FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 64

[WC Docket No. 16–106; FCC 16–39]

Protecting the Privacy of Customers of Broadband and Other Telecommunications Services

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: The Federal Communications Commission initiates a rulemaking seeking public comment on how to apply the privacy requirements of the Communications Act to broadband Internet access service (BIAS). This Notice of Proposed Rulemaking (NPRM) focuses on transparency, choice, and data security, in a manner that is consistent with the Commission's history of protecting privacy, the Federal Trade Commission's leadership, and various sector-specific statutory approaches, tailored to the particular circumstances that consumers face when they use broadband networks and with an understanding of the particular nature and technologies underlying those networks. The NPRM would recognize that consumers cannot give their permission for the use of protected data unless relevant broadband provider practices are transparent. The NPRM proposes a framework to ensure that consumers; understand what data the broadband provider is collecting and what it does with that information; can decide how their information is used; and are protected against the unauthorized disclosure of their information. The NPRM also seeks comment on a number of closely-related questions.

DATES: Submit comments on or before May 27, 2016. Submit reply comments on or before June 27, 2016. Written comments on the Paperwork Reduction Act proposed information collection requirements must be submitted by the public, Office of Management and Budget (OMB), and other interested parties on or before June 20, 2016.

ADDRESSES: You may submit comments, identified by WC Docket No. 16–106, by any of the following methods:

- *Federal Communications Commission's Web site: http://apps.fcc.gov/ecfs/.* Follow the instructions for submitting comments.
- *People with Disabilities:* Contact the FCC to request reasonable accommodations (accessible format documents, sign language interpreters, CART, etc.) by email: *FCC504@fcc.gov* or phone: 202–418–0530 or TTY: 202–418–0432.

For detailed instructions for submitting comments and additional information on the rulemaking process, see the **SUPPLEMENTARY INFORMATION** section of this document. In addition to filing comments with the Secretary, a copy of any comments on the Paperwork Reduction Act information collection requirements contained herein should be submitted to the Federal Communications Commission via email to *PRA@fcc.gov* and to Nicole Ongele, Federal Communications Commission, via email to *Nicole.Ongele@fcc.gov.*

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: Pursuant to Sections 1.415 and 1.419 of the Commission's rules, 47 CFR 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). *See Electronic Filing of Documents in Rulemaking Proceedings,* 63 FR 24121 (1998), *http://www.fcc.gov/Bureaus/OGC/Orders/1998/fcc98056.pdf.*

- *Electronic Filers:* Comments may be filed electronically using the Internet by accessing the ECFS: *http://apps.fcc.gov/ecfs/.*
- *Paper Filers:* Parties who choose to file by paper must file an original and one copy of each filing. If more than one docket or rulemaking number appears in the caption of this proceeding, filers must submit two additional copies for each additional docket or rulemaking number.

Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

- All hand-delivered or messenger-delivered paper filings for the Commission's Secretary must be delivered to FCC Headquarters at 445 12th St. SW., Room TW–A325, Washington, DC 20554. The filing hours are 8:00 a.m. to 7:00 p.m. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of *before* entering the building.
- Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9300 East Hampton Drive, Capitol Heights, MD 20743.
- U.S. Postal Service first-class, Express, and Priority mail must be addressed to 445 12th Street SW., Washington, DC 20554.

People with Disabilities: 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).

Synopsis

In this Notice of Proposed Rulemaking (NPRM), we propose to apply the privacy requirements of the Communications Act to broadband Internet access service (BIAS) and seek comment on how best to protect the privacy of the personal information of BIAS customers.

I. Introduction

1. The intersection of privacy and technology is not new. In 1890, Samuel Warren and Louis Brandeis inaugurated the modern age of privacy protection when they warned that ''numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet should be proclaimed from the house-tops.' '' The new technology they had in mind? The portable camera.

2. In this Notice of Proposed Rulemaking (NPRM or Notice), we propose to apply the traditional privacy requirements of the Communications Act to the most significant communications technology of today: Broadband Internet access service (BIAS). This is important because both consumers and Internet Service Providers (ISPs) would benefit from additional, concrete guidance explaining the privacy responsibilities created by the Communications Act. To that end, our approach can be simply stated: *First,* consumers must be able to protect their privacy, which requires transparency, choice, and data security. *Second,* ISPs are the most important and extensive conduits of consumer information and thus have access to very sensitive and very personal information that could threaten a person's financial security, reveal

embarrassing or even harmful details of medical history, or disclose to prying eyes the intimate details of interests, physical presence, or fears. But, *third,* the current federal privacy regime, including the important leadership of the Federal Trade Commission (FTC) and the Administration efforts to protect consumer privacy, does not now comprehensively apply the traditional principles of privacy protection to these 21st Century telecommunications services provided by broadband networks. That is a gap that must be closed, and this NPRM proposes a way to do so by securing what Congress has commanded—the ability of every telecommunications user to protect his or her privacy.

3. Privacy protects important personal interests. Not just freedom from identity theft, financial loss, or other economic harms but also from concerns that intimate, personal details could become grist for the mills of public embarrassment or harassment or the basis for opaque, but harmful judgments, including discrimination. The power of modern broadband networks is that they allow consumers to reach from their homes (or cars or sidewalks) to the whole wide world instantaneously. The accompanying concern is that those broadband networks can now follow the activities of every subscriber who surfs the web, sends an email or text, or even walks down a street carrying a mobile device. Absent legally-binding principles, those networks have the commercial motivation to use and share extensive and personal information about their customers. The protection of privacy thus both protects individuals and encourages use of broadband networks, by building trust.

4. Today, as the FTC has explained, ISPs are ''in a position to develop highly detailed and comprehensive profiles of their customers—and to do so in a manner that may be completely invisible.'' This is particularly true because a consumer, once signed up for a broadband service, simply cannot avoid that network in the same manner as a consumer can instantaneously (and without penalty) switch search engines (including to ones that provide extra privacy protections), surf among competing Web sites, and select among diverse applications. Indeed, the whole purpose of the customer-provider relationship is that the network becomes an essential means of communications with destinations chosen by the customer; which means that, absent use of encryption, the broadband network has the technical capacity to monitor traffic transmitted between the consumer and each destination, including its content. Although the ability to monitor such traffic is not limitless, it is ubiquitous. Even when traffic is encrypted, the provider has access to, for example, 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. Providers of BIAS (''broadband providers'') thus have the ability to capture a breadth of data that an individual streaming video provider, search engine or even e-commerce site simply does not. And they have control of a great deal of data that must be protected against data breaches. To those who say that broadband providers and edge providers must be treated the same, this NPRM proposes rules that recognize that broadband networks are not, in fact, the same as edge providers in all relevant respects. But this NPRM looks to learnings from the FTC and other privacy regimes to provide complementary guidance.

5. The core privacy principles—transparency, choice, and security—underlie the critical steps that the federal government has taken to protect the privacy of many specific forms of data. Indeed, these three principles are the heart of the internationally recognized Fair Information Practices Principles (FIPPs) that have informed our nation's thinking on privacy best practices while providing the framework for most of our federal privacy statutes.

6. Today, the Commission is empowered to protect the private information collected by telecommunications, cable, and satellite companies in Sections 222, 631, and 338 of the Communications Act and the Commission has recognized the importance of longstanding privacy principles in adopting and refining its existing Section 222 rules and enforcing privacy requirements. Thus, from the outset of its implementation of Section 222, the Commission has focused on ensuring that consumers have the tools to give their approval for the use and sharing of protected information.

7. Meanwhile, as consumer use of the Internet exploded, the FTC, using its authority to prohibit ''unfair or deceptive acts or practices in or affecting commerce,'' entered into a series of precedent-setting consent orders addressing privacy practices on the Internet. Taken together, the FTC's online privacy cases focus 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. Although the application of Section 222 to BIAS has implications for the jurisdiction of the FTC, that agency's leadership is critically important in this sphere and the Commission is determined to continue its close working relationship with the FTC. Most recently, the two agencies entered into a consumer protection Memorandum of Understanding (MOU). In the MOU each agency recognizes the others' expertise and we each agreed to coordinate and consult on areas of mutual interest.

8. This NPRM supports the ability of broadband networks to be able to provide personalized services, including advertising, to consumers—while reaping the financial rewards therefrom. For example, many consumers want targeted advertising that provides very useful information in a timely (sometimes immediate) manner. Nothing in this NPRM stops consumers from receiving targeted recommendations—or any other form of content they wish to consume. But well-functioning commercial marketplaces rest on informed consent. Permission is required before purchasers can be said to agree to buy a product; permission is needed before owners of property transfer their interests in that property. This NPRM embraces the basic economic principle that informed choice is necessary to protect the fundamental interest in privacy. Thus, the consumer who possesses private information must provide the broadband provider advanced approval for the use of that data. In many instances, that approval is inherent in the use of the broadband Internet access service (for example, the routing of communications to or from the consumer), but where it is not, this NPRM proposes that separate consent must be obtained. This is good for consumers and it is good business, as the success of opt-in provisions in other contexts demonstrates.

9. In the *2015 Open Internet Order,* we concluded that Section 222 should be applied to the broadband connections consumers use to reach the Internet, the newly-reclassified Title II service defined as ''Broadband Internet Access Service'' (BIAS). Section 222 is a sector-specific statute that includes detailed requirements that Congress requires be applied to the provision of telecommunications services, but not to the provision of other services by broadband providers nor to information providers at the edge of the network.

Thus, this NPRM applies existing statutory authority solely to the existing class of services that Congress included within the scope of Title II, namely the delivery of telecommunications services.

II. Ensuring Privacy Protections for Customers of Broadband Services

A. Defining Key Terms

10. To provide guidance to both broadband providers and customers regarding the scope of the privacy protections we propose today, in this section we propose to define the entities to which our rules apply and the scope of information covered by such rules. We also propose to define other key terms, including what constitutes ''opt-out'' and ''opt-in'' for purposes of giving customers control over the use of their confidential information, what constitutes aggregate customer proprietary information, and what constitutes a ''breach'' for purposes of our proposed data security and data breach notification rules. Finally, we seek comment on whether and how we should modify any of the current Section 222 definitions, either to update those definitions or harmonize them with the rules we propose to adopt with respect to BIAS providers. We recognize there will be an interplay between commenters' proposals about what substantive rules we should adopt to protect BIAS customers' privacy interests and how we should define key terms and we invite commenters to explore in detail the relationships between the two.

1. Defining BIAS and BIAS Provider

11. We propose to apply the definition of ''Broadband Internet Access Services'' or ''BIAS'' that we used in the *2015 Open Internet Order.* In that proceeding, we defined BIAS to mean ''[a] mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up Internet access service. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence, or that is used to evade the protections set forth in this part.'' We propose to define ''broadband Internet access service provider'' (BIAS provider) as a person or entity engaged in the provision of BIAS.

