FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 64

[WC Docket No. 16–106; FCC 16–148]

Protecting the Privacy of Customers of Broadband and Other Telecommunications Services

AGENCY: Federal Communications Commission.

ACTION: Final rule.

SUMMARY: In this document, the Federal Communications Commission (Commission) adopts final rules based on public comments applying the privacy requirements of the Communications Act of 1934, as amended, to broadband Internet access service (BIAS) and other telecommunications services. In adopting these rules the Commission implements the statutory requirement that telecommunications carriers protect the confidentiality of customer proprietary information. The privacy framework in these rules focuses on transparency, choice, and data security, and provides heightened protection for sensitive customer information, consistent with customer expectations. The rules require carriers to provide privacy notices that clearly and accurately inform customers; obtain opt-in or opt-out customer approval to use and share sensitive or non-sensitive customer proprietary information, respectively; take reasonable measures to secure customer proprietary information; provide notification to customers, the Commission, and law enforcement in the event of data breaches that could result in harm; not condition provision of service on the surrender of privacy rights; and provide heightened notice and obtain affirmative consent when offering financial incentives in exchange for the right to use a customer's confidential information. The Commission also revises its current telecommunications privacy rules to harmonize today's privacy rules for all telecommunications carriers, and provides a tailored exemption from these rules for enterprise customers of telecommunications services other than BIAS.

DATES: Effective January 3, 2017, except for §§ 64.2003, 64.2004, 64.2006, and 64.2011(b) which contain information collection requirements that have not yet been approved by OMB. The Federal Communications Commission will publish a document in the **Federal Register** announcing the effective date of these rules upon approval. Section 64.2005 is effective March 2, 2017.

FOR FURTHER INFORMATION CONTACT: For further information about this proceeding, please contact Sherwin Siy, FCC Wireline Competition Bureau, Competition Policy Division, Room 5–C225, 445 12th St. SW., Washington, DC 20554, (202) 418–2783, *sherwin.siy@fcc.gov.* For additional information concerning the Paperwork Reduction Act information collection requirements contained in this document, send an email to *PRA@fcc.gov* or contact Nicole Ongele at (202) 418–2991.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Report and Order in WC Docket No. 16–106, FCC 16–148, adopted October 27, 2016 and released November 2, 2016. The full text of this document is available for public inspection during regular business hours in the FCC Reference Information Center, Portals II, 445 12th Street SW., Room CY–A257, Washington DC 20554. It is available on the Commission's Web site at *https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A1.pdf.* 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, *see* 5 U.S.C. 801(a)(1)(A).

Synopsis

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 Web sites 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 Notice of Proposed Rulemaking (*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). We include within the definition of 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); (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 Web sites, applications, and the functional equivalents thereof. Finally, consistent with FTC best practices and with the requirements in the CPBR, 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 of customer PI, and to easily adjust those choices over the course of time. Section 222 addresses the conditions under which carriers may ''use, disclose, or permit access to'' customer information. For simplicity throughout this document we sometimes use the terms ''disclose'' or ''share'' in place of ''disclose or permit access to.'' In adopting rules governing customer choice, we look to the best practices framework recommended by the FTC in its 2012 Privacy Report 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:

- *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. 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. Throughout the 1980s and 1990s, the Commission imposed limitations on incumbent telephone companies' use and sharing of customer information.

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. 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.''

22. 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 otherwise provided for by law. 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.

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. The current section 222 rules focus on transparency, choice, data security, and data breach notification.

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,'' 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. 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.

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.'' 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.''

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. 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.''

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. 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.

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. 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''—a position that we have referred to as a gatekeeper. As such, BIAS providers can collect ''an unprecedented breadth'' of electronic personal information.

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. As commenters have explained, ''customers who hop between ISPs on a daily basis often connect to the same networks routinely,'' and as such, over time, ''each ISP can see a substantial amount of that user's Internet traffic.''

30. While we recognize that there are other participants in the Internet ecosystem that can also see and collect consumer data, 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. 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 Web sites, and none of those have access to more than approximately 25 percent of Web pages. 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. In contrast, a BIAS provider sees 100 percent of a customer's unencrypted Internet traffic.

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 prominent third parties, ''but these tools do nothing to stop data collection on the wire.'' 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.

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.

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.''

33. We agree with commenters that point out that encryption can significantly help protect the privacy of consumer content from BIAS providers. 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 Web sites a customer has visited, how long and during what hours of the day the customer visited various Web sites, the customer's location, and what mobile device the customer used to access those Web sites. Moreover, research shows that encrypted web traffic 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.

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. We observe that several commenters rely on projections that 70 percent of Internet traffic will be encrypted by the end of 2016. 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. Moreover, ''raw packets make for a misleading metric.'' 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.'' What's more, research shows that approximately 84 percent of health Web sites, 86 percent of shopping Web sites, and 97 percent of news Web sites remain unencrypted. These types of Web sites generate less Internet traffic but contain ''much more personalized data.'' 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.

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 expect that their broadband service is being subsidized by advertising revenues as they do with other Internet ecosystem participants. 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.

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.' '' 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. Moreover, even if a customer was willing to switch to a new broadband provider, the record shows consumers often have limited options. 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. Given all of these factors, we conclude that, contrary to assertions in the record, 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.

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. We further find that when consumers are confident that their privacy is protected, they will be more likely to adopt and use broadband services. 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.'' The privacy framework we adopt today will bolster consumer trust in the broadband ecosystem, which is essential for business growth and innovation.

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 ''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. Although not limited to voice services, our existing rules have been focused on voice services. 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. 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. In accordance with these definitions, we continue to consider entities providing interconnected VoIP service to be telecommunications carriers for the purposes of these rules. 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. 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.* We define ''broadband Internet access service provider'' or ''BIAS provider'' to mean a person engaged in the provision of BIAS. 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. Under the *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.'' Moreover, consistent with the *2015 Open Internet Order,* 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, Web sites, cloud storage services, social media sites, music streaming services, and video streaming services (to name a few).

2. The Rules Protect Customers' Confidential Information

41. Section 222 governs how telecommunications carriers treat the ''proprietary'' and ''proprietary network'' information of their ''customers.'' 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. 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.

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. We are, however, persuaded by commenters that argue that the existing rule's limitation to current subscribers is too narrow. As data storage costs decrease and computing power increases, previous barriers to data analysis based on cost, time, or feasibility are receding. 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. 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. These outcomes would run counter to our firm commitment to promote broadband adoption, competition, and innovation. 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.''

43. We disagree with commenters that assert that including prospective and former customers within the definition of customer could unduly burden providers. 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 share one account. 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. 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.

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.

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 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; as well as information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier, but does not include subscriber list information. 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.

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. 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. 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. 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.

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.'' 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. 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. We agree with 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.

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. 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.''

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.

52. We do not believe it is necessary to categorize all personally identifiable information (PII) as CPNI, as suggested by Public Knowledge. 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.

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

53. In keeping with the Commission's past practice, 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. 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 and market user data.'' 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. 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. 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, enabling rapid innovation in Internet-based protocols and applications. Within one device, information is typically transmitted vertically through the various layers. Across all devices, equivalent layers perform the equivalent functions. This compatibility and interoperability is typically represented as horizontal relationships. 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.'' 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. As a component of their provision of service, BIAS providers may analyze each of these layers for reasonable network management.

57. Common representations of the Internet's architecture range from four to seven layers. 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. 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 Web page, 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 Web page constitutes application header information. In a conversation via email, instant message, or video chat, an application header may disclose the parties to the conversation.

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. 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. 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.

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. 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.

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. 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.

(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. 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.'' 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. We agree with NTCA that ''information related to a customer's broadband service plan can be viewed as analogous to voice telephony service plans,'' which the Commission has long considered to be CPNI in the voice context. 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 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, and Congress emphasized the importance of geo-location data by adding Section 222(f).

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. 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. 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. Link layer protocol headers convey MAC addresses, along with other link layer protocol information. 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). 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. 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. For the same reasons, we conclude that other device identifiers and other information in link layer protocol headers are CPNI in the broadband context because they relate to the technical configuration and destination of use of a telecommunications service.

