to support services, innovation, and competition, as we and others discussed in previous filings.") (citing Tom Lenard and Scott Wallsten, Technology Policy Institute, *An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking* (May 2016); Avi Goldfarb, Catherine E. Tucker and Liad Wagman, *Comments on Notice of Proposed Rule Making: 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services'* (May 20, 2016)).

[25] Comcast Comments at 48 (citing Mindi Chahal, *Consumers less likely to 'opt in' to marketing than to 'opt out,' Marketing Week* (May 7, 2014), https://www.marketingweek.com/2014/05/07/consumers-less-likely-to-opt-in-to-marketing-than-to-opt-out/).

[26] *Id.* at 52.

connection with its provision of telecommunications service." Information obtained from an edge provider does not meet that definition.[27]

Therefore, all that the FCC has really done is raise the transaction costs. The FCC, in its typical nanny state fashion, seems to assume that consumers prefer an opt-in regime. But when consumers find out the end result is that they may have to pay more for heightened privacy rules that they never asked for, I doubt they will be grateful that the FCC intervened on their behalf. Indeed, this is a grandiose attempt to enact legacy talking points into rules so that Commission leadership can pat itself on the back while consumers receive no actual, practical protections. Added costs and burdens for providers? Yes. Benefits for consumers? No.

In another departure from the FTC framework and widespread consumer expectations, the order limits inferred consent to first party marketing within a service category, as well as the marketing of customer premises equipment (CPE) and "communications services commonly bundled together with the subscriber's telecommunications service." Here again, there is no rational reason to place undue restrictions on broadband providers.[28] While allowing providers to inform their customers about certain bundled offerings is a welcome change to the original, untenable draft, I would have extended inferred consent to the marketing of all products and services offered by broadband providers and affiliates as long as the affiliated relationship is clear to consumers.[29] Therefore, at a minimum, I would not require opt out consent to market new products and services that are "reasonably understood by customers as within the existing service relationship."[30] As the record demonstrated, consumers expect to receive information from their providers about new products, services, and discounts.[31] In addition, if broadband providers

[27] And even if the Commission "fixed" the definition, it would still be precluded by the statute from placing restrictions on a broadband provider's purchase or use of third-party data. *See, e.g.,* Comcast Comments at 75-76.

[28] *See, e.g.,* NCTA Oct. 20, 2016 *Ex Parte* at 8 ("The FCC has recognized that the statute permits carriers to use customer data to market products and services distinct from the underlying telecommunications service from which the data is collected. In interpreting the degree to which Section 222 accommodates first party marketing, the Commission stated that the relevant inquiry should focus on 'the customer's reasonable expectations of privacy in connection with CPNI.'") (citing *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, para. 41 (1999) (*1999 CPNI Order*)).

[29] *See* 2012 FTC Privacy Report at 41-42; Internet Commerce Coalition Oct. 18, 2016 *Ex Parte* at 4 (explaining that "first-party marketing of an ISP's other products and services should be permissible based on implied consent, as both the FTC and Administration have previously concluded"); NCTA Oct. 20, 2016 *Ex Parte* at 8 (noting that "both the FTC and White House privacy frameworks afford companies flexibility to use customer data to engage in first-party marketing and advertising of their own services based on implied consent") (citing 2012 FTC Privacy Report at 40 ("[M]ost first-party marketing practices are consistent with the consumer's relationship with the business and thus do not necessitate consumer choice"); The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, at 17 (2012) ("[C]ompanies may infer consent to use personal data to conduct marketing in the context of most first-party relationships, given the familiarity of this activity in digital and in person commerce, the visibility of this kind of marketing, the presence of an easily identifiable party to contact to provide feedback, and consumers' opportunity to end their relationship with a company if they are dissatisfied with it.")); ITTA Oct. 21, 2016 *Ex Parte* at 2-3.