2. Defining Affiliate

12. We seek comment on how we should define ''affiliate'' for purposes of our proposed rules. The Act, as amended, and our current rules, define ''affiliate'' to mean ''a person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another person,'' where the term ''own'' is defined to mean ''to own an equity interest (or the equivalent thereof) of more than 10 percent.'' We seek comment on whether we should adopt this definition or another definition for purposes of our proposed rules, as well as any associated benefits and burdens, particularly for small providers.

3. Defining Customer

13. We propose to define ''customer'' to mean (1) a current or former, paying or non-paying subscriber to broadband Internet access service; and (2) an applicant for broadband Internet access service. We seek comment on our proposal and on whether we should harmonize the existing Section 222 definition of customer with our proposed broadband definition.

14. Under our current Section 222 rules, ''[a] customer of a telecommunications carrier is a person or entity to which the telecommunications carrier is currently providing service.'' We believe that the existing rule's limitation to current subscribers is insufficiently narrow, perhaps particularly as applied to the broadband context. As technological capabilities have progressed, data retention and processing have increased, concomitantly increasing the incentives for retaining, using, and selling personal information of applicants and of former customers. Because BIAS providers have the ability to retain and reuse applicant and former customer proprietary information long after the application process is over, or the former customer has discontinued its subscription, we propose to define customer for BIAS purposes to include both applicants for BIAS and former BIAS customers. We recognize that not all aspects of our proposed rules will be applicable to all such customers in every situation (*e.g.,* a data breach may impact some customers but not others). For the purposes of these proposed rules we sometimes refer to ''affected customers'' or ''existing customers'' to designate a subset of customers, as appropriate.

15. In seeking comment on our proposed definition of ''customer'' we inquire as to whether, without the privacy protections of Section 222, consumers may be hesitant to apply for BIAS or current BIAS users may be apprehensive about switching service providers out of concern that their current provider may stop protecting their privacy after they switch providers. Could such apprehension inhibit competition and innovation in the BIAS marketplace?

16. We recognize that a single BIAS subscription is often used by multiple people. Residential fixed broadband services typically have a single subscriber, but are used by all members of a household, and often by their visitors. Some mobile BIAS providers offer friends and family plans in which multiple people are enrolled on one BIAS account, each with their own identified device(s) or user login. Should the definition of customer reflect the possibility of multiple broadband users? Should each member of a group plan or each user with a login be treated as a distinct customer who must receive individualized notices and consent requests? Is such a definition of ''customer'' appropriately consistent with the definition of ''end user'' adopted in the *2015 Open Internet Order*? Under such an interpretation, how would or should BIAS providers treat members of a group plan who are minors or are otherwise unable to understand notice and consent? How can we ensure that BIAS providers protect the information of all users of broadband Internet access service, given that the contract is between the BIAS provider and its subscriber? Should we define ''subscriber'' as any person about whom broadband providers hold customer information? How should we treat the interests of persons using corporate accounts, for example, including the employees of a small business? We seek comment on these issues and the benefits and burdens of any proffered alternatives.

17. At the same time, we are cognizant of the potential burdens that defining the term ''customer'' too broadly could place on BIAS providers, and we believe that the definition we propose today strikes the right balance between minimizing the burdens on BIAS providers and protecting customer proprietary information. We believe that our proposed definition will minimize the burden on BIAS providers by limiting the proposed notice and consent requirements to interactions with a single account holder, as opposed to every individual who connects to a broadband service over that subscription. Do commenters agree? We seek comment on the benefits and burdens associated with our proposed definition, and any alternatives,

including, in particular, burdens on small providers.

18. We also seek comment on whether we should revise the definition of ''customer'' in the existing CPNI rules to be consistent with our proposed definition of ''customer'' in the BIAS context. At least some of the concerns we identified above in regard to BIAS customers are not unique to BIAS; voice customers in today's world of big data face similar issues related to the protection of their own private information when they apply for and after they have terminated service. Given these concerns, we seek comment whether we should harmonize the definition of ''customer'' across voice and broadband platforms for purposes of protecting customer privacy.

19. Finally, to the extent we adopt rules that harmonize the privacy requirements under section 222 with the requirements for cable and satellite providers under Sections 631 and 338(i), should we understand the term ''subscriber'' in those provisions of the Act to be coextensive with the term ''customer'' we propose here?

4. Defining CPNI in the Broadband Context

20. As with the existing CPNI rules, we propose to adopt the statutory definition of CPNI for use in the broadband context. Section 222(h)(1) defines CPNI to mean ''information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship'' and ''information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer or a carrier,'' except that CPNI ''does not include subscriber list information.'' We seek comment on this proposal. Is there any need to include the second part of that definition in our rules regarding BIAS services, given its applicability only to telephone exchange service and telephone toll service?

21. We propose to interpret the phrase ''made available to the carrier by the customer solely by virtue of the carrier-customer relationship'' in the definition of CPNI to include any information falling within a CPNI category, as discussed below, that the BIAS provider collects or accesses in connection with the provision of BIAS. Consistent with the Commission's *2013 CPNI Declaratory Ruling,* this includes information that a BIAS provider causes to be collected and stored on customer premises equipment (CPE) or other devices, including mobile devices, in order to allow the carrier to collect or access the information. As the Commission held, 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.'' We also recognize that a BIAS provider has the ability to create and append CPNI to a customer's Internet traffic, such as by inserting a user ID header (UIDH). We interpret any information the BIAS provider attaches to a customer's Internet traffic to be CPNI if it falls within one of the categories delineated in Section 222(h)(1)(A). We seek comment on our approach.

22. In order to provide guidance to consumers and to BIAS providers, we propose to provide specific examples of the types of information that we consider CPNI in the broadband context. In the context of the existing CPNI rules, the Commission has explicitly declined to set out a comprehensive list of data elements that do or do not satisfy the statutory definition of CPNI, and we propose to continue to follow that model in the broadband context. The Commission has, however, enumerated certain data elements that it considers to be 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 consumer, such as call waiting—and we propose to delineate similar non-exhaustive examples of the types of information that we would consider to constitute CPNI in the broadband context. We believe that such guidance will help provide direction regarding the scope of broadband providers' obligations and help to increase consumers' confidence in the security of their confidential information as technology continues to advance. We seek comment on this approach, alternatives, and any associated benefits and burdens, particularly for small providers.

a. Types of Information That Meet the Statutory Definition of CPNI

23. We propose that, at a minimum, we consider the following types of information to constitute CPNI in the broadband context: (1) Service plan information, including type of service (*e.g.,* cable, fiber, or mobile), service tier (*e.g.,* speed), pricing, and capacity (*e.g.,* information pertaining to data caps); (2) geo-location; (3) media access control (MAC) addresses and other device identifiers; (4) source and destination Internet Protocol (IP) addresses and domain name information; and (5) traffic statistics. Below we offer explanations for why we consider each of these type of data to fall within our proposed definition of CPNI with respect to BIAS. We seek comment on our proposed interpretations. We ask that commenters explain their responses to our proposed interpretations and identify any other element of the definition of CPNI which commenters believe covers any of the specific data elements described below.

24. *Broadband Service Plans.* We propose to consider information related to a customer's broadband service plan as CPNI in the broadband context. Broadband service plans are analogous to voice telephony service plans, which the Commission has long considered to be CPNI under the existing CPNI rules. We believe that information related to the telecommunications services the BIAS provider provides to the customer, including type of service (*e.g.,* fixed or mobile; cable or fiber; prepaid or term contract), speed, pricing, and capacity (including information pertaining to data caps) is information relating to the ''quantity,'' ''technical configuration,'' ''type,'' and ''amount of use'' of a telecommunications service subscribed to by a customer. We seek comment on this proposed interpretation. Are there other data elements that are analogous to those included in a voice telephony service plan that we should consider CPNI in the broadband context?

25. *Geo-Location.* We propose to consider information related to the physical or geographical location of a customer or the customer's device(s) (geo-location), regardless of the particular technological method a BIAS provider uses to obtain this information, to be CPNI in the broadband context. The statutory definition of CPNI includes information related to ''location'' of a telecommunications services subscribed to by a customer. The Commission has held that ''[t]he location of a customer's use of a telecommunications service also clearly qualifies as CPNI.'' We seek comment on this proposed interpretation.

26. *Media Access Control (MAC) Addresses and Other Device Identifiers.* We propose to consider any MAC address associated with a customer's device to be CPNI in the broadband context. 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); as such, we believe it is analogous to the IMEI mobile device identifier in the

voice telephony context. Because BIAS providers use MAC addresses to route data packets to the end user, we believe that we should consider such information ''destination'' and ''technical configuration'' information under Section 222(h)(1)(A). Similarly, we propose to consider other device identifiers and other information in link layer protocol headers to be CPNI in the broadband context. We seek comment on our proposed interpretation. We also seek comment on other types of device identifiers that meet the statutory definition of CPNI. For example, our TRS rules recognize that a unique device identifier such as an ''electronic serial number'' is ''call data information'' in the TRS CPNI context.

27. *Internet Protocol (IP) Addresses and Domain Name Information.* We propose to consider both source and destination IP addresses as CPNI in the broadband context. An IP address is the 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, IP addresses are roughly analogous to telephone numbers in the voice telephony context, and 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. IP addresses are also frequently used in geo-location. As such, we believe that we should consider IP addresses to be ''destination'' and ''location'' information under Section 222(h)(1)(A). Similarly, we propose to consider other information in Internet layer protocol headers to be CPNI in the broadband context, because they may indicate the ''type'' and ''amount of use'' of a telecommunication service. We seek comment on this proposed interpretation.

28. Similarly, we propose to consider the domain names with which an end user communicates CPNI in the broadband context. Domain names (*e.g.,* ''*www.fcc.gov*'') are common monikers that the end user uses to identify the endpoint to which they seek to connect. Domain names also translate into IP addresses, which we propose to consider CPNI. We therefore propose to treat domain names as destination and location information. We seek comment on this proposed interpretation.

29. *Traffic Statistics.* We propose to consider traffic statistics to be CPNI pertaining to the ''type'' and ''amount of use'' of a telecommunications service. We believe that ''amount of use'' encompasses quantifications of 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). We recognize that modern technology enables easily collecting and analyzing traffic statistics to draw powerful inferences that implicate customer privacy. For example, a BIAS provider could deduce the type of application (*e.g.,* VoIP or web browsing) that a customer is using, and thus the purpose of the communication. Further, traffic statistics can be used to determine the date, time, and duration of use, and deduce usage patterns such as when the customer is at home, at work, or elsewhere. We believe traffic statistics are analogous to call detail information regarding the ''duration[] and timing of [phone] calls'' and aggregate minutes in the voice telephony context. We seek comment on our proposed interpretation.

b. Other Broadband Data Elements That Could Meet the Statutory Definition of CPNI

30. We also seek comment on whether we should consider other types of information to fall within the statutory definition of CPNI in the broadband context, including: (1) Port information; (2) application headers; (3) application usage; and (4) CPE information.