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. An IP address is a routable address for each device on an IP network, and BIAS providers use the end user's and edge provider's IP addresses to route data traffic between them. As such, source and destination IP addresses are roughly analogous to telephone numbers in the voice telephony context. The Commission has previously held telephone numbers dialed to be CPNI. Further, our CPNI rules for TRS providers recognize IP addresses as call data information. By this analogy, we mean only that both are ''roughly similar numerical identifiers'' used to route telecommunications. We do not intend to imply that IP addresses are or should be administered in the same manner as telephone numbers. This definitional change to our regulations in no way asserts Commission jurisdiction over the assignment or management of IP addressing.

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. IP addresses are also frequently used in geo-location. 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. As Public Knowledge explains, ''IP addresses can easily be mapped to geographic locations, meaning that both the subscriber and the service can be located.'' 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.

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 IP address to the customer, and thus it is not ''made available to the carrier by the customer solely by virtue of the carrier-customer relationship.'' 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. 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.'' However, as discussed above, whether information is available to third parties does not affect whether it meets the statutory definition of CPNI.

71. We also disagree with commenters who assert that dynamic IP addresses do not meet the statutory definition of CPNI. A dynamic IP address is one that the BIAS provider can change. 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.'' A dynamic IP address may be used for a shorter period of time than a static IP address. 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). 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 customer uses to identify the end point to which they seek to connect. 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. 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. 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. As such, other information in the network layer protocol headers relates to the technical configuration and amount of use of a telecommunications service.

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. 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). 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. 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. 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. A port is a logical endpoint of communication with the sender or receiver's application, and consequently relates to the ''destination'' of a communication. The transport layer protocol header of a data packet contains the destination port number, which determines which application receives the communication. Port destinations are analogous to telephone extensions in the voice context. 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. Though sometimes port numbers may not reveal anything of significance, they often do, and therefore we conclude that they relate to the destination, type, or technical configuration of the service. 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. 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.

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. 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. Application headers contain data for application-specific protocols to help request and convey application-specific content. 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.''). The application header communicates information between the application on the end user's device and the corresponding application at the other endpoint of the communication. 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. 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. 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. 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 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. BIAS providers sometimes append information to application headers, in particular HTTP headers, in order to uniquely tag communications with a specific subscriber account. 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. 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. 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 provider directs the collection or storage of such information, we conclude that it is CPNI. 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.

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. Examples of application payloads include the body of a Web page, 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. BIAS providers also use various network management techniques to minimize network congestion while transmitting application payloads. 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 Web site), 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.

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. The Act defines CPE as ''equipment employed on the premises of a person (other than a carrier) to originate, route, or terminate telecommunications.'' The Commission has long-understood CPE to include customers' mobile devices, such as cell phones. 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.'' We disagree with commenters that argue that only devices furnished by the BIAS provider can qualify as CPE; 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 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. As discussed above, 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. 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[.]'' 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.'' ''[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. 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. This interpretation of section 222(a) is consistent with other provisions of the Communications Act that use the term ''proprietary information,'' and with the Commission's use of that term before enactment of Section 222. As we discuss in more detail below, protecting PII and content is at the heart of most privacy regimes 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.''

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. 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.'' 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. 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. 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.

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 information. 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.* According to FTC staff, ''[t]o date, the FTC has brought over 500 cases protecting the privacy and security of consumer information.'' We have held providers responsible for protecting these private data under section 222(a). In *TerraCom,* we also found that the failure to protect customer's private information was an unjust and unreasonable practice under section 201(b). Likewise, providers have been required to protect the content of communications for decades. Moreover, customers reasonably expect and want their providers to keep these data secure and confidential. 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.'' 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.'' We also observe that omitting PII from the scope of these rules would result in a gap in protection for PII under the Act's primary privacy regime for telecommunications services. 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. 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. 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.

89. We define personally identifiable information, or PII, as any information that is linked or reasonably linkable to an individual or device. 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. 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. In addition to NIST, CPBR, and the FTC, the Department of Education, the Securities and Exchange 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.

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.'' While we recognize that '' '[i]dentifiable' information is increasingly contextual''—especially when a provider can cross-reference multiple types and sources of information—anchoring the standard to a mere ''possibility of logical association'' could result in ''an overly-expansive definition.'' 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. This conclusion has broad support in the record.

91. We also adopt the FTC staff recommendation that PII should include information that is linked or reasonably linkable to a customer device. 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. 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.'' 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. While some commenters argue that we should not include information linkable to a device in the definition of PII, we find that such identifiers are often and easily linkable to an individual, as we discussed above.

92. We disagree with commenters that argue that PII should only include information that is sensitive or capable of causing harm if disclosed. 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. We address the treatment of sensitive versus non-sensitive information below.

93. We agree with commenters that we should offer illustrative, non-exhaustive examples of PII. We have analyzed descriptions of PII in the record, our prior orders, NIST, the FTC, the Administration's proposed CPBR, and other federal and state statutes and regulations. 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; 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. OTI asks us to clarify the meaning of ''other online contact information.'' The term is meant to be technology neutral and encompass other methods of BIAS-enabled direct messaging.

94. We disagree with commenters that argue that we should not consider MAC addresses, IP addresses, or device identifiers to be PII. First, as discussed above, a customer's IP address and 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. In many cases, a unique numerical identifier will be *more* specific than the person's actual name. 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). 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. 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.''

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. 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.'' Through this definition, Congress recognized that a dispositive factor is whether the information has been published or accepted for publication in a directory format.

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. 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.'' 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.'' 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 Web site 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. Nor does the record reflect more than speculation about any future interest in publishing directories. 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. 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. As such, we disagree with commenters who ask us to ignore the publication requirement in order to exempt names, addresses, telephone numbers, and IP addresses from these rules.

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. 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. As PII, this information is subject to our customer choice rules, discussed in detail below. 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.

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. 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.'' Content is highly individualistic, private, and sensitive. 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. 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. We agree with FTC staff that ''[c]ontent data can be highly personalized and granular, allowing analyses that would not be possible with less rich data sets.'' 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. 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.'' 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. 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. 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. 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.

103. Multiple components of an IP data packet may constitute or contain BIAS content. First and foremost, we agree with commenters that the application payload is always content. As discussed above, 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. Examples of application payloads include the body of a Web page, 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. 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. However, other portions of the packet also may contain content. 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 Web site URLs. Application usage information may also reveal content by disclosing the applications customers use or the substance of how they use them. 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[.]'' 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, and the Electronic Communications Privacy Act (ECPA) or the Communications Assistance for Law Enforcement Act (CALEA), already protect content. 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 content carried by telecommunications carriers. Given the importance of protecting content, it is reasonable to interpret section 222 as creating additional, complementary protection. 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.

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. 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.'' 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. The Administration's CPBR also uses this standard. 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. 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 (*e.g.,* ''We offer great coverage in rural areas, because that is where 70% of our customers live.'') We apply these requirements to both BIAS and other telecommunications services. 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[.]''

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. 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.'' 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.'' 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.''

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, 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. 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.

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. 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. 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, 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. 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). 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. 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. New methods are increasingly capable of re-identifying information previously thought to be sufficiently anonymized. For these reasons, we will not specify an exhaustive list of identifiers, nor will we declare certain techniques to be *per se* sufficient or insufficient to achieve de-identification. 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.''

112. We make clear that reasonableness depends on ease of *re-*identification, not the cost of *de-*identification. 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. 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. 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.''

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. Cross-referencing the datasets links the de-identified information with an identified customer, thus rendering the de-identified information linked or reasonably linkable. We agree with Verizon that ''providers should not be allowed to use de-identification and re-identification to circumvent consumers' privacy choices.''

114. We disagree with commenters who argue that the linkability standard should apply only to individuals and should not extend to devices. 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.'' This is not an uncommon conclusion in the Internet 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.''

115. Similarly, for the reasons discussed above, 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.'' 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. NCTA expresses concern that finding that IP addresses can constitute PII will undermine judicial precedent under the Video Privacy Protection Act. 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.'' 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.