[30] AT&T Oct. 17, 2016 *Ex Parte* at 2 (*1999 CPNI Order*, 14 FCC Rcd 14409, para. 42). *See also* NCTA Oct. 20, 2016 *Ex Parte* at 8; ITTA Oct. 21, 2016 *Ex Parte* at 2-3.

[31] *See, e.g.,* Cox Communications Inc. October 20, 2016 *Ex Parte* at 2 ("Regulatory authorities and experts recognize first-party marketing is a wide-spread practice and a well understood tool for establishing and maintaining . . . customer relationships. Both the FTC and the White House privacy frameworks specifically recognize this commonly accepted practice and permit companies to use customer data to communicate with their customers and personalize their customers' experience based on the customer's implied consent in most instances. Even existing FCC CPNI rules permit carriers to use CPNI to engage in some first-party marketing, without customer approval. Regulating such activities here would be unprecedented and would not reflect customers' current expectations of their broadband providers: to anticipate what they want and when they want it, to provide maximum value, and then

(continued….)

"cannot market new products and services on the same terms as online companies – or even other brick and mortar businesses – there will be less incentive to invest and develop new services."[32]

In addition, I was appalled to see a case-by-case approach imported to review mislabeled "pay for privacy" offers. These are consumer incentives offered every day in the real world and now ISPs will need to obtain a blessing from an agency that has no privacy experience.[33] The result is that broadband providers will be reluctant to extend, and may even forgo, valuable offers and discounts that consumers would want for fear that they will fall into another zero-rating style abyss. From that experience, we know that the game is perpetually on hold awaiting heavenly intervention, and some players have just stopped playing. Trying that again here in the privacy context does not make any sense, unless the real intention is to effectively ban pay for privacy offers without actually saying so in an attempt to avoid a legal challenge.

Moreover, I reject the Commission's effort to insert itself into mandatory arbitration clauses by committing to initiate a proceeding on the issue. As commenters explained in the record, mandatory arbitration clauses have benefitted both companies and consumers. In particular, "[m]ultiple studies have found that consumers obtain relief in arbitration at rates higher than they do in court, while being less costly and time-consuming for consumers than litigation."[34] I have heard the argument that eliminating these clauses will enable consumers to band together in class action lawsuits, but that is unrealistic. The fact-specific nature of many of the disputes that end up in arbitration – such as an incorrect bill – do not lend themselves to class certification.[35]

Any foray into mandatory arbitration clauses is unlikely to withstand legal challenge, so committing to initiate a proceeding is a complete waste of Commission resources. Under the Federal Arbitration Act (FAA), any "written provision in any . . . contract evidencing a transaction involving commerce to settle by arbitration a controversy thereafter arising out of such contract or transaction . . . shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract."[36] Supreme Court precedent has made clear that Congressional intent to override the FAA can only be demonstrated through a "contrary congressional command" that is "discernible from the text, history, or purposes of the statute" and it must be explicit.[37] Accordingly, "given the stringency of this test, the Supreme Court has never held that any federal statute overrides the

(Continued from previous page)
tell them about it.") (citations omitted); NCTA Oct. 20, 2016 *Ex Parte* at 7-8 (also noting that broadband providers are new entrants to many products and services offered by large edge providers).

[32] Cox Communications Inc. October 20, 2016 *Ex Parte* at 3.

[33] Technology Policy Institute Oct. 17, 2016 *Ex Parte* at 1 ("Requiring regulatory approval for new business models is likely to reduce experimentation, and reducing the number of potential methods of paying for service is likely to harm consumers."); Nokia Oct. 14, 2016 *Ex Parte* at 2 (describing the benefits of such offers).

[34] Verizon Oct. 21, 2016 *Ex Parte* at 2. *See also* CTIA Comments at 50-55.

[35] *See* CTIA Comments at 50 ("Most wrongs suffered by wireless consumers are relatively small and individualized, involving excess charges on a bill, a defective piece of equipment, or the like. These claims are simply too small to justify paying a lawyer to handle the matter and, in any event, most consumers do not have the resources to do so—and a lawyer is needed to navigate the complicated procedures that apply in court. And claims of this sort cannot be brought as class actions because they involve facts specific to an individual consumer's situation. . . . For this large category of consumer claims, arbitration provides the only realistic option for obtaining a fair resolution of the dispute.").