31. *Port Information.* We seek comment on whether we should consider port information to be ''technical configuration,'' ''type,'' ''destination'' information, and/or any other category of CPNI under Section 222(h)(1)(A). A port is a logical endpoint of communication with the sender or receiver's application. The destination port number determines which application receives the communication. We believe that 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 or web browsing. We understand that BIAS providers sometimes configure their networks using port information for network management purposes, such as to block certain ports to ensure network security. We seek comment on whether we should consider port numbers and other information regarding port usage CPNI in the broadband context. Similarly, we seek comment on whether we should consider other information in transport layer protocol headers to be CPNI in the broadband context, for instance because it may be information that relates to the ''technical configuration'' or ''amount of use'' of a telecommunications service.

32. *Application Header.* We seek comment on whether we should consider application headers ''technical configuration,'' ''type,'' and/or ''destination'' information, or any other category of CPNI under Section 222(h)(1)(A). Application headers are application-specific data that assist with or otherwise relate to requesting and conveying application-specific content. The application header communicates information between the application on the end user's device and the corresponding application at the other endpoint(s) with which the user communicates. For example, application headers for web browsing typically contain the Uniform Resource Locator (URL), operating system, and web browser; application headers for email typically contain the source and destination email addresses. 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. We understand that BIAS providers sometimes configure their networks using application headers for network management purposes. We believe that access to application headers is analogous in the voice telephony context to accessing a customer's choices within telephone menus used to route calls within an organization (*e.g.,* ''Push 1 for sales. Push 2 for billing.''). We seek comment on whether we should consider application headers CPNI in the broadband context. Similarly, we seek comment on whether we should consider any other application layer information to be CPNI in the broadband context.

33. *Application Usage.* We seek comment whether and under what circumstances we should consider information the broadband provider collects about the use of applications to meet the statutory definition of CPNI. As the Commission discussed in the *2013 CPNI Declaratory Ruling,* if such information meets the terms of Section 222(h)(1)(A) and the broadband provider directs the collection or storage of the information, it is CPNI. Based on this clarification, should we conclude that information the broadband provider collects about the usage of applications is CPNI in the broadband context, if the broadband provider directs such collection and the information collected falls within the statutory elements of CPNI? Based on the principles discussed in the *2013 CPNI Declaratory Ruling,* could application usage that

does not result in transmission also qualify as CPNI?

34. *Customer Premises Equipment (CPE) Information.* We seek comment whether we should consider information regarding CPE as ''relat[ing] to the . . . technical configuration'' and/or ''type . . . of use of a telecommunication service,'' or any other category under the statutory definition of CPNI. CPE is defined in the Act as ''equipment employed on the premises of a person (other than a carrier) to originate, route, or terminate telecommunications.'' In the broadband context, we believe CPE would include, but not be limited to, a customer's smartphone, tablet, computer, modem, router, videophone, or IP caption phone. The nature of a customer's device may impact the technical configuration of the broadband service based on the communications protocol that the device uses and may also identify the type of service to which the customer subscribes (*e.g.,* fixed vs. mobile, cable vs. fiber). We seek comment whether we should consider CPE information CPNI in the broadband context.

35. *Other.* We seek comment on what other customer information there is to which a BIAS provider has access by virtue of its provision of BIAS, whether such information should appropriately be considered CPNI, and why. We also seek comment on whether we should include any additional information in the definition of CPNI in the mobile context. If we find that any of the information discussed in this section is not CPNI, we seek comment on whether and how it should be protected.

36. We also seek comment on whether we should consider adopting a broader definition of CPNI and include additional categories of customer information into CPNI. If so, what should that definition be and what should it include? Is adopting a broader definition of CPNI the best way to provide consumers with robust privacy protections? What are the benefits and drawbacks to adopting a broader definition of CPNI?

37. Finally, we seek comment on any other issues we should address in conjunction with the definition of CPNI, as well as the benefits and burdens associated with any proposals to remedy those concerns, and in particular any associated benefits and burdens for small providers.

5. Defining Customer Proprietary Information

38. Section 222(a) imposes a general duty on telecommunications carriers ''to protect the confidentiality of proprietary information of, and relating to . . . customers.'' Although the Commission's previous rulemakings addressing Section 222 have been limited to CPNI, subsection (a) by its terms does not appear to be limited to protecting customer information defined as CPNI. In its initial Section 222 rulemaking, the Commission limited itself to adopting rules implementing the CPNI requirements of Sections 222(c)–(f) in response to a petition from local exchange carrier associations. More recently, however, the Commission recognized the obligation of providers to protect the confidentiality of customer proprietary information pursuant to Section 222(a) in the enforcement context. In the *TerraCom NAL* we interpreted customer ''proprietary information'' as ''clearly encompassing private information that customers have an interest in protecting from public exposure,'' including, but not limited to, ''privileged information, trade secrets, and personally identifiable information.'' We explained that, in 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.''

39. In keeping with that interpretation of Section 222(a), we propose to define ''proprietary information of, and relating to . . . customers'' to include private information that customers have an interest in protecting from public disclosure, and consider such information to fall into two categories: (1) Customer proprietary network information (CPNI); and (2) personally identifiable information (PII) the BIAS provider acquires in connection with its provision of BIAS. We refer to these two categories of data together as ''customer proprietary information'' or ''customer PI.'' We believe Section 222(a) protects CPNI because customer proprietary network information is a specific subtype of customer proprietary information generally. As described in more detail below, consistent with well-developed concepts of what constitutes personally identifiable information in the modern world, we propose to define PII to mean any information that is linked or linkable to an individual. Protecting personally identifiable information from breaches of confidentiality is a core value of most privacy regimes. We seek comment on our proposal.

40. Providing protection for PII as well as CPNI will benefit consumers, while having limited adverse impacts on BIAS providers, as both are types of information that customers reasonably expect their BIAS provider to keep secure and confidential. We expect that, for the most part, broadband providers already keep such information secure and treat it with some degree of confidentiality based on, among other things, FTC guidance that BIAS providers would have reasonably understood applied to them prior to the reclassification of broadband in the *2015 Open Internet Order.* We seek comment on whether there are other categories of information that should be treated as falling under Section 222(a) in the broadband context, and for which customers and providers expect protection. Are there any categories of information that are specific to the mobile BIAS context?

41. We also seek comment on whether we should harmonize the existing CPNI rules with our proposed rules for broadband providers by adopting one unified definition of customer PI, and on the benefits and burdens of such an approach. We recognize that because the Commission has not previously focused its attention on adopting rules defining the scope of information protected by Section 222(a), our existing Section 222 rules do not separately define customer PI. Are voice telecommunications providers' obligations to protect customer PI sufficiently clear, or would it be helpful to have a codified definition? Further, we observe that many telecommunications carriers also provide both voice and broadband services. Would a harmonized standard help reduce burdens for such companies, especially for small providers?

6. Defining Personally Identifiable Information

42. Protecting personally identifiable information is at the heart of most privacy regimes. We propose to define personally identifiable information, or PII, as any information that is linked or linkable to an individual. We recognize that, historically, legal definitions of PII adopted different approaches. Some incorporated checklists of specific types of information; others deferred to auditing controls. Advances in computer science, however, have demonstrated that seemingly anonymous information can often (and easily) be re-associated with identified individuals. Our proposal incorporates this modern understanding of data privacy, which is reflected in our recent enforcement actions, and tracks the FTC and National Institute of Standards and Technology (NIST) guidelines on PII. We propose to define PII broadly because of both the interrelated nature

of different types of personal information and the large risks posed by unauthorized uses and disclosures. We seek comment on our proposal.

43. *Linked and linkable information.* We propose that information is ''linked'' or ''linkable'' to an individual if it can be used on its own, in context, or in combination to identify an individual or to logically associate with other information about a specific individual. The ''linked or linkable'' standard for determining the metes and bounds of personally identifiable information is well established. In addition to NIST 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. We seek comment on our approach.

44. We propose to offer illustrative, non-exhaustive guidance regarding the types of data that are PII. In order to provide such guidance, we look to a number of sources, including our prior orders, NIST, the FTC, the White House's proposed Consumer Privacy Bill of Rights, and other federal and state statutes and regulations. We propose that types of PII include, but are not limited to: Name; Social Security number; date and place of birth; mother's maiden name; unique government identification numbers (*e.g.,* driver's license, passport, taxpayer identification); physical address; email address or other online contact information; phone numbers; MAC address or other unique device identifiers; IP addresses; persistent online identifiers (*e.g.,* unique cookies); eponymous and non-eponymous online identities; account numbers and other account information, including account login information; Internet browsing history; traffic statistics; application usage data; current or historical geo-location; financial information (*e.g.,* account numbers, credit or debit card numbers, credit history); shopping records; medical and health information; the fact of a disability and any additional information about a customer's disability; biometric information; education information; employment information; information relating to family members; race; religion; sexual identity or orientation; other demographic information; and information identifying personally owned property (*e.g.,* license plates, device serial numbers). We recognize and acknowledge that several of these data elements may overlap with our proposed interpretation of the terms of the CPNI definition. We seek comment on these examples and whether there are other categories of linked or linkable information that we should recognize.

45. *Other PII Considerations.* Consistent with a widespread understanding of what constitutes PII, we propose to consider a BIAS customer's name, postal address, and telephone number as PII and, consequently, that they are customer PI protected by Section 222(a) in the broadband context. We recognize that because of the unique history of telephone directory information, the Commission has previously treated such information as not falling within the statutory definition of CPNI in the voice telephony context. Indeed, the statutory definition of CPNI ''does not include subscriber list information,'' which the Act defines as information ''(A) identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications . . . and (B) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format.''

46. Unlike fixed voice providers in the 1990s, today's broadband providers do not publish directories of customer information. Even in the voice context, mobile providers have never published subscriber list information, and in the fixed context, customers have long had the option to request such customer information not be disclosed (*i.e.,* that the customer be ''unlisted''), inherently recognizing the personal nature of such information. Further, by signing up for broadband service, customers do not think they are consenting to the public release of their name, postal address, and telephone number, none of which play the same role in the context of BIAS, as they do in the context of telephone service. As such, we propose that there is no subscriber list information in the broadband context, and therefore that BIAS customers' names, postal addresses, and telephone numbers should be treated as PII, and seek comment on our approach. We also seek comment on whether we should treat such information as CPNI. We also propose to harmonize our voice and broadband rules and treat such information as customer PI in the voice context, except where such information is published subscriber list information. We seek comment on this proposal. Do commenters agree that this approach is consistent with current customer expectations? What are the positive and negative ramifications from this proposal? Is there another approach we can take that will give consumers control over their personal information?