(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.'' As we discussed above, this level of transparency is a cornerstone of privacy best practices generally and these rules specifically. As such, we disagree with commenters who argue that such public commitments are unnecessary. This part of the test is consistent with FTC guidance—which has broad support in the record—and the CPBR. We agree that ''[c]ompanies that can demonstrate that they live up to their privacy commitments have powerful means of maintaining and strengthening consumer trust.'' 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.

(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. 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.

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 . . . .'' The record demonstrates that such contractual prohibitions are an important part of protecting consumer privacy because re-identification science is rapidly evolving. 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.'' It is our expectation that carriers will need to monitor their contracts to maintain the carriers' continued adherence to these requirements. Consequently, we need not adopt a separate part of the test to delineate monitoring requirements. 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 violations occur, we expect carriers to take steps to protect the confidentiality of customer's proprietary information.

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. 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. Professor Narayanan concurs, noting that when statistical data is highly abstract, there is minimal risk of re-identification. 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. As explained below, we find that certain uses and disclosures of customer PI for the purpose of conducting research to improve and protect 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. 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.

(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. 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. 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.'' As Professor Ohm has stated, the FTC guidance on which we pattern our standard is ''a very aggressive and appropriately strong form of de-identification'' 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.

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), and it is an essential component of many privacy laws and regulations, including the Satellite and Cable Privacy Acts. Customer notification is also among the least intrusive and most effective measures at our disposal for giving consumers tools to make informed privacy decisions. 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. 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 with BIAS providers' existing requirement to disclose their privacy policy under the 2010 and 2015 *Open Internet Orders.* For today's rules, we look to the record in this proceeding, which includes submissions from providers, consumer advocates, other government agencies, and others about what does and does not work with respect to privacy policies. 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. 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. Moreover, the record reflects that many BIAS providers and other telecommunications carriers already provide thorough notice of their privacy practices. 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. However, none of these criticisms eliminates the fundamental need for and benefit of privacy notices. 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 Administration Big Data Report explains, notice and choice structures may not be sufficient to account for all privacy effects of ''big data,'' 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. We will consider information to be misleading if it includes material misrepresentations or omissions. 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 Web sites, 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.

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. We also agree with the FTC that disclosing this information ''provides an important accountability function,'' as disclosure of this information ''constitute[s] public commitments regarding companies' data practices.'' To enable customers to exercise informed choice, and to reduce the potential for confusion, misunderstanding, and carrier abuse, 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. Pursuant to the voice rules and the *2010 Open Internet Order,* all BIAS providers already provide customers with information about their privacy policies. As such, we find that this requirement will not impose a significant burden on providers, and in some cases will decrease existing burdens.

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

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. 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, 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. The FTC's rules further specify that institutions should provide examples of businesses in those categories. 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. 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. We therefore reject calls to mandate disclosure of a list of the specific entities that receive customer PI. 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, in turn, would be inconvenienced with an overabundance of notices. 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. 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.

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.

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 customers to make informed decisions. 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] Web page where subjects choose whether to reveal their information eliminates the privacy-protective effect of the notice.'' As discussed further below, 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 Web site, 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 Web site, in a provider's app, or in a paper disclosure presented in a provider's store).

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. 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. As noted below, this provision does not mean that carriers categorically cannot engage in financial incentive practices. 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.'' 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. 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. NTCA recommends that we remove or modify from the *NPRM*'s proposal the requirement that the explanation be brief. In the interest of allowing more 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.'' 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. 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.

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. 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' Web sites 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, 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. 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. The point-of-sale requirement is also consistent with the transparency requirements of the *2010 Open Internet Order,* which requires disclosure of privacy policies at the point of sale. 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. 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.

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 Web site, 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.

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. 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 . . . Web site,'' 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. 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 Web site, 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 a clear and conspicuous location on its homepage, to ensure that customers who visit the homepage may easily find it.

141. We require the notice of privacy policies to be clearly and conspicuously present not only on the provider's Web site, 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 Web site 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 Web site interface, giving customers tools to manage their accounts with their providers. 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. 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. Nor do we require providers who lack an app to develop one. 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 Web site, to ensure that those apps provide at least a link to a viewable notice of privacy policies.

142. Providing the notice both via the app and on the provider's Web site 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 Web site or app that may be developed. While we anticipate that all BIAS providers and most other telecommunications providers have a Web site, 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, 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' Web sites, and notices of material change to privacy policies, is sufficient to keep customers informed. Additionally, we believe that periodic notices might distract from notices of material changes, reducing the amount of customer attention to such changes. 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.

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. This concern is especially prevalent for smaller carriers. 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. 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. 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. 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. We note that as standard business practices for conveying complex information improve, we expect notices of providers' privacy policies to keep pace. 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. As such, as described below, 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.'' 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. 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.

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.'' 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.

149. We agree with the FTC's observation that existing notices of privacy policies are frequently too long and unclear; overlong notices are often inherently less comprehensible. As T-Mobile states, ''today's busy consumers often have limited ability to fully review the hundreds of privacy policies that apply to the apps, Web sites, and services they use, and prefer simpler notices that provide meaningful information.'' We recognize that providers must balance conveying the required information in a comprehensive and comprehensible manner, 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.

150. The record also reflects that transparency is only effective in preventing deception when the information shared is meaningful to the recipient. 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. This requirement is also consistent with FTC precedent.

151. *Other Languages.* We agree with the FTC that providers should convey notices to their customers in a language that the customers can understand. 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. This requirement ensures that customers who are advertised to in a particular language may also understand their privacy rights in that same language. 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. 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.

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. So long as 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, 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. 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. 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.

154. The CAC has significant expertise in developing standard broadband disclosures and other consumer disclosure issues. 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.

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. As with our requirements for the notice of privacy policy, if a carrier does not have a Web site, it may provide notices of material change notices to customers in paper form or some other format agreed upon by the customer. 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. 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. This requirement to notify customers of material change finds strong support in the record.

157. The record reflects strong justifications for requiring providers to give customers advance notice of material changes to their privacy policies. 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. 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,'' which includes privacy policies. 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; to the extent 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.* 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. 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 Web site 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. 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 Web site, and providers may not have a customer's email address. 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. Some commenters have expressed concern that requiring carriers to send multiple notices in different formats for each material change would present ''significant logistical challenges.'' The rules do not require multiple formats for 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. 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. Given these existing obligations, we disagree with commenters who suggest that providing more than one notice is overly burdensome.

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. 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.

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. 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). 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. 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 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) services within this category to operate under a more uniform set of privacy rules, reducing potential compliance costs. 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. 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' Web sites, an already common practice, we eliminate the requirement that notices of privacy practices be re-sent to customers every 2 years. 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'' —a requirement that has apparently been interpreted as requiring that language to appear verbatim in privacy policies. 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 of their personal information, and to easily adjust those choices over the course of time. Respecting the choice of the individual is central to any privacy regime, and a fundamental component of FIPPs. 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. 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.

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, and to decrease compliance burdens for all affected telecommunications carriers, particularly small providers. 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. We also require carriers to obtain customer opt-in consent for material retroactive uses of customer PI, as discussed below. 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.* Having sought comment on a sensitivity-based framework in the *NPRM,* 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 used by the FTC in its settlements. 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.

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. 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. 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. Some commenters argue that carriers can use a system of whitelists to determine sensitive versus non-sensitive Web sites. 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 precedent and numerous other privacy statutes and regimes. 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.

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, financial information, precise geo-location information, children's information, and Social Security numbers. The FTC explicitly regards these categories of information as sensitive, as well. Despite some commenters' assertions to the contrary, the FTC does not claim to define the outer bounds of sensitive information with this list. 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. 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. 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. Each of these categories has a clear and well attested case in the record and in federal law for being considered sensitive.

179. Consistent with the FTC and the record, we conclude that precise geo-location information is sensitive customer PI. Congress specifically amended section 222 to protect the privacy of wireless location information as the privacy impacts of it became clear. 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.'' In some cases, a BIAS provider can even pinpoint in which part of a store a customer is browsing. 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.'' 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.