[36] Verizon Oct. 21, 2016 *Ex Parte* at 2 (citing 9 U.S.C. § 2).

[37] CTIA Comments at 56 (citing Shearson/Am. Express, Inc. v. McMahon, 482 U.S. 220, 226-227 (1987); CompuCredit Corp. v. Greenwood, 132 S. Ct. 665, 673 (2012)).

FAA."[38] And nothing in section 222 or the Communications Act generally meets that high hurdle.[39] In short, the Commission would be asking for another muni broadband style reversal.

Shifting to data security and data breach, I recognize that the Commission has significantly moved away from the irrationally strict and unworkable proposals in the NPRM by adopting a reasonableness standard for data security and a harm-based approach for data breach notifications. However, the Commission still lacks authority to adopt all of these rules, and I remain concerned that the Commission is not giving providers sufficient time to come into compliance.[40] Even the larger providers requested at least 12 months,[41] but the Commission does not even afford the smallest providers that much time. The training and auditing alone could take more time than what is given. If it is so important to act on data security and data breach notifications, then the Commission should at least ensure that it is done right rather than right now.

As a whole, this order places substantial, unjustified costs on businesses and consumers. Had the FCC conducted a cost-benefit analysis, which it committed to do but failed to live up to once again, it would have been unable to justify adopting these significant additional restrictions. Given that consumer privacy has been adequately protected under the current FTC framework and that there has been no evidence of any privacy harms, there is no benefit to be gained from increased regulation. On the other hand, there are substantial costs, including the increased transaction costs to purchase the information from unregulated Internet companies that will ultimately be passed on to consumers, the lost opportunity and revenues for broadband providers precluded from competing against Internet companies in the online advertising space, the foreclosure of innovative services that providers won't be able to offer and consumers won't receive, and the costs to consumers themselves who will be forced to participate in the opt-in regime and will pay more as a result.

While there are some statements about changes made to reduce compliance costs (i.e., one type of cost that is reviewed, in part, by the Office of Management and Budget), there is no overall analysis of the costs and benefits of this order. To the extent Commission leadership promised that rulemakings would serve as cost-benefit analyses, which I have explained is not adequate to comply with the relevant Executive Orders in any event, this order never engages in a serious discussion of the costs raised by commenters, failing to deliver even on that meager promise.

Finally, I want to point out that, despite my fundamental objections to this item based on the lack of statutory authority to adopt broadband privacy rules, I was willing to try to find common ground on specific issues, including the treatment of web browsing and app usage information, in order to mitigate the most harmful aspects of the order. My overtures were completely rebuffed by my colleagues. If anyone thinks that the only thing standing in the way of a more bipartisan Commission is an intransigent Commission minority, then this proceeding has proven, once again, that is absolutely incorrect.

---

[38] CTIA Comments at 56.

[39] *See, e.g.,* Verizon Comments at 74; CTIA Comments at 56-58.

[40] *See, e.g.,* WISPA Comments at 27-28 (seeking a two-year extension for all the Commission rules); ITTA Sept. 30, 2016 *Ex Parte* at 3 (same).

[41] *See, e.g.,* Verizon Sept. 23, 2016 *Ex Parte* at 1 ("Once rules are adopted, providers must go through an extensive and complex implementation process. Specifically, providers must perform an assessment of their existing processes and systems to determine what changes must be made; review, update, and negotiate supplier and other contracts; update written requirements documents; research, design, code, and test updates to customer care, self-serve, and back-office applications and systems; train employees and suppliers; draft customer communications; develop notice methods and periods; and set up a system for ensuring ongoing compliance. These actions will take a significant amount of time to complete, requiring approximately 18 months from the date rules are adopted.").