47. If we adopt rules harmonizing the privacy requirements of Sections 222, 631, and 338(i), how should we interpret the term ''personally identifiable information'' as used in Sections 631 and 338(i)? Should we use the same definition we propose here?

48. Finally, we seek comment on alternative approaches to defining PII. For example, instead of defining the term PII, what are the benefits and burdens of leaving that term undefined and simply providing guidance on what types of information qualify? What are the benefits and burdens any alternative approaches?

7. Content of Customer Communications

49. We seek comment on how we should define and treat the content of customer communications. The sensitivity and confidentiality of the content of personal communications is one of the oldest and most-established cornerstones of privacy law. Other federal and state laws, including the Electronic Communications Privacy Act (ECPA), the Communications Assistance for Law Enforcement Act (CALEA), and Section 705 of the Communications Act provide strong protections for the content of communications carried over broadband and public switched telephone networks. In light of the strong protections for the content of communications offered by other laws, we seek comment on how we should treat content under Section 222. As a threshold matter, should some or all forms of content should also be understood as customer PI under Section 222(a) or CPNI under Section 222(h)? What are the implications of considering content as being covered by Section 222(a) or (h), as well as by other relevant federal and state laws? We do not think that providers should ever use or share the content of communications that they carry on their network without having sought and received express, affirmative consent for the use and sharing of content. We therefore seek comment on whether there is a need to provide heightened privacy protections to content of communications beyond Section 705 and ECPA, and if there is, what additional protections should be provided. Given that Section 705 provides an additional basis for requiring heightened protections for content, should we consider regulations under Section 705? We invite commenters to address any legal authorities affecting commenters' conclusions regarding content, including relevant provisions of the

ECPA and Section 705 of the Communications Act.

8. Defining Opt-Out and Opt-In Approval

50. We propose to define the term ''opt-out approval'' as a method for obtaining customer consent to use, disclose, or permit access to the customer's proprietary information in 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 customer is provided appropriate notification of the BIAS provider's request for consent consistent with the proposed requirements set forth below in Section 64.7002 of the proposed rules. We base our proposal on the definition for ''opt-out approval'' in the Commission's existing CPNI rules. In the broadband context, we propose to expand the Commission's existing definition to encompass all customer PI (rather than limiting it to CPNI), and eliminate the existing 30-day waiting period currently required to make a voice customer's opt-out approval effective, as the existing definition of opt-out approval for voice providers requires. We believe that, given our proposed requirements that customers must be able to opt out at any time and with minimal effort, a 30-day period may prove more cumbersome than a customer's rapid expressions of preference. Since BIAS providers come into contact with many types of customer PI beyond CPNI in their provision of broadband services, we think it appropriate under Section 222(a) to include all customer PI so that customers can exercise more control over the use and sharing of all their private information.

51. We propose to define the term ''opt-in approval'' as a method for obtaining customer consent to use, disclose, or permit access to the customer's proprietary information that requires that the BIAS provider obtain from the customer affirmative, express consent allowing the requested usage, disclosure, or access to the covered information after the customer is provided appropriate notification of the provider's request consistent with the requirements set forth below in Section 64.7002 of the proposed rules and before any use of, disclosure of, or access to such information. We base our proposal on the definition for ''opt-in approval'' in the Commission's existing CPNI rules for voice providers.

52. We seek comment on these proposed definitions, and more specifically, whether there any changes to them that can be made to (1) adapt them more appropriately to the BIAS context, or (2) provide additional clarity for consumers and providers alike. We seek comment on alternative approaches to defining these terms. We invite commenters to offer real-world examples of choice-mechanisms and discuss whether they would satisfy these definitions.

9. Defining Communications-Related Services and Related Terms

53. We seek comment on how best to define ''communications-related services'' for purposes of our proposal to allow BIAS providers to use customer PI to market communications-related services to their subscribers, and to disclose customer PI to their communications-related affiliates for the purpose of marketing communications-related services subject to opt-out approval. Should we limit communications-related services to telecommunications, cable, and satellite services regulated by the Commission? If so, how should we treat services that compete directly with services that are subject to Commission jurisdiction? Alternatively, should we delineate other types of services that we would consider communications-related?

54. The current Section 222 rules define communications-related services to mean ''telecommunications services, information services typically provided by telecommunications carriers, and services related to the provision or maintenance of customer premises equipment.'' The current Section 222 rules define ''information services typically provided by telecommunications carriers'' to mean information services as defined in the Communication Act of 1934, as amended, that are typically provided by telecommunications carriers, such as Internet access or voice mail services. The definition further specifies that ''such phrase 'information services typically provided by telecommunications carriers,' as used in this subpart, shall not include retail consumer services provided using Internet Web sites (such as travel reservation services or mortgage lending services), whether or not such services may otherwise be considered to be information services.'' If used in the BIAS context the combination of those definitions would include a broad array of services. We are not inclined to adopt such an expansive reading of ''communications-related services,'' so we seek comment on how we might amend the current definitions to narrow the scope of services we would treat as ''communications-related services'' in the broadband context. We also seek comment on how we can best limit the definitions of ''communications-related services'' and, if necessary, ''information services typically provided by a telecommunications provider'' to align with consumer expectations about the extent to which BIAS providers use and share customer PI with communications-related affiliates.

55. Even if we adopt a narrower definition of communications-related services for purposes of the BIAS rules, we propose to amend the definition of ''information services typically provided by telecommunications carriers'' for purposes of the voice rules, in light of the reclassification of broadband Internet access service as a telecommunications service in the *2015 Open Internet Order,* and to align with current consumer expectations about the extent to which telecommunications carriers (other than BIAS providers) use and share customer PI with communications-related affiliates for purposes of marketing communications-related services. Should we harmonize the meaning of ''communications-related services'' across BIAS and other telecommunications services? Relatedly, we seek comment on what constitutes ''marketing'' for the purposes of this proposed rule.

10. Defining Aggregate Customer PI

56. We propose to define aggregate customer proprietary information as collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed. We observe that our proposed definition for ''aggregate customer proprietary information'' mirrors the statutory definition for the term ''aggregate customer information'' in Section 222(h)(2). We use slightly different terminology to make clear that our proposed rules addressing the use of aggregate customer information are intended to address the use of all aggregate customer PI and not just aggregate CPNI. We seek comment on our proposal. Are there any reasons we should restrict our definition to include only aggregate CPNI, or alternatively, to mirror the statute's terminology of ''aggregate customer information''? Do any additional security concerns arise from the use of aggregate customer PI, in the fixed or mobile context, that would not arise if our definition were restricted to including only CPNI? Would adopting the statutory term ''aggregate customer information'' lead to any enforcement concerns regarding what information is covered? Should our proposed definition of aggregate

customer PI apply to both voice telephony and BIAS services? Are there any reasons that the same definition of aggregate customer PI should not be used for both of these types of services?

11. Defining Breach

57. For purposes of our proposed data breach notification requirements, we propose to define ''breach'' as any instance in which ''a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information.'' Unlike the ''breach'' definition in our current Section 222 rules, our proposal does not include an intent element, and it covers all customer PI, not just CPNI. In defining breach we also look to state data breach notification laws, many of which do not include an intent requirement. We seek comment on this approach.

58. Not including a requirement that the unauthorized access be intentional in the definition of ''breach'' will ensure data breach notification in the case of inadvertent breaches that have potentially negative consequences for customers. We seek comment on this approach. Do commenters believe it is appropriate to require customer notification of all breaches, whether inadvertent or intentional? What are the burdens and benefits associated with this proposal? Should we retain the intentionality requirement in certain contexts? If so, what contexts and why? State statutes often include a provision exempting from the definition of breach a good-faith acquisition of covered data by an employee or agent of the company where such information is not used improperly or further disclosed. Should we include such an exemption in our definition of ''breach'' or is such a provision unnecessary or otherwise unadvisable? Are there any alternative proposals we should consider for the definition of breach?

59. We propose to include customer PI within the definition of breach, which will have the effect of applying our data breach notification requirements to breaches of customer proprietary information. Although CPNI covers many categories of confidential information, we believe that it is equally important that customers, the Commission, and other law enforcement (in certain circumstances) receive notice of a breach of other customer PI from or about the customer. Section 222(a) requires carriers to protect the confidentiality of ''proprietary information'' of and relating to customers. As such, we believe we have authority to extend our proposed breach reporting requirements to breaches of all customer PI, to ensure that customers receive critical protection for this broader subset of information. We seek comment on our proposal and on our authority to require breach reporting for breaches of all customer PI. What are the burdens and benefits of our proposed expansion of our requirements? How will our proposal affect small businesses?

12. Other Definitions

60. We seek comment on whether there are other terms we should define as part of adopting rules to protect the privacy of BIAS customers' proprietary information, or voice telecommunications definitions that we should revise in light of our proposals today.

61. For example, the existing CPNI rules define the term ''customer premises equipment'' (CPE) to mean ''equipment employed on the premises of a person (other than a carrier) to originate, route, or terminate telecommunications.'' We seek comment whether we should adopt this definition for purposes of the proposed broadband privacy rules. What would be the scope of covered devices under the statutory definition or any alternatives? Would ''premises of a person'' include Internet-connected devices carried outside one's home or office? With large numbers of consumer products becoming networked devices (*e.g.,* thermostats, cars, home appliances, and others), are there particular types of uses, activities, or devices that operate over broadband Internet access service that we should or should not include within the definition of CPE? Are there other terms the Commission should define for the broadband privacy context?

62. We also seek comment on whether there are any other terms from the existing CPNI rules that we need to revise, either to differentiate them or to harmonize them with our proposed broadband privacy rules, and to address the existing forbearance for BIAS. We propose to revise the existing rules to make clear that they apply only to telecommunications services other than BIAS, by revising the definition of ''telecommunications carrier'' to exclude a provider of BIAS for purposes of the existing rules. We seek comment on this approach, as well as alternative approaches for doing so. Are any other changes to the definitions necessary to preserve the existing voice CPNI rules following the reclassification of broadband Internet access service? What are the benefits and burdens of updating or not updating any of these definitions, particularly for small providers? With regard to all of the current definitions, should we merely update them and keep them applicable solely to voice services, or should we craft one uniform set of definitions for both voice and broadband CPNI? Is there any reason not to harmonize these or other definitions as applied to voice and broadband providers? What are the benefits and burdens of harmonizing versus not harmonizing the definitions, particularly for small providers?