180. The record also reflects the historical and widely-held tenet that the content of communications is particularly sensitive. 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. This finding is strongly supported by the record, and consistent with FTC guidance. As the FTC explains, ''content data can be highly personalized and granular, allowing analyses that would not be possible with less rich data sets.'' We therefore concur with the large number of commenters who assert that content must be protected 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.'' As such, we consider communications contents to be sensitive information. 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.

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 usage history frequently reveal the contents of her communications, but also constitute sensitive information on their own—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. We therefore decline to define a subset of non-sensitive web browsing and application usage history, as a number of commenters urge. 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. 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.

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. The notion is that before a BIAS provider tracks the Web sites 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.'' For instance, a user's browsing history can provide a record of her reading habits—well-established as sensitive information—as well as information about her video viewing habits, or who she communicates with via email, instant messaging, social media, and video and voice tools. The cable and satellite privacy provisions of the Act were created in significant part to protect the privacy of video viewing habits. Video rental records have also been recognized by Congress as worthy of particular privacy protection. As such, we disagree with Google's assertions that web browsing has not traditionally been considered sensitive information. 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 Web site. 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. 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. 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. The wealth of information revealed by a customer's browsing history indicates that it, even apart from communications content, deserves the fullest privacy protection.

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

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. 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. 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 Web site 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. 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 Web site; it could also, unlike the store, associate that information with the customer's other communications. 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. 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), 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.

186. Also, contrary to some commenters' arguments, the existence of encryption on Web sites or even in apps does not remove browsing history from the scope of sensitive information. As noted above, encryption is far from fully deployed; the volume of encrypted data does not represent a meaningful measure or privacy protection; 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. Comcast notes that few dispute on the record that a growing volume of traffic is encrypted. 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. Comcast argues that because BIAS providers are limited to this information, they have less access to information overall. 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. 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. 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.

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. Although commenters cite various industry attempts to categorize consumer interests, and identify the sensitive categories among those, the definitions vary significantly between them. 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. 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. 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 Web pages you visit, so we can tailor ads and offers to your interests.'' 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.'' 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. 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.

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.'' 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. 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. We do not adopt the CFAA's definitions of ''damage'' or ''loss'' for the purposes of this Order.

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, biometric identifiers, and electronic signatures. 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. 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, and as customer expectations or the public interest may require us to refine the categories of sensitive customer PI, we will do so. For instance, some commenters have suggested that information considered non-sensitive at one point might reveal through later analysis information about protected classes.

(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.'' 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, 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. 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. 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. For instance, the FTC recognizes that consumer expectations drive increased protections for sensitive information. 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, 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. 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.

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 will remain in the default position, even if they would not have actively chosen it. Further, opt-in regimes provide additional incentives for a company to invest in making notices clear, conspicuous, comprehensible, and direct. 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. 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. The record demonstrates widespread conviction

that material retroactive changes to privacy policies should require opt-in approval from customers. 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 prominent disclosures and obtain affirmative express consent before using data in a manner materially different than claimed at the time of collection.'' 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. Empowering consumers by providing choice is a standard component of privacy frameworks. 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. 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.

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. 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. 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 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. 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,'' 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.'' 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. 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. 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.' '' Thus, we reject arguments that ''opt-out is not an appropriate mechanism to obtain user approval'' in any circumstances.

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. 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 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. Our conclusion is also consistent with Commission precedent and FTC Staff comments. 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. While some comments assert that customers expect some degree of targeted marketing absent explicit customer approval, the record also indicates that customers expect choice with regard to the privacy of their online communications. 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.'' 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 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. Consumers have registered over 222 million phone numbers with the Do Not Call Registry in order to stop unwanted marketing calls. 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, with businesses required to place the consumer on a do-not-call list upon the consumer's request. The CAN SPAM Act of 2003, 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. 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. 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. We disagree with commenters who argue that extending these limitations and exceptions to approval requirements unduly risk customers' privacy. We make clear that carriers using 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).

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. Consent to use customer PI for the provision of service is implied in the service relationship. 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. 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. 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. 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). 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). However, we provide guidance 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.

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. 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. 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. 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.

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. 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 protocol conversion, and we continue to do so today. 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. 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. 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. Customers require working inside wiring to receive service, and often depend upon technical support to fully utilize their services. As such, carriers may use and share non-sensitive customer PI, without additional customer approval, to provide and market such services.

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. 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. 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. 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. 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.'' 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 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. We recognize that reasonable network management plays an 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. 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 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. 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. 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.'' 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.'' NCTA also argues that carriers must be able to use customer data for internal operational purposes such as improving network performance. Some commenters, such as CDT, caution that a research exemption, read too broadly, might permit privacy violations. 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. Telecommunications carriers and researchers should design research projects that incorporate principles of privacy-by-design, and agree not to publish or otherwise publicly share individually identifiable data without customer consent. This would include, for instance, practicing data minimization and not using more identifiable information than necessary for the research task. 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. 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.'' 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.

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. We agree with the broad set of commenters who expressed the opinion that this exception should be incorporated into the rules, and further agree that it should also apply to customer PI beyond CPNI. 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.'' 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 to protect against spam, malware such as viruses, and other harmful traffic, including fraudulent, abusive, or otherwise unlawful robocalls. As proposed, this includes any form of customer PI, not merely calling party phone numbers. 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. 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, 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. When combined with the immunity granted by CISA, this exception addresses carriers' concerns about participating in cybersecurity sharing initiatives. As noted above, CISA permits the sharing of cybersecurity threat indicators ''notwithstanding any other provision of law.'' 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. 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. 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. 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. 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.

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 emergency assistance through means other than dialing 9–1–1 on a voice line. 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, 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. 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. 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.

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. This allows carriers to supply customers with relevant information at the most relevant time and in the most relevant context. 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.

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. 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 Web site, an email address that will receive the customer's choice, or a toll-free number that a customer can call to make his choice.

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 (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.

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 Web site; on the carrier's app, if it provides one for account management purposes; and on any functional equivalents of either. We intend for this requirement to mirror the requirements for a provider's provision of its notice of privacy policies. If a carrier lacks a Web site, 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. 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.'' ACA adds that creating a privacy dashboard would be a ''near-impossible task'' for small BIAS providers. 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.'' Aside from the ordinary time that might be required for 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. 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. The Commission has long held this interpretation to be consistent with the language and design of section 222.

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. 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 Web sites 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' Web sites. 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 Web site or app may be able to accept customer preferences by providing on their Web sites, 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. 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.

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. 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.

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, the NIST Cybersecurity Framework (NIST CSF), the Satellite and Cable Privacy Acts, and the CPBR, and finds broad support in the record. 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 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.

239. As we observed in the *NPRM,* privacy and security are inextricably linked. Section 222(a) imposes a duty on telecommunications carriers to ''protect the confidentiality of proprietary information of and relating to . . . customers.'' Fulfilling this duty requires a provider to have sound data security practices. 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,'' three dynamic and interrelated principles typically referred to together as the ''CIA'' triad. Confidentiality refers specifically in this context to protecting data from unauthorized access and disclosure; integrity refers to protecting information from unauthorized modification or destruction; and availability refers to providing authorized users with access to the information when needed. 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. We 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.'' The record confirms that these are core principles that underlie the modern-day practice of data security. 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. 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, and in numerous cases the FTC has taken enforcement action against companies for failure to take ''reasonable and appropriate'' steps to secure customer data. Many states also have laws that require regulated entities to take ''reasonable measures'' to protect the personal data they collect. The CPBR reaffirms this standard, directing companies to ''establish, implement and maintain safeguards reasonably designed to ensure the security of'' personal customer information. Placing the responsibility on companies to develop and manage their own security practices is also a core tenet of the NIST CSF. A diverse range of commenters in this proceeding support adoption of a data security requirement for BIAS providers that is consistent with these principles. Indeed, several providers acknowledge the importance of and need for reasonable data security.

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. 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.'' We agree with these parties, and others such as the Federal Trade Commission staff, 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. 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. 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 relating to the small subscriber bases of [rural carriers].'' Several small provider commenters also point out that many such providers have few employees and limited resources. 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. Our decision not to adopt minimum required security practices should further allay concerns about the impact of the rule on small providers. 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. 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.

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, our data security rule must cover both. 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. We believe the modifications we have made to the proposal, including our decision not to adopt minimum required security practices, sufficiently address this concern. At the same time, we decline to require ''the same, strict data security protections'' for all such information. Rather, we direct providers to calibrate their security measures to ''the sensitivity of the underlying data.'' This approach finds broad support in the record and is consistent with FTC guidance and precedent. Where sensitive and non-sensitive customer PI are commingled, a carrier should err on the side of treating the information as sensitive. Similarly, our inclusion of ''technical feasibility'' as a factor makes clear that reasonable data security practices must evolve as technology advances. 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. 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. 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. 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. 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. Moreover, in *TerraCom* and other data security enforcement proceedings, parties have agreed to detailed data security obligations on individual carriers as conditions of settlement. For example, as part of one consent decree entered into 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. 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. The Commission values the NIST CSF and has demonstrated its commitment to promoting its adoption across the communications sector, 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. 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. 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). 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 backdrop of existing privacy and data security laws, best practices, and public-private initiatives. 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, 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. 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. For example, National Consumers League recommends adoption of multi-factor authentication as a required ''minimum baseline.'' 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. 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. Rather than mandate what these practices must entail, we provide guidance to assist each provider in achieving reasonable data security on its own terms. Taking this approach will also allay concerns that overly prescriptive rules would frustrate rather than improve data security.

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. 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'' 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 and will provide sufficient guidance to providers. Our 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. The CPBR also takes a similar approach.

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. 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. 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, as well as materials that have been issued to guide the implementation of data security requirements under HIPAA, GLBA, and other relevant statutory frameworks. 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 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 industry associations that have participated in this proceeding are active contributors to the CSRIC's work. 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.'' 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. 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. Another practice that is indicative of reasonable data security is training employees and contractors on the proper handling of customer PI. Employee training is a longstanding component of data security under the Commission's existing rules. We encourage providers to seek out expert guidance and best practices on the design and implementation of efficacious training programs. 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. 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. We also remind providers that they are directly accountable for the acts and omissions 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.

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. That said, the record documents some discernable trends in this area that we would currently expect providers to take into account. For instance, we encourage providers to consider stronger alternatives to relying on rudimentary forms of authentication like customer-generated passwords or static security questions. 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. In addition, we encourage providers to periodically reassess the efficacy of their authentication practices and consider possible improvements. 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. 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. The principle of data minimization is also embodied in FTC guidance, in the CPBR, and in the Satellite and Cable Privacy Acts. We encourage providers to look specifically to the FTC's ''Disposal Rule'' for guidance on the safe destruction and disposal of customer PI. 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, another practice that the FTC advises companies to consider. We agree with commenters that technologically sound data encryption can significantly improve data security, in part by minimizing the consequences of a breach. 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. 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. 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. This data security rule replaces the more inflexible data security requirements presently codified in Part 64 of the rules.

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. 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 providers' data security operations, which may be particularly burdensome for smaller providers. 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. The highly specific procedures outlined in the existing voice rules are incongruous with this approach to customer authentication.

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. 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.

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. The data breach notification requirements adopted in this Report and Order extend to breaches involving a carrier's vendors and contractors. 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 customer data is improperly accessed, used, or disclosed incentivizes carriers to adopt strong data security practices. 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. 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. 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. 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. The record reflects various harms inherent in unnecessary notification, including notice fatigue, erosion of consumer confidence in the communications they receive from their provider, and compliance costs. 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. 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. 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.'' Our rule similarly requires the carrier to reasonably determine that no harm to 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. 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. 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. 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.

266. In adopting a harm-based trigger, we clarify that its scope is not limited to ''easily recognized financial harm.'' In the *NPRM,* we acknowledged that ''harm'' is a concept that can be broadly construed to encompass ''financial, physical, and emotional harm.'' 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. 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 all. 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.'' 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.

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. Even commenters that favor minimal breach reporting generally concede that customers are entitled to notification when their most sensitive information is misused or disclosed. 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. While breaches of sensitive customer PI often present severe risks of concrete economic harm, 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. 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.'' The record indicates that smaller providers tend to collect and use customer data, including sensitive information, far less extensively than larger providers. 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. It also will depend on, among other things, the scope and magnitude of potential harm if the data were unencrypted. 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.

271. We agree with other commenters that inadvertent breaches can be just as severe and harmful for consumers as intentional breaches, and consumers are likely to care about serious breaches even when they occur by accident or mistake. Moreover, whether or not a breach was intentional may not always be immediately apparent. 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. 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. 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. 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. 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.'' 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.''

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. 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. 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. 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 and is also consistent with or similar to provisions in various legislative and administration proposals for a federal data breach law. 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.

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 general public. 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 breach 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. 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. We reject arguments that the timeframes for Commission and law enforcement notification that we adopt are too burdensome. 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. Further, to address concerns expressed in the record regarding the complexity and costs of data breach notification for smaller providers, 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. 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. 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.'' 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. This provision replaces the more prescriptive requirements in the existing rules specifying the timing and methods for law enforcement intervention. 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. We also observe that the laws of several states and the District of Columbia include similar law enforcement delay provisions. We are not persuaded that such a provision unduly interferes with the interests of customers in taking informed action to protect themselves against breaches. 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. 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, 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.

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. 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.

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. 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. 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. 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. FTC staff recommends that breach notifications occur without unreasonable delay, but within an outer limit of between 30–60 days. 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.

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.'' 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. 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. While we are sensitive to these concerns, we also note, however, that customer exposure to avoidable or 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. 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. 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, 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 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. 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. Several states currently require data breach notices to contain information about both credit monitoring and credit freezes. 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. 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 Web site. 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 notification frameworks. One of the few commenters to address this issue supports the *NPRM* proposal, while also suggesting that providers post ''substitute breach notifications'' on their Web sites. While some other breach notification frameworks do include such a requirement, 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. 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. 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. 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. Moreover, we find that the modifications we have made to the 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.

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. 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. 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, 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).'' 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. We find that a ''take-it-or-leave it'' approach to the offering of broadband service contingent upon relinquishing customer privacy rights is inconsistent with the telecommunications carriers' ''duty to protect the confidentiality of proprietary information of, and related to . . . customers.'' 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.

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). 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.'' Congress directed the Commission to ''execute and enforce'' the provisions of the Act, including the prohibition on ''unjust or unreasonable'' practices. 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). 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). 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. 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 companies of allowing BIAS providers the flexibility to offer innovative financial incentives. The record does, however, reflect concerns that these programs may be coercive or predatory in persuading consumers to give up their privacy rights. 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. 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.

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. 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. Discount service offerings can benefit consumers. As MMTC explains, for example, such programs ''significantly drive online usage'' as well as ''help financially challenged consumers.''

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. 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.'' Commenters also raise concerns about the potential disproportionate effect on low income individuals. 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.

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. We therefore require BIAS providers offering financial incentives in exchange for consent to use, disclose, 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. Notices that contain material misrepresentations or omissions will not be considered accurate. 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. 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. 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. 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 Web site; 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 Web site, 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.

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 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. 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. The record does not demonstrate a need to modify our complaint process for purpose of the rules we adopt today.

305. On the question of whether BIAS providers should adopt specific dispute resolution processes, we received significant feedback both in support of and in opposition to 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. We expect that 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.

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. 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,'' and ''businesses are typically able to negotiate the appropriate protection of CPNI in their service agreements.'' 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.'' Moreover, business customers may have different privacy and security needs and therefore different expectations. For example, Verizon explains that ''many businesses may want their CPNI used in different ways than a typical consumer.'' Allowing sophisticated enterprise customers to 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'' and allow carriers ''to compete by offering innovative pro-customer options and contracts that meet business customers' privacy and data security expectations.'' 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.

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. 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. We reject the contention that we should exempt enterprise services from our rules entirely with regard to the two limitations above. 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. We clarify that the contract at issue need not be a fully negotiated agreement, but can take the shape of standard order forms. In this regard, as XO observes, an enterprise carrier would ''face significant liability if it violated contractual terms governing privacy and data security.'' 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.