63. We recognize that if we do update any definitions, we may need to revise other aspects of the current CPNI rules to align with any revised definitions. Likewise, if we revise any of the current substantive rules we may need to revise additional definitions. Below, we seek comment on harmonizing the current rules with our proposed rules. Here we also seek comment on what other provisions of the current CPNI rules we should revise and why. For example, our current rules permit wireless providers to ''use, disclose, or permit access to CPNI derived from its provision of CMRS, without customer approval, for the provision of CPE and information service(s).'' At the time of adoption, BIAS was classified as an ''information service,'' and as such, this rule was intended to cover such services. We seek comment on how we should revise this rule to reflect our reclassification of BIAS as a telecommunications service.

B. Providing Meaningful Notice of Privacy Policies

64. Transparency is one of the core fair information practice principles. Indeed, there is widespread agreement that companies should provide customers with clear, conspicuous, and understandable information about their privacy practices. There is also widespread agreement about the challenge of providing useful and accessible privacy disclosures to consumers. In recognition of the importance of transparency, we propose rules requiring BIAS providers to provide customers with clear and conspicuous notice of their privacy practices at the point of sale and on an on-going basis through a link on the provider's homepage, mobile application, and any functional equivalent. In order to ensure customers have the information they need about BIAS providers' privacy practices, we propose to provide specific direction about what information must be provided in BIAS providers' privacy notices, and we propose to require BIAS providers to provide existing customers with advanced notice of material changes in their privacy policies. To

ensure that the information that BIAS providers provide about their privacy policies is accessible to consumers, we seek comment on standardizing the formatting of broadband privacy notices and of notices regarding material changes to privacy policies. We also seek comment on ways to harmonize our proposed notice requirements with privacy notice requirements for providers of voice and video services.

1. Privacy Notice Requirements

65. In proposing specific disclosure requirements for BIAS providers' privacy and security policies, we look to the Commission's open Internet transparency rule and the existing notice obligations for traditional telecommunications carriers under Section 64.2008 of the Commission's rules, as well as the notice provisions of the Cable Privacy Act. We also look to the California Online Privacy Protection Act, which establishes privacy policy requirements for online services, and to numerous best practices regimes, including those proposed by the FTC and the National Telecommunications and Information Administration (NTIA). We also find various trade association recommendations informative, including those adopted by the Digital Advertising Alliance and the Network Advertising Initiative. In so doing, we propose rules that would impose the following notice requirements with respect to BIAS providers' privacy policies:

- *Types of Customer PI Collected and How They Are Used and Disclosed.* The notice must specify and describe:
  - The types of customer PI that the BIAS provider collects by virtue of its provision of broadband service;
  - How the BIAS provider uses, and under what circumstances it discloses, each type of customer PI that it collects; and
  - The categories of entities that will receive the customer PI from the BIAS provider and the purposes for which the customer PI will be used by each category of entities.
- *Customers' Rights With Respect to Their PI.* The notice must:
  - Advise customers of their opt-in and opt-out rights with respect to their own PI, and provide access to a simple, easy-to-access method for customers to provide or withdraw consent to use, disclose, or provide access to customer PI for purposes other than the provision of broadband services. Such method shall be persistently available and made available at no additional cost to the customer.
  - Explain that a denial of approval to use, disclose, or permit access to customer PI for purposes other than providing BIAS will not affect the provision of any services to which the customer subscribes. However, the provider may provide a brief description, in clear and neutral language, describing any consequences directly resulting from the lack of access to the customer PI.
  - Explain that any approval, denial, or withdrawal of approval for the use of the customer PI for any purposes other than providing BIAS is valid until the customer affirmatively revokes such approval or denial, and inform the customer of his or her right to deny or withdraw access to such PI at any time. However, the notification must also explain that the provider may be compelled to disclose a customer's PI, when such disclosure is provided for by other laws.
- *Requirements Intended to Increase Transparency of Privacy Notices.* To ensure customers can understand BIAS privacy notices, such notices must:
  - Be comprehensible and not misleading;
  - Be clearly legible, use sufficiently large type, and be displayed in an area so as to be readily apparent to the customer; and
  - Be completely translated into another language if any portion of the notice is translated into that language.
- *Timing of Notice.* To ensure customers receive timely and persistent notice of a BIAS provider's privacy policies, the notice must:
  - Be made available to prospective customers at the point of sale, prior to the purchase of BIAS, whether such purchase is being made in person, online, over the telephone, or via some other means;
  - Be made persistently available:
    - Via a link on the BIAS provider's homepage;
    - Through the BIAS provider's mobile application; and
    - Through any functional equivalent to the provider's homepage or mobile application.

66. We seek comment on these proposed notice requirements. To what extent are these practices already being followed by some or most BIAS providers? To what extent are these practices consistent with the best practices of other industries? Will the proposed requirements provide BIAS customers with (1) clear and adequate notice of their BIAS provider's privacy policies, and (2) sufficient information to enable them to make informed decisions about their use and purchase of BIAS services? Will the proposed requirements ensure that BIAS customers receive sufficient information to give them confidence that their broadband provider is protecting the confidentiality of their proprietary information and providing them with sufficient ability to decide whether and when to opt in to the sharing of data with third parties? Are there additional specific requirements that we should adopt so that privacy policy information is accessible to customers with a disability, such as, for example, a link to a video of the notice conveyed in American Sign Language (ASL)?

67. *Required Disclosures.* We seek comment whether there are other types of information that we should require BIAS providers to include in the notices of their privacy policies, or if there are any categories of information we propose including that should not be required. For example, should we require BIAS providers to provide customers with information concerning their data security practices or their policies concerning the retention and deletion of customer PI? Further, to the extent that we determine that the content of customer communications is covered by the transparency requirements we propose to adopt, how can we ensure that customers have adequate notice concerning how BIAS providers treat such information? In addition, would it be technically and/or practically feasible to require that BIAS providers provide consumers with notice of the specific entities with which they intend to share their customer PI, rather than the categories of entities, as we propose above? We note that California's Shine the Light law requires businesses, upon request, to provide to their customers, free of charge and within 30 days: (1) A list of the categories of personal information disclosed by the business to third parties for the third parties' marketing purposes; (2) the names and addresses of all the third parties that received personal information from the business in the preceding calendar year; and (3) if the nature of the third parties' business cannot be reasonably determined by the third parties' name, examples of the products or services marketed by the third party. We seek comment on whether we should adopt a similar requirement. Would such a requirement place too onerous a burden on BIAS providers? What are the estimated costs of compliance associated with such a requirement, if any? Are these costs outweighed by the potential benefit to customers of disclosing this information?

68. Although our current Section 222 rules do not require voice providers to have privacy notices, many of the categories of information we propose to

require in BIAS providers' privacy notices are required as part of the current Section 222 requirements for notice before seeking approval for using or sharing CPNI. We seek comment from providers and other stakeholders on their experience with privacy disclosures in that context and on how those experiences should inform the privacy notice rules we propose to adopt for BIAS providers.

69. *Timing and Placement of Privacy Notices.* We seek comment on our proposal regarding the timing and placement of privacy notices. We believe that by requiring point-of-sale notices and requiring that notices of a BIAS provider's privacy policies be persistently available through a link on the provider's homepage and through its mobile application, gives providers two existing, user-friendly avenues for providing customers with notice of their privacy policies, while also leaving open a technology-neutral, ''functional equivalent'' option in the event that future innovations in technology offer new and innovative ways to provide customers with transparency. Do commenters agree? Are homepages and mobile applications two platforms through which customers are likely to interface with privacy policies? Are there any other times and points at which providers should provide customers with notice of their privacy practices, other than those we discuss above? If so, how should such notice be delivered? Should it be provided through email or another agreed-upon means of electronic communication, or should it perhaps be included regularly on customers' bills for BIAS? What would be the cost of compliance, if any, of supplying customers with privacy practice notifications via email or as part of the customer's regular bill? Are there technical means of conveying privacy notices that we might adopt?

70. Some rules and laws require annual or bi-annual notification of privacy rights. The Commission's existing voice notification rules require carriers using the opt-out mechanism to provide notices to their customers every two years. Because we require BIAS providers to have easy-to-access links to their privacy notices that are persistently available on their homepage, through their mobile applications, and through any functional equivalent, we do not think it is a good use of resources to require BIAS providers to periodically provide their privacy notices to their customers. We invite comment on that approach. When customers receive regular privacy notices, do they typically review and understand such annual notices? Do customers typically take any action in regard to such notices? Would the administrative costs of providing such annual notices outweigh the benefits to the customer of receiving annual notices? If we do adopt a regular privacy notice requirement, how should the notice be sent to BIAS customers? Would email notice to the customer's email address of record be sufficient? Should we require that any such annual notices be sent by mail to the address of record? Is there another, more effective way of providing annual notices to BIAS customers?

71. *Compliance Burden.* We seek comment on the burdens associated with complying with our proposed privacy notice framework for BIAS providers. What are the estimated costs of compliance, if any, that this notice framework will impose on providers, given that they are already obligated to provide notice of their privacy policies to customers under the open Internet transparency rule? We believe that the benefits to customer privacy of providing end users, edge providers, and the general public with meaningful information about the privacy policies of BIAS providers outweigh the administrative and regulatory costs of the proposed notice requirements. We seek comment on this conclusion. Are there any alternatives that would reduce the burdens on BIAS providers, particularly small providers, while still ensuring that BIAS providers' privacy practices are sufficiently transparent?

72. *Standardization of Privacy Notices.* We also seek comment on whether BIAS providers' privacy policy notices should be standardized to enable better comprehension and comparison of privacy practices by customers and to reduce the burden of regulatory compliance on BIAS providers. There is broad recognition of the importance of simplifying and standardizing privacy notices to make them more accessible to consumers. In its 2012 Privacy Report, for example, the FTC recognized that privacy policies in different industries would need to reflect those differences, but called for the standardization of some elements of privacy policies, including formatting and terminology ''to allow consumers to compare the privacy practices of different companies and to encourage companies to compete on privacy.'' The following year, NTIA released a voluntary code of conduct detailing a uniform set of guidelines for mobile application providers to use in crafting short form privacy notices. In drafting the code, NTIA acknowledged that the ''transparency created by displaying information about application practices in a consistent way . . . is intended to help consumers compare and contrast data practices of apps.''

73. We seek comment on whether we should adopt a standardized approach for BIAS providers' privacy notices in this proceeding. Would a one-size-fits-all approach provide clear, conspicuous, and understandable information? Are there models we should look to in crafting our privacy notice requirements? For example, in the *2015 Open Internet Order,* we directed the Consumer Advisory Committee (CAC), composed of both industry and consumer interests, to formulate and submit to the Commission a proposed consumer-facing disclosure for purposes of complying with the transparency rule. Should we follow a similar approach? In a recent study of online privacy notices, researchers at Carnegie Mellon University found that certain, specific discrepancies exist between companies' actual privacy practices and users' expectations of how their information is being used or shared. The study concluded by suggesting that companies could develop shorter, user-facing privacy notices that specifically emphasize those practices where mismatches exist between a company's actual use and disclosure policies and consumers' expectations. By using models of people's privacy expectations, the study's authors suggest that companies could selectively highlight or display those elements of privacy policies that are likely to be most relevant to users. We seek comment on whether we should use such a model in developing a standardized template for privacy notices. Would such a model, or one similar to it, lessen the burden on providers of providing privacy notices while also ensuring that customers are kept adequately informed as to how their BIAS providers use and share their information? Or, should we consider multiple but structurally similar privacy policy disclosures?

74. In addition, we seek comment on whether such a standardized disclosure should be adopted as a voluntary safe harbor for any adopted privacy notice requirements. Would a safe harbor ease the regulatory burden on BIAS providers, particularly small providers? How could we ensure that a notice provided under such a safe harbor provision still allows consumers adequate opportunity to consider and comprehend the privacy policies of their respective BIAS providers?

75. We recognize that not all privacy policies may conform to a uniform template. Is there a risk that using a uniform template for privacy notices may result in the omission of crucial

information and ensuing consumer confusion or mistake? What is the best way to ensure that BIAS providers are able to convey this privacy policy information in accessible formats, like ASL? Are more general guidelines that allow for flexibility preferable to the creation of a uniform template? Should we, for example, look to the model code of conduct for mobile application short-form privacy notices that came out of the multi-stakeholder process convened by the NTIA at the Department of Commerce in 2012 and 2013? If so, what elements from that model will work well in the BIAS context and which will need to be adjusted?

76. Are there other approaches we can take to simplifying privacy notices? For example, should we require a layered privacy notice that includes a plain-language disclosure policy in addition to a more in-depth disclosure? If so, what should go into the different layers of such privacy notices?

77. In addition to simplifying and standardizing privacy notices, we seek comment on whether we should take further steps to ensure (1) that customers have access to sufficient information regarding their BIAS provider's privacy policies, and (2) that such information is presented in a form that is both palatable and easily comprehensible for customers. In particular, we seek comment on whether the Commission should require BIAS providers to create a consumer-facing privacy dashboard that would allow customers to: (1) See the types and categories of customer PI collected by BIAS providers; (2) see the categories of entities with whom that customer PI is shared; (3) grant or deny approval for the use or disclosure of customer PI; (4) see what privacy selection the customer has made (*i.e.,* whether the customer has chosen to opt in, opt out, or take no action at all with regards to the use or disclosure of her PI), and the consequences of this selection, including a description of what types and categories of customer PI may or may not be used or disclosed by a provider depending on the customer's privacy selection; (5) request correction of inaccurate customer PI; and (6) request deletion of any categories of customer PI that the customer no longer wants the BIAS provider to maintain (*e.g.,* online activity data), so long as such data is not necessary to provide the underlying broadband service or needed for purposes of law enforcement. We seek comment on the costs and benefits of requiring the creation of such a dashboard, and any alternatives the Commission should consider to minimize the burdens of such a program on small providers.

2. Providing Notice of Material Changes in BIAS Providers' Privacy Policies

78. In order to ensure that BIAS customers are fully informed of their providers' privacy policies, and can exercise informed decisions about consenting to the use or sharing of customer PI, we propose to require BIAS providers to (1) notify their existing customers in advance of any material changes in the BIAS provider's privacy policies, and (2) include specific types of information within these notices of material changes. Our proposal is consistent with, but more extensive than, the requirement we adopted in the *2015 Open Internet Order* that BIAS providers update the disclosure of their network practices, performance characteristics, and commercial terms (including privacy practices) whenever there is a material change in that disclosure. More specifically, we propose that a notice of material changes must:

- Be clearly and conspicuously provided through (1) email or another electronic means of communication agreed upon by the customer and BIAS provider, (2) on customers' bills for BIAS, and (3) via a link on the BIAS provider's homepage, mobile application, and any functional equivalent.
- Provide a clear, conspicuous, and comprehensible explanation of:
  - The changes made to the BIAS provider's privacy policies, including any changes to what customer PI the BIAS provider collects, and how it uses, discloses, or permits access to such information;
  - The extent to which the customer has a right to disapprove such uses, disclosures, or access to such information and to deny or withdraw access to the customer PI at any time; and
  - The precise steps the customer must take in order to grant or deny access to the customer's PI. The notice must clearly explain that a denial of approval will not affect the provision of any services to which the customer subscribes. However, the provider may provide a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to the customer's PI. If accurate, a provider may also explain in the notice that the customer's approval to use the customer's PI may enhance the provider's ability to offer products and services tailored to the customer's needs.
- Explain that any approval or denial of approval for the use of customer PI for purposes other than providing BIAS is valid until the customer affirmatively revokes such approval or denial.
- Be comprehensible and not misleading.
- Be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to customers.
- Have all portions of the notice translated into another language if any portion of the notice is translated into that language.

79. We seek comment on our proposal. In particular, we seek comment on whether the elements and disclosures that we propose to require as part of the notification of material changes are sufficient to provide customers with adequate and comprehensible notice of any material changes in their BIAS providers' privacy policies. Are there any additional disclosures not included in this proposed framework that might be helpful to consumers? Are any of the proposed requirements unnecessary or potentially unhelpful to consumers? Should we require that the notification triggered by this proposed provision occur within a specified timeframe in advance of the effectiveness of the provider's material change? If so, what is an appropriate timeframe during which BIAS providers should provide the notification? The *2015 Open Internet Order* defined a ''material'' change as ''any change that a reasonable consumer or edge provider would consider important to their decisions on their choice of provider, service, or application.'' Do we need to update this definition to more clearly address privacy concerns raised by material changes?

80. Our proposal is consistent with industry guidelines and other standards regarding customer notice of material changes to privacy policies. Our proposed rules build on these existing regulatory frameworks and our own existing material change disclosure requirement in an attempt to ensure that customers receive proper notice of any material changes in their BIAS providers' privacy policies that may affect how those customers' PI is used or disseminated, *before* such material changes are made. We believe that by requiring BIAS providers to furnish their customers with advance notice of material changes to their privacy policies, our proposed requirement will help to ensure that the manner in which customer PI is being used and disclosed will remain transparent to customers, and will also enable customers to make informed decisions about whether to

approve or disapprove any new uses or disclosures of their PI.

81. We believe that our proposal will also help to ensure that BIAS providers cannot materially alter their privacy practices and use or share customer PI in a way in which customers may not approve or may not envision prior to customers even being made aware of such an alteration in the first place. Further, our proposed requirements that notices of material changes be clearly legible, placed in an area so as to be readily apparent to customers, and be provided through email or another electronic means of communication agreed upon by the customer and BIAS provider—as well as on customers' bills for BIAS services and through a link on the BIAS provider's homepage, mobile app, and any functional equivalent—will help ensure that customers have ample opportunity to learn of any material changes in their BIAS providers' privacy practices. This will also have the added benefit of informing interested members of the public, including privacy advocates, of any such material changes.

82. We are particularly concerned about material changes to privacy policies that BIAS providers seek to make retroactive. Our sister agency, the FTC, has also long held as a ''bedrock principle'' that companies should obtain affirmative express consent before making material retroactive changes to their privacy policies. This principle is echoed in the Organization for Economic Cooperation and Development's privacy guidelines, which require that data controllers specify the purpose of data use whenever those purposes change. We seek comment on whether our proposed rules are sufficient to ensure that providers seeking to retroactively change their privacy policies obtain consent to any new or newly disclosed use or sharing of customer PI, and that they honor consumers' decisions.

83. Finally, we seek comment on the burden that our proposed material change notice requirements will place on BIAS providers, particularly small providers. What are the estimated costs of compliance, if any, that this framework will impose on BIAS providers? Is there any way to modify our proposed material change rules so as to lessen the burden of these requirements on small providers while still achieving the Commission's stated goals of increasing transparency in the BIAS market and keeping consumers well-informed of their BIAS providers' privacy practices?

3. Mobile-Specific Considerations

84. As a general matter, we do not see a justification for treating fixed and mobile BIAS differently. However, we understand that there are fundamental differences between the two technologies: Specifically, their mobility. We therefore seek comment on whether there are any mobile-specific considerations to the notice requirements we have proposed above. Given the increasing ubiquity of mobile devices in today's society, we recognize that many consumers may utilize BIAS via a mobile platform—some to the exclusion of fixed devices. We seek comment on the technical feasibility of our proposed notice requirements for mobile BIAS providers. Are there any practical difficulties for providers of mobile BIAS in providing customers with adequate notice? For instance, are there any ways in which our existing and proposed notice requirements can or should be tailored to the unique characteristics of mobile services and smaller screens? Are our existing and proposed methods of notice adequate to ensure that mobile customers, specifically, are kept well-informed of their providers' respective privacy policies, as well as any material changes to such policies? What other types of notice, if any, should be required, specific to mobile BIAS providers? Is there any reason to hold mobile BIAS providers to different notice requirements, or should they be obligated to comply with the same framework as non-mobile BIAS providers? Why or why not? How would any such mobile-specific requirements benefit users of mobile BIAS? What would be the effect, if any, on broadband competition from having a different set of notice requirements applicable to mobile versus fixed BIAS providers?

4. Harmonizing Notices for Voice, Video, and Broadband Services

85. We seek comment on whether the Commission should harmonize required privacy notices regarding the use of customer information for voice, video, and broadband services. Section 64.2008 of the Commission's rules requires telecommunications carriers to provide individual notice to customers when soliciting approval to use, disclose, or permit access to customers' CPNI. Additionally, Sections 631 and 338(i) of the Act require cable operators and satellite carriers to provide notice to their subscribers of the collection, use, and disclosure of subscribers' personally identifiable information. This notice must be provided at the point of sale and at least once a year thereafter. We seek comment on the best way to harmonize privacy notice requirements for providers of voice, video, and broadband Internet access services.

86. We observe that in today's market of bundled communications services, many voice, broadband, and video providers offer multiple services. Indeed, many companies currently offer double or triple play packages that typically include both BIAS and video services, or BIAS, video, and voice services, respectively. In a variety of proceedings, the Commission has recognized the nexus between providing broadband and ''triple play'' packages that include other services such as video programming, and we have acknowledged that '' 'a provider's ability to offer video service and to deploy broadband networks are linked intrinsically, and the federal goals of enhanced cable competition and rapid broadband deployment are interrelated.' '' In light of the pre-existing notice requirements for providers of voice and video services, we seek comment on how we can minimize the burden of the notification processes proposed in this NPRM on BIAS providers.

87. We observe that some BIAS providers already provide one privacy notice for all of their bundled services on their Web sites. Given that many providers are already providing a single notice of their privacy policies on their Web sites to all their voice, video, and BIAS customers, we seek comment on whether harmonizing the privacy notice requirements for these various types of services could lessen the burden imposed on providers. More specifically, if a BIAS provider also provides privacy notices to customers under our voice rules and/or cable and satellite statutory requirements, should we allow that provider to combine the notices so that their customers only receive one notice as opposed to two or three? Should we reconcile the types of information that are required to be in consumer privacy notices across voice, video, and broadband Internet access platforms so that a provider of these services need only send a single notice to customers regarding its privacy practices? Is combining such notices likely to confuse customers? Will requiring separate privacy notices for voice, video, and broadband Internet access services be more easily understood by customers? Do the administrative costs of providing separate notices under the proposed rules as well as our voice and video rules outweigh any benefits to

consumers of receiving these notices separately?

C. Customer Approval Requirements for the Use and Disclosure of Customer PI

88. In this section, we propose a framework that empowers customers to make informed decisions about the extent to which they will allow their BIAS providers to use, disclose, or permit access to customer proprietary information for purposes other than providing BIAS. Choice is a critical component of protecting the confidentiality of customer proprietary information. When armed with clear, truthful, and complete notice of how their information is being used, customers can still only protect their privacy if they have the ability to exercise their privacy choices in a meaningful way. Empowering customers with control over their information does not, however, mean prohibiting all uses of their information, or bombarding them with constant solicitations for approval. BIAS providers may make many beneficial uses and disclosures of customer PI, and we do not propose to prevent these, so long as customers can exercise their choice in the matter. We therefore offer a proposed consumer choice framework that allows BIAS providers to engage in certain necessary and beneficial uses and sharing of information without the need for additional customer approval (such as providing service itself, or facilitating emergency response to 911 calls), as well as an efficient means of facilitating customer decisions regarding BIAS provider use and sharing of customer PI.

89. We begin this section by addressing the types of customer approval we propose to require for BIAS providers to use customer PI, and for BIAS providers to disclose customer PI to their affiliates and third parties. Section 222 and our current CPNI rules provide different levels of customer approval depending on the type of uses and the user, and we propose to do the same here. Specifically, we propose to require BIAS providers to give a customer the opportunity to opt out of the use or sharing of her customer PI prior to the BIAS provider (1) using the customer's PI to market other communications-related services to the customer; or (2) sharing the customer's PI with affiliates that provide communications-related services, in order to market those communications-related services to the customer. We also propose to require BIAS providers to solicit and receive opt-in approval from a customer before using customer PI for other purposes and before disclosing customer PI to (1) affiliates that do not provide communications-related services and (2) all non-affiliate third parties. We also seek comment on other approaches to seeking customer approval.

90. Second, we propose and seek comment on when BIAS providers should notify customers of their opportunities to approve or disapprove the use or disclosure of their information; the forms that such notification and solicitation should take, including how customers should be able to exercise their approval or disapproval; and how and when customers' choices take effect. Third, we propose and seek comment on how BIAS providers should document their compliance with the proposed rules. Fourth, we seek comment on the applicability of these proposals to small BIAS providers. Fifth, recognizing that the framework proposed here differs from the current framework in place for voice providers, we seek comment on whether we should harmonize the two frameworks, or otherwise revise and modernize the existing voice framework. We also seek comment on harmonizing the approval requirements for cable and satellite providers under Sections 631 and 338(i) of the Act with those we propose for BIAS providers.

1. Types of Approval Required for Use and Disclosure of Customer PI

91. In this section, we propose rules addressing the type of customer approval required for the use and sharing of customer PI. Customers' privacy is affected differently depending upon the entity using or accessing their private information and the purposes for which that information is being used. Each of these factors can independently affect the privacy impact of a given practice. For instance, customers who would not object to their BIAS provider using information about their bandwidth use to market a different monthly plan may object to that same information being disclosed to third parties. Meanwhile, customers may object even to uses of the same information for unexpected purposes, such as marketing wholly unrelated services to the customer. We therefore propose a framework to take these factors into account. We welcome comment on this approach.

92. Below, we first address uses and disclosure that do not require approval, or for which we propose to treat customer approval as implied. We then address the circumstances under which we propose to require customer opt-out and opt-in approval for the use and disclosure of customer PI. Finally, we seek comment on alternative frameworks for customer choice.

a. Permissible Uses and Disclosures of Customer PI for Which Customer Approval Is Implied or Unnecessary

93. In this section, we seek comment on how to implement Section 222(c)(1)'s direction that broadband providers may use, disclose, or permit access to individually identifiable CPNI without customer approval in their provision of BIAS or ''services necessary to, or used in, the provision'' of BIAS. We also propose to implement the goals of the statutory exceptions found in Section 222(d)—which permit BIAS providers to use, disclose, or permit access to CPNI without customer approval in specifically enumerated circumstances—to all customer PI in the broadband context, and below, propose rules that adapt those provisions to BIAS. We believe that our proposed implementation of these provisions in the broadband context is consistent with customer expectations, necessary for the efficient delivery of BIAS, and essential to allow emergency and law enforcement personnel to respond quickly and effectively during those times when their services are needed the most.

94. *Services for Which Consent to the Use of Customer PI Is Implied.* Section 222(c)(1) permits a BIAS provider to ''use, disclose, or permit access to individually identifiable [CPNI] in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service.'' We seek comment on how to apply this in the broadband context. In particular, how should we interpret the scope of activities that are ''in the provision'' of BIAS? We also seek comment on how we should interpret the clause ''services necessary to, or used in, the provision'' of broadband service in the BIAS context.

95. We propose to allow BIAS providers to use any customer PI, and not only CPNI, for the purpose of providing BIAS or services necessary to, or used in, the provision of BIAS. Is such a permissive expansion consistent with Congress' direction that telecommunications carriers ''protect the confidentiality of proprietary information of, and relating to . . . customers''? Why or why not? Is it necessary for BIAS providers to use customer PI other than CPNI to provide BIAS? We also note that Section 222(c)(1) does not restrict uses or disclosures of CPNI that are ''required by law,'' and seek comment whether our

rules need to explicitly recognize that BIAS providers may disclose any customer PI as required by law, including information that is not specifically CPNI.

96. We also propose to adopt rules permitting BIAS providers to use customer PI for the purpose of marketing additional BIAS offerings in the same category of service (*e.g.,* fixed or mobile BIAS) to the customer, when the customer already subscribes to that category of service from the same provider without providing the opportunity to provide opt-out or opt-in consent. We observe that the current Section 222 rules permit carriers to ''use, disclose, or permit access to CPNI for the purpose of . . . marketing service offerings among the categories of service (*i.e.,* local, interexchange, and commercial mobile radio service (CMRS)) to which the customer already subscribes from the same carrier, without customer approval.'' Given the additional types of customer PI and CPNI available to BIAS providers today, and the ways such information may impact the privacy of customers, will permitting BIAS providers to use customer PI for their own BIAS marketing purposes without explicit customer approval adequately protect customer privacy in the broadband context? Are there some forms of customer PI that a BIAS provider should not be permitted to use in this context without receiving additional consent from its subscribers? As discussed above, if we find that Section 222 provides protections for the content of communications, we think that use of content should be subject to heightened approval requirements. What sort of requirements should we apply to a provider's use of content for purposes of marketing BIAS to an existing BIAS customer? We also seek comment whether (1) permitting broadband providers to use customer PI to market broadband services to the customers in this manner is within the bounds of authority contemplated by the statute, and (2) whether we should revise our existing Section 222 rules to limit the exception to ''use'' of CPNI, or otherwise revise our rules.

97. *Statutory Exceptions.* Under Section 222(d) of the Act, providers may use, disclose, or permit access to CPNI, without customer notice or approval, to: (1) Initiate, render, bill, and collect for broadband services; (2) protect the rights or property of the provider, or to protect users and other providers from fraudulent, abusive, or unlawful use of, or subscription to, broadband services; (3) provide any inbound telemarketing, referral, or administrative services to the customer for the duration of a call, if such call was initiated by the customer and the customer approves of the use of such information to provide service; and (4) provide call location information concerning the user of a commercial mobile radio service or an IP-enabled voice service in certain specified emergency situations. We propose to adopt these exceptions, tailored to the broadband context, to the use or disclosure of all customer PI. We seek comment on our proposal and on potential alternatives.

98. Section 222(d)(4) permits providers to use and disclose CPNI to provide ''call location information'' concerning the user of a commercial mobile service for public safety. We believe that the critical public safety purposes that underlie this provision counsel in favor of applying a similar rule in the broadband context, and that providing customer PI to emergency services, to immediate family members in case of emergency, or to providers of information or database management services for the delivery of emergency services, are uses for which customer approval is implied. We therefore propose to allow BIAS providers to use or disclose any geo-location information, or other customer PI, for these purposes. We also propose to permit BIAS providers to use or disclose location information to support Public Safety Answering Point (PSAP) queries pursuant to the full range of next generation 911 (NG911) calling alternatives, including voice, text, video, and data, in addition to the circumstances delineated by statute. Our proposal will help ensure that PSAPs and emergency personnel have timely access to the full set of information they may need to respond quickly and effectively to locate and aid not only users of legacy voice services, but users of data, video, and text services as well. We also seek comment whether BIAS providers must support automated requests from PSAPs, to ensure that emergency response is not hampered by time-consuming or inefficient processes for necessary information. We seek comment on our proposed application of this statutory provision in the broadband context and on potential alternative approaches to the Section 222(d)(4) exception. Alternatively, we seek comment whether we could directly apply the provisions of Section 222(d)(4) to BIAS, by interpreting ''call location information'' to mean ''broadband usage location information.''

99. In addition, we propose to interpret Section 222(d)(2) to permit BIAS providers to use or disclose CPNI whenever reasonably necessary to protect themselves or others from cyber security threats or vulnerabilities. Section 222(d)(2) permits providers to use 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. We believe that this proposal comports with the statute, because cyber security threats and vulnerabilities frequently harm the rights or property of providers, and typically harm users of those services and other carriers through the fraudulent, abusive, or unlawful use of, or subscription to, such services. Furthermore, we note that other statutes explicitly permit particular types of disclosure, which may encompass customer PI. We seek comment on this proposal. Should we extend this exception to include all customer PI? What, if any, guidance should we provide about what constitutes a cybersecurity threat entitled to this exception?