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. 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. PRA approval, as defined herein, is not complete until the Commission publishes notice of OMB approval in the **Federal Register**. 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**. This implementation schedule also applies to the disclosure and consent requirements for financial incentive practices. We acknowledge that our new notice and choice rules may ''represent a significant shift in the status quo'' for carriers. 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. 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**. We find that six months is an appropriate minimum implementation period for data breach implementation. Although providers of telecommunications services other than BIAS are subject to our current breach notification rule and we are confident that carriers are cognizant of the importance of data breach notification in the appropriate circumstances, 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. 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**. 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. 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. 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**. 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. 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**.

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. 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.

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 requires carriers to modify the way they obtain consent for BIAS and voice services based on our sensitivity-based framework discussed above. We seek to minimize disruption to carriers' business practices and therefore do not require carriers to obtain new consent from all their customers. 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, 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. 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. We find that the parameters set forth above create the appropriate balance to limit 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. 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. 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, and throughout this Order we have identified numerous ways to reduce burdens and compliance costs while providing robust privacy protections to their customers. 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. 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.'' 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. 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 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.'' 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. 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. 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. 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. Therefore for these reasons, and the critical importance of privacy protections to 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.

323. We decline to provide any longer or broader extension periods or exemptions to our new privacy rules. 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. 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. 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. State law includes any statute, regulation, order, interpretation, or other state action with the force of law. This limited application of our preemption authority is consistent with our precedent in this area. We have long appreciated and valued the important role states play in upholding the pillars of privacy and protecting customer information. 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 work. 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.'' 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. 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.'' 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. 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. The Commission reviews petitions for preemption of CPNI rules on a case-by-case basis. If a provider believes that it is unable to comply 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. 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,'' 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. 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.

328. In taking this approach, we reject ACA's suggestion that we should ''preempt state data breach notification laws entirely.'' 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.

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, and we welcome state agencies to use our data breach notification rules as a model. 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 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. 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.

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. 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. 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. Accordingly, we adopt a harmonized preemption standard across BIAS and other telecommunications services. 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.

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 confidentiality of proprietary information of, and relating to'' customers, fellow carriers, and equipment manufacturers. Section 222(c) imposes more specific requirements with regard to a subset of customers' proprietary information, namely customer proprietary *network* information. 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. In so doing, we reject the view that Section 222 applies only to voice telephony. The *2015 Open Internet Order* reclassified BIAS as a telecommunications service, making BIAS providers ''telecommunications carriers'' insofar as they are providing such service. 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. 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. The relevant term that defines the scope of section 222 is ''telecommunications carrier,'' and we simply are applying the holding of the *2015 Open Internet Order* that this statutory term encompasses BIAS. Nor does the fact that Section 230 of the Act uses the term Internet, while Section 222 does not, compel us to disregard the clear uses of ''telecommunications carrier'' in Section 222.

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. 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. But their purpose is to specify duties that apply in that limited context, not to define the outer bounds of Section 222. The definition of CPNI found in section 222(h)(1) illustrates this point. 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. 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'' and to exclude ''subscriber list information''—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. 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). 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. 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 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. 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. But the limited scope of this condition does not serve to limit the applicability of Section 222 as a whole. 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. 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. 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. 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). 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. The NET 911 Act 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. We have exercised our ancillary jurisdiction to apply rules adopted under section 222 to providers of interconnected VoIP services.

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''—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, 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. When we forbore from application of the existing implementing rules to BIAS, we made clear that the statute itself still applies. Commenters do not present any compelling reason to revisit this decision.

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).

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. 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. It is well-established that the Commission may adopt rules to implement and enforce an obligation imposed by the Act, including section 222(a). 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.'' 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.'' The term is thus firmly rooted in the language of section 222(a).

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.'' 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).

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'' among the classes of entities owed confidentiality protections as part of a carrier's ''general'' duty. 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). 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.

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. 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. In addition, there is no textual indication that sections 222(b) and (c) define the outer bounds of section 222(a)'s scope. 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.'' 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. Finally, our interpretation of subsection (a) does not render subsection (b) or (c) superfluous. The latter subsections directly impose specific requirements on telecommunications carriers to address concerns that 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. 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.

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. 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.'' 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. In any event, CTIA does not explain what it believes to be the significance of this distinction. 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. 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. Subsection (c) in turn directs the Commission to adopt rules to implement this prohibition and specifies their ''minimum contents.'' 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. In 2009, the D.C. Circuit upheld Commission rules adopted under section 628(b) that prevented cable operators from entering exclusivity agreements with owners of multi-unit buildings, an anti-competitive practice that is only tenuously related to the ''minimum'' regulations implemented under section 628(c). 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). Rather, it held that the Commission's ''remedial powers'' to enforce subsection (b) reached beyond circumstances that Congress ''specifically foresaw.'' 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). In construing the latter we must give effect to the ''actual words'' of the provision. 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.'' 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.'' 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.'' 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,'' or that the provision ''merely identifies the categories of information to which section 222 applies.'' 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) would render that provision superfluous, contrary to the canon against such interpretations. 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. 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. 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 is *published* and therefore is not confidential. 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.'' 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. 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.'' Rather, there was simply no need for Congress to have included subsection (a) in these clauses. 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. 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 duty to protect the confidentiality of such information. 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).

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.'' 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. . . .'' 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.'' 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. 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. 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.* 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. 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 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. 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. 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. 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. 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.''

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.'' Commenters appear to interpret this statement as evidence that Section 222 was intended to apply *only* to CPNI. 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.'' Furthermore, subsections (e) and (g) impose affirmative obligations on carriers in certain circumstances to share SLI, which by definition is not CPNI. 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). 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 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.

357. We acknowledge that prior Commission orders implementing section 222 have focused largely on CPNI rather than customer PI more broadly. 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.'' 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. 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. This early focus on CPNI makes sense: Section 222 was adopted against the background of existing Commission regulations concerning CPNI, and the first section 222 proceeding was instituted in response to a petition from industry seeking clarity about the use of CPNI. However, the Commission has never expressly endorsed the view that section 222(a) fails to reach customer information beyond CPNI. We expressly disavow any prior Commission statement that could be read as endorsing such a view. We therefore disagree that interpreting the provision in a contrary manner will have the effect of unsettling ''18 years'' of Commission precedent in this area.

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. 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. 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). 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 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). 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, subsection (c) concerns the confidentiality of ''individually

identifiable customer proprietary network information'' in particular. 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. 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. The rules we adopt today uphold this widespread customer expectation. 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. 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.

362. We agree with Comcast that ''protect[ing] confidentiality'' of proprietary information involves, among other things, ''preventing [such information] from being exposed without authorization.'' This is among the core purposes of our rules. The requirement to obtain customer 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. The notice requirement advances this purpose further by providing customers the information they need to make informed choices regarding such use, disclosure, and access. As for the data security rule we adopt, its essential purpose is to safeguard customer PI from inadvertent or malicious ''expos[ure].'' 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.'' 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.

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.'' 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. 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],'' and use is the *sole* conduct regulated to address the ''confidentiality of carrier information'' under subsection (b). 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. We agree with Verizon that '' 'protect' and 'use' are different words [that] must have different meanings'' within the statute, 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 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. 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, and commenters generally support some combination of the three. 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. 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 Web sites and in mobile apps. 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. We believe that this prohibition is necessary to give effect to the customer approval that subsection (c) requires.

366. We next require carriers to take reasonable measures to secure the individually identifiable CPNI they collect, possess, use and share. 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. The Commission has long required such reporting as part of a carrier's duty to protect the confidentiality of its customers' information. 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.'' 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). In addition, our rules include provisions that implement the exceptions to Section 222(c) that are set forth in section 222(d). 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.

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.'' 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.* 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.'' 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.

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. 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. 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. 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.'' These rules do so. 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. 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, 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.'' Throughout this Order, we determine that the rules adopted here will promote the public interest.

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.'' 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. 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.

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. Since then, interconnected VoIP providers have operated under these rules. Today, we exercise the same authority to apply to interconnected VoIP services the harmonized set of rules we are adopting for BIAS and other telecommunications services. We make no decisions in this Order on the regulatory classification of interconnected VoIP 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. 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,* 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. 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.'' 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.'' 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,'' defined expressly to incorporate the Commission's definition of ''interconnected VoIP service.''

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. 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. We have also broadened the enterprise customer exemption and taken measures to address the potential for disproportionate impacts on smaller providers, including those that provide interconnected VoIP service. We therefore are not persuaded that our rules will overburden interconnected VoIP providers in particular with ''expand[ed] privacy obligations'' that would ''forestall competition.''

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. 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. 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. By adopting a sensitivity-based 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. The record indicates broad agreement on this point, which is further reinforced by the wealth of case law reiterating the substantial state interest in protecting privacy. 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, 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.

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. Failure to protect the privacy of consumer information can, of course create a risk of financial harm, identity theft and physical threat. The Commission has also found that emotional and dignitary harms are privacy harms, in other contexts. In implementing the Truth in Caller ID Act, the Commission found that ''harm'' was a broad concept encompassing financial, physical, and emotional harm. The FTC similarly recognized that harms beyond the economic, physical, and intrusive are nonetheless real and cognizable, 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.''

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. 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.'' 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.'' This conception of privacy is embedded within the history of the Fair Information Practice Principles (which form the broadly-supported basis for our privacy rules), and within the long history of communications privacy as well. 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. 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. Scholarly literature on privacy also finds that misuse by the collecting entity can harm individuals' privacy, even apart from disclosure.

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. 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). Consumers also object to their data being used, and not only disclosed, in the service of targeted advertising. 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.'' There is evidence that unexpected uses of private customer information can increase fear, uncertainty, powerlessness, and vulnerability. 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. 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 Web sites and 29 percent stopped using an app. In contrast, when companies protect consumers' privacy, consumers' adoption of their products, services, and technologies increases.

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. 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. 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. Customers have an important interest in ensuring that their personal 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.

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. 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.'' 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. 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. 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.'' 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 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. 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, and the record here supports that view . Commenters nearly unanimously argue that use and sharing of sensitive customer information be subject to customer opt-in approval. 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. 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.'' 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. 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.* 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. 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. Were we to interpret *Sorrell* to hold sector-specific privacy laws such as section 222 and our rules to be content-based simply 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. 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. 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. 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.

390. *Compelled Speech.* Some commenters argue that the notice requirements unconstitutionally compel speech from carriers. 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. 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, require only that companies provide factual and uncontroversial information to consumers.

391. *Constitutional Avoidance.* Some commenters raise arguments citing the canon of constitutional avoidance. 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.'' 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.'' The Court further found ''no precedent for applying it to limit the scope of authorized executive action.'' 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, we note that it is well established that common carriers transmitting speech through communications networks are not speakers for First Amendment purposes.

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), an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *Broadband Privacy NPRM.* 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 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. Final Regulatory Flexibility Analysis

399. As required by the Regulatory Flexibility Act of 1980, as amended (RFA), an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *Broadband Privacy NPRM* for this proceeding. 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. This present Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA.

A. Need for, and Objectives of, the Rules

400. In the Order, we adopt privacy requirements for providers of broadband Internet access service (BIAS) and other telecommunications services. 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.

401. 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.

402. 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.''

403. In March 2016, we adopted the *Broadband Privacy NPRM,* which proposed a framework for applying the longstanding privacy requirements of the Act to BIAS. 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.

404. 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''—a position that we have referred to as a gatekeeper. As such, BIAS providers can collect ''an unprecedented breadth'' of electronic personal information.

405. 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

406. 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 Service Providers Association (WISPA). 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.

407. 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; (2) give small carriers additional time to comply with the rules; (3) harmonize notice and choice requirements with the preexisting voice CPNI rules; (4) exempt small carriers from any privacy dashboard requirements and otherwise give them flexibility in the structure of their privacy notices; (5) grandfather existing customer approvals for use and disclosure of customer information; (6) exempt small carriers from any opt-in approval requirements; (6) not impose specific data security requirements on small providers; (7) not impose specific data breach reporting deadlines on small providers, and instead allow them to report breaches as soon as practicable; and (8) not hold small carriers liable for misuse of customer PI by third parties with whom they share the information. We considered these proposals and concerns when composing the Order and the accompanying rules.

C. Response to Comments by the Chief Counsel for Advocacy of the Small Business Administration

408. 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.

409. The SBA filed comments in response to the IRFA encouraging the Commission to examine measures, exemptions, and alternatives that would ease compliance by small telecommunications carriers with our rules. 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.'' 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.''

410. 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. 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. 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. 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

411. 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. The RFA generally defines the term ''small entity'' as having the same meaning as the terms ''small business,'' ''small organization,'' and ''small governmental jurisdiction.'' In addition, the term ''small business'' has the same meaning as the term ''small business concern'' under the Small Business Act. 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.

412. 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 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.*

413. 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

414. 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. First, as of 2013, the SBA estimates there are an estimated 28.8 million small businesses nationwide—comprising some 99.9% of all businesses. 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.'' Nationwide, as of 2007, there were approximately 1,621,315 small organizations. 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.'' Census Bureau data for 2011 indicate that there were 90,056 local governmental jurisdictions in the United States. We estimate that, of this total, as many as 89,327 entities may qualify as ''small governmental jurisdictions.'' Thus, we estimate that most governmental jurisdictions are small.

2. Broadband Internet Access Service Providers

415. 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, which has an SBA small business size standard of 1,500 or fewer employees. These are also labeled ''broadband.'' The latter are within the category of All Other Telecommunications, which has a size standard of annual receipts of $32.5 million or less. 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. Of this total, 3,083 firms had employment of 999 or fewer employees. For the second category, the data show that 1,442 firms operated for the entire year. 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.

416. 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

417. *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.'' 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. 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. Thus, under this size standard, the majority of firms in this industry can be considered small.

418. *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 the applicable SBA size standard, such a business is small if it has 1,500 or fewer employees. 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. The Commission therefore estimates that most providers of local exchange carrier service are small entities that may be affected by the rules adopted.

419. *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. According to Commission data, 3,117 firms operated in that year. Of this total, 3,083 operated with fewer than 1,000 employees. 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. Of this total, an estimated 1,006 have 1,500 or fewer employees.

420. *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. 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. 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. Of these 1,442 carriers, an estimated 1,256 have 1,500 or fewer employees. 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. Also, 72 carriers have reported that they are Other Local Service Providers. Of this total, 70 have 1,500 or fewer employees. Consequently, based on internally researched FCC data, the Commission estimates that most providers of competitive local exchange service, competitive access providers, Shared-Tenant Service Providers, and Other Local Service Providers are small entities.

421. 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.'' 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. 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.

422. *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. 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. According to internally developed Commission data, 359 companies reported that their primary telecommunications service activity was the provision of interexchange services. Of this total, an estimated 317 have 1,500 or fewer employees. Consequently, the Commission estimates that the majority of interexchange service providers are small entities that may be affected by the rules adopted.

423. *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. 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. Consequently, the Commission estimates that the majority of OSPs are small entities that may be affected by these rules.

424. *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 networks operators (MVNOs) are included in this industry. Under the applicable SBA size standard, such a business is small if it has 1,500 or fewer employees. 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. 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. All 193 carriers have 1,500 or fewer employees. Consequently, the Commission estimates that the majority of prepaid calling card providers are small entities that may be affected by the rules adopted.

425. *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. 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. 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. Of this total, an estimated 211 have 1,500 or fewer employees. Consequently, the Commission estimates that the majority of local resellers are small entities that may be affected by the rules adopted.

426. *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. Under that size standard, such a business is small if it has 1,500 or fewer employees. 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. 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. Of this total, an estimated 857 have 1,500 or fewer employees. Consequently, the Commission estimates that the majority of toll resellers are small entities.

427. *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. 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. 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. Of these, an estimated 279 have 1,500 or fewer employees. Consequently, the Commission estimates that most Other Toll Carriers are small entities.

4. Wireless Providers—Fixed and Mobile

428. 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.