100. We also propose to interpret Section 222(d)(2) to allow telecommunications carriers to use or disclose calling party phone numbers, including phone numbers being spoofed by callers, without additional customer consent when doing so will help protect customers from abusive, fraudulent or unlawful robocalls. Month after month, unwanted voice robocalls and texts (together, ''robocalls'') top the list of consumer complaints we receive at the Commission. At best, robocalls represent an annoyance; at worst they can lead to abuse and fraud. All concerned parties—regulators, providers, and consumer advocates—agree that better call blocking and filtering solutions are critical to helping consumers. To that end, we recently clarified that voice providers may offer their customers call blocking solutions without violating their call completion requirements, and encouraged providers to offer those solutions. We expect that sharing of calling party information to prevent robocalls will benefit consumers. We seek comment on this proposal, and on how well it fits within the framework of 222(d)(2). Is it consistent with customer expectations?

101. We also seek comment on what other customer PI telecommunications carriers, including interconnected VoIP providers, should be allowed to use or share without additional consumer consent pursuant to Section 222(d)(2) in order to prevent abusive, fraudulent, or unlawful robocalls. What other types of customer PI could help prevent robocalls, if shared with other providers and third party robocall solution

providers? Are BIAS or other providers already using or sharing some types of customer PI to mitigate the propagation of traffic that is fraudulent, abusive, or unlawful? If so, are there lessons that can be learned about the use or sharing of information that will assist in the fight against robocalls?

102. We also seek comment on whether we should expand the exceptions in Section 222(d) in the broadband context to permit broadband providers to use all customer PI for these delineated purposes. Is there any reason why providers would need to use customer PI that is not CPNI for the purposes Congress enumerated? If so, would such needs be outweighed by the countervailing interest in protecting the privacy of customer information?

103. Finally, consistent with our findings in the voice context, we propose to permit broadband providers to use CPNI without customer approval in the provision of inside wiring installation, maintenance, and repair services. We seek comment on this proposal, and specifically whether commenters believe there is any reason not to apply this provision in the broadband context. We also seek comment whether we should establish any other exceptions to our proposed framework. For instance, the existing CPNI rules permit providers to use or disclose information for the limited purpose of conducting research on the health effects of CMRS. Should a similar exception apply in the BIAS context? We encourage commenters to identify why any such exceptions would be consistent with Section 222 or other applicable laws.

b. Customer Approval Required for Use and Disclosure of Customer PI for Marketing Communications-Related Services

104. FTC best practices counsel that consumer choice turns on the extent to which the practice is consistent with the context of the transaction or the consumer's existing relationship with the business. Consistent with this and our existing rules, we propose that, except as permitted above in Part III.C.1.a, BIAS providers must provide a customer with notice and the opportunity to opt out before they may use that customer's PI, or share such information with an affiliate that provides communications-related services, to market communications-related services to that customer. We seek comment on this proposal.

105. This approach is similar to the approach taken by our current Section 222 rules, and we believe it is consistent with customers' expectations. However, we invite comment on this approach, specifically on customers' expectations and preferences regarding how their broadband provider may itself use customer PI; and for what purposes it should be allowed to share information with its affiliates subject to opt-out approval. Given the prevalence of bundled service offerings, do customers expect that their broadband providers could or should themselves use or share the customers' proprietary information with affiliates to market voice, video, or any types of communications-related services tailored to their needs and preferences without their express or implied approval? Or would customers prefer and expect to have their customer PI used or shared with affiliates only after the customers have affirmatively consented to such use or sharing? Do customers' expectations depend as much on the type of customer PI that is being shared as with the purpose of the sharing or the parties with whom the information is being shared? For example, below, we seek comment on whether we should require heightened consent obligations for highly sensitive information, including geo-location information.

106. We are mindful that in adopting a framework for customer approval for use by and disclosure to affiliates of customer PI, we do not want to inadvertently encourage corporate restructuring or gamesmanship driven by an interest in enabling use or sharing of customer PI subject to less stringent customer approval requirements. We believe that we can discourage such gamesmanship by treating use by an affiliate as subject to the same limits as use by a BIAS provider. We seek comment on this proposal. We also seek comment on what effect our proposed choice requirements will have on marketing of broadband and related services, as well as on the digital advertising industry. What effect will they have on competition between BIAS providers and over-the-top (OTT) service providers that offer services that may be a competitive threat or a potential competitor to separate voice, video, or information services offered by broadband providers, and which are not subject to our rules?

107. We also observe that in adopting the existing Section 222 rules for the sharing of CPNI with affiliates, the Commission concluded that because principles of agency law hold carriers responsible for their agents' improper uses or disclosures of CPNI, carriers have greater incentives to maintain appropriate control of CPNI disclosed to agents. The Commission concluded that an opt-out regime for the sharing of CPNI with affiliates that offer communications-related services for purposes of marketing such services would adequately protect consumers' privacy because a carrier's need to maintain a continuing relationship with its customer, and the risk of being held responsible for the misuse of customer information by an affiliate, would incentivize the carrier to prevent privacy harms. We believe such findings to be relevant in the broadband context as well, and seek comment on whether such findings are applicable to BIAS. Do consumers have a different expectation of privacy when it comes to BIAS, as opposed to voice, affiliates? Does the changing nature of affiliate relationships require more caution in the BIAS context than the voice context?

108. Alternatively, we seek comment whether we should require BIAS providers to obtain customer opt-in approval for the use and sharing of all customer PI, except as described in Part III.C.1.a. Would such an approach be ''narrowly tailored'' to materially advance the government's interest under *Central Hudson*? Conversely, would a requirement of opt-out approval be more appropriate for *all* BIAS provider uses of customer PI and sharing with affiliates? Should we adopt the FTC's recommendation that affiliates generally be treated as ''third parties . . . unless the affiliate relationship is clear to consumers''? If so, how would we determine if the relationship is clear to consumers? Would co-branding suffice? We also seek comment on whether we should treat all affiliates as third parties, that is, requiring opt-in consent from customers for any sharing with any affiliates. Would such a rule be properly tailored to meet the substantial interest in protecting customer privacy? Would it promote gamesmanship in the corporate structure of BIAS providers? We also seek comment on how we should treat third parties acting as contractors and performing functions for or on behalf of a BIAS provider. Should they be treated differently than other types of third parties?

c. Customer Approval Required for Use and Disclosure of Customer PI for All Other Purposes

109. Consistent with the existing voice rules and other privacy frameworks, we propose to require BIAS providers to seek and receive opt-in approval from their customers before using or sharing customer PI for all uses and sharing other than those described above in Parts III.C.1.a and III.C.1.b. Specifically, we propose to require BIAS providers to obtain customer opt-in approval before (1) using customer PI

for purposes other than marketing communications-related service; (2) sharing customer PI with affiliates providing communications-related services for purposes other than marketing those communications-related services; and (3) sharing customer PI with all other affiliates and third parties. Consistent with the Commission's existing rules, we include joint venture partners and independent contractors within the category of ''third parties'' for purposes of our proposed rules. We believe that customers desire and expect the opportunity to affirmatively choose how their information is used for purposes other than marketing communications-related services by their provider and its affiliates. We seek comment on this proposal and on potential alternatives to these requirements.

110. *BIAS Providers and Affiliates.* We seek comment whether BIAS providers need or benefit from using customer PI for purposes other than marketing communications-related services. If so, what are those uses, and are they consistent with customer expectations? What are the privacy risks for customers from those additional uses? We observe that many companies can meet the Act's definition of ''affiliate'' while bearing little resemblance—in the services offered, or even in their name—to what customers recognize as their provider. This, combined with lack of competition between BIAS providers and with high switching costs, could negatively impact BIAS providers' incentives in protecting the customer-carrier relationship with respect to use and disclosure of customer PI to affiliates. Does obtaining opt-in permission for these uses or disclosures prevent BIAS providers or consumers from making valuable use of this information? Does our proposed approach align with customer expectations of how their PI should be treated by their BIAS provider and the provider's affiliates? Should opt-in consent be required for disclosure or use of certain customer PI in the mobile context? Most notably, should we require opt-in consent in the mobile context for sharing geo-location data with affiliates, regardless of whether it is required in the fixed context? Does this proposal accommodate the expanded scope of uses and services now provided by BIAS affiliates and others, particularly given the above-noted concerns about the breadth of affiliates in today's BIAS environment?

111. *Third Parties.* The Commission has a substantial government interest in protecting the privacy of customer information, and our proposal is designed to materially advance that interest. Research demonstrates that customers view the use of their personal information by their broadband provider differently than disclosure to or use by a third party for a variety of reasons. More recently, studies from the Pew Research Center show that the vast majority of adults deem it important to control who can get information about them. Increasing the number of entities that have access to customer PI logically increases the risk of unauthorized disclosure by both insiders and computer intrusion. Risk of harm to the customer is exacerbated by the fact that third-party entities receiving customer information have no direct business relationship with the consumer and, hence, a reduced or absent incentive to honor the privacy expectations of those customers. As the Commission has found in the voice context, once confidential customer information ''enters the stream of commerce, consumers are without meaningful recourse to limit further access to, or disclosure of, that personal information.'' We anticipate that this is equally true for other forms of customer PI.

112. For these reasons, and because the use of customers' personal information might fall outside the protections of Section 222 once that information is disclosed to third parties, we believe that the threat to broadband customers' privacy interest from having their personal information disclosed to such entities without their affirmative approval is a substantial one, and there is a greater need to ensure express consent from an approval mechanism for third party disclosure. We seek comment on this analysis, and in particular, the threat to broadband customers' privacy stemming from disclosure of customer information to third parties.

113. We seek comment on the burdens that the proposed opt-in framework for disclosure to third parties would impose on broadband providers. Are such costs outweighed by the providers' duty to protect their customers' private information and customers' interest in maintaining control over their private information? We note that our current voice rules require opt-in approval for disclosure to most third parties. Further, some state laws also require customer permission for ISPs to disclose information if the disclosure is not in the ordinary course of the ISP's business. We also seek comment on the effect that our proposal will have on small providers.

114. We seek comment on what effect, if any, our proposed opt-in approval framework will have on marketing in the broadband ecosystem, over-the-top providers of competing services, the larger Internet ecosystem, and the digital advertising industry. We recognize that edge providers, who may have access to some similar customer PI, are not subject to the same regulatory framework, and that this regulatory disparity could have competitive ripple effects. However, we believe this circumstance is mitigated by three important factors. First, the FTC actively enforces the prohibitions in its organic statute against unfair and deceptive practices against companies in the broadband ecosystem that are within its jurisdiction and that are engaged in practices that violate customers' privacy expectations. We have no doubt that the FTC will continue its robust privacy enforcement practice. Second, the industry has developed guidelines recommending obtaining express consent before sharing some sensitive information, particularly geo-location information, with third parties, and large edge providers are increasingly adopting opt-in regimes for sharing of some types of sensitive information. Third, edge providers only have direct access to the information that customers choose to share with them by virtue of engaging their services; in contrast, broadband providers have direct access to potentially *all* customer information, including such information that is not directed at the broadband provider itself to enable use of the service. We seek comment on these expectations. Do commenters agree that