429. *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. 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. Of this total, an estimated 261 have 1,500 or fewer employees. Thus, using available data, we estimate that the majority of wireless firms can be considered small.

430. *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 revenues of $15 million for each of the three preceding years. The SBA has approved these definitions.

431. *1670–1675 MHz Services.* This service can be used for fixed and mobile uses, except aeronautical mobile. 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.

432. *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). Under the SBA small business size standard, a business is small if it has 1,500 or fewer employees. According to Commission data, 413 carriers reported that they were engaged in wireless telephony. Of these, an estimated 261 have 1,500 or fewer employees and 152 have more than 1,500 employees. Therefore, a little less than one third of these entities can be considered small.

433. *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. 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. These small business size standards, in the context of broadband PCS auctions, have been approved by the SBA. 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. On April 15, 1999, the Commission completed the reauction of 347 C-, D-, E-, and F-Block licenses in Auction No. 22. Of the 57 winning bidders in that auction, 48 claimed small business status and won 277 licenses.

434. 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. 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. On May 21, 2007, the Commission completed an auction of 33 licenses in the A, C, and F Blocks in Auction No. 71. Of the 12 winning bidders in that auction, five claimed small business status and won 18 licenses. On August 20, 2008, the Commission completed the auction of 20 C-, D-, E-, and F-Block Broadband PCS licenses in Auction No. 78. Of the eight winning bidders for Broadband PCS licenses in that auction, six claimed small business status and won 14 licenses.

435. *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. 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. The SBA has approved these small business size standards for the 900 MHz Service. 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. 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.

436. 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. 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. 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.

437. 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. 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.

438. *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. 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. 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. 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. The SBA approved these small size standards. 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. 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. Seventeen winning bidders claimed small or very small business status and won 60 licenses, and nine winning bidders claimed entrepreneur status and won 154 licenses. 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.

439. In 2007, the Commission reexamined its rules governing the 700 MHz band in the *700 MHz Second Report and Order.* 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. 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.

440. *Upper 700 MHz Band Licenses.* In the *700 MHz Second Report and Order,* the Commission revised its rules regarding Upper 700 MHz licenses. 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. 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.

441. *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. 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. 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. SBA approval of these definitions is not required. An auction of 52 Major Economic Area licenses commenced on September 6, 2000, and closed on September 21, 2000. 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.

442. *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. 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. 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. These definitions were approved by the SBA. 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.

443. *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, 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.

444. *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.

445. *Fixed Microwave Services.* Microwave services include common carrier, private-operational fixed, and broadcast auxiliary radio services. They also include the Local Multipoint Distribution Service (LMDS), the Digital Electronic Message Service (DEMS), and the 24 GHz Service, where licensees can choose between common carrier and non-common carrier status. 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. Under the present and prior categories, the SBA has deemed a wireless business to be small if it has 1,500 or fewer employees. 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.

446. *Broadband Radio Service and Educational Broadband Service.* Broadband Radio Service systems, previously referred to as Multipoint Distribution Service (MDS) and Multichannel 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)). 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. 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. 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.

447. In 2009, the Commission conducted Auction 86, the sale of 78 licenses in the BRS areas. 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. Auction 86 concluded in 2009 with the sale of 61 licenses. 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.

448. 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. 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 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.'' 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. According to Census Bureau data for 2007, there were a total of 996 firms in this category that operated for the entire year. 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. Thus, the majority of these firms can be considered small.

5. Satellite Service Providers

449. *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. The second has a size standard of $30 million or less in annual receipts.

450. 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.'' For this category, Census Bureau data for 2012 show that there were a total of 333 firms that operated for the entire year. Of this total, 299 firms had annual receipts of under $25 million. Consequently, we estimate that the majority of Satellite Telecommunications firms are small entities that might be affected by our action.

451. 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.'' 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. Thus, a majority of ''All Other Telecommunications'' firms potentially affected by the rules adopted can be considered small.

6. Cable Service Providers

452. *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.'' 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. According to Census Bureau data for 2007, there were a total of 2,048 firms in this category that operated for the entire year. Of this total, 1,393 firms had annual receipts of under $10 million, and 655 firms had receipts of $10 million or more. Thus, the majority of these firms can be considered small.

453. *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. Industry data shows that there were 1,141 cable companies at the end of June 2012. Of this total, all but ten cable operators nationwide are small under this size standard. In addition, under the Commission's rules, a ''small system'' is a cable system serving 15,000 or fewer subscribers. Current Commission records show 4,945 cable systems nationwide. 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.

454. *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.'' There are approximately 52,403,705 cable video subscribers in the United States today. 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. Based on available data, we find that all but nine incumbent cable operators are small entities under this size standard. 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. 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

455. ''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. 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. 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. Thus, a majority of ''All Other Telecommunications'' firms potentially affected by the rules adopted can be considered small.

E. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

456. 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.

457. *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' Web sites 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. We have declined to require periodic notice on an annual or bi-annual basis, similar to what the preexisting CPNI rules require.

458. *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. 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.

459. 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.

460. *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 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.

461. *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. We also require providers to keep records, for two years, of the dates of breaches and the dates when customers are notified.

462. 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. 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.

463. *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. However, the Order does not prohibit BIAS providers from offering financial incentives to permit the use or disclosure of such information. 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. BIAS providers must make financial incentive notices easily accessible and separate from any other privacy notifications. 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 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.

F. Steps Take To Minimize the Significant Economic Impact on Small Entities and Significant Alternatives Considered

464. 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.''

465. 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. Additionally, harmonizing our rules across all telecommunications services will reduce and streamline compliance costs for small carriers. 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.

466. *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. We also decline to adopt specific notice requirements in mobile formats and we decline to require periodic notices of privacy practices.

467. *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. 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 develop specific customer service architecture. Third, we decline to require a specific format for accepting customer privacy choices and therefore allow carriers, particularly small carriers, that lack sophisticated Web sites 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. To further reduce compliance burdens, we have clarified that choice solicitations may be combined a carrier's other privacy policy notices.

468. *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. 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.

469. *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. 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. 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.

470. *Implementation.* To provide certainty to customers and carriers alike, we establish a 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.

471. 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. 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.

472. 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.

473. 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.

474. 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 the **Federal Register**. We also adopt a uniform implementation timetable for both BIAS and other telecommunications services.

475. 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. 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.

476. 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. 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. 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.

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. 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**.

VII. Ordering Clauses

477. 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.*

478. *It is further ordered* that part 64 of the Commission's rules IS AMENDED as set forth in Appendix A.

479. *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**.

480. *It is further ordered* that, except as set forth in the prior paragraph, this Report and Order *shall be* effective 30 days after date of 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.

481. *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).

482. *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.

List of Subjects in 47 CFR Part 64

Claims, Communications common carriers, Computer technology, Credit, Foreign relations, Individuals with disabilities, Political candidates, Radio, Reporting and recordkeeping requirements, Telecommunications, Telegraph, Telephone.

Federal Communications Commission.

Marlene H. Dortch,

Secretary.

Final Rules

For the reasons discussed in the preamble, the Federal Communications Commission amends 47 CFR part 64 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. In part 64, revise subpart U to read as follows:

Subpart U—Protecting Customer Information

Sec.

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.

The following definitions apply to this subpart.

(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 § 9.3 of this chapter.

(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 § 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 paragraph (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 paragraph (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 paragraph (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 § 64.2004;

(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 paragraph (a) of this section 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 Web site, 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 paragraph (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 § 64.2004; 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 paragraph (a) of this section, 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 paragraphs (b) and (c) of this section.

(d) *Notice and solicitation required.* (1) Except as described in paragraph (a) of this section, a telecommunications carrier must at a minimum solicit customer approval pursuant to paragraph (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 § 64.2003.

(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 § 64.2003(a) and a means to access the mechanism required by paragraph (e) of this section.

(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 Web site; 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 Web site, 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 paragraph 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 on 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 paragraph 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 § 64.2004(c) 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 Web site; 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 Web site, 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.

[FR Doc. 2016–28006 Filed 12–1–16; 8:45 am]

BILLING CODE 6712–01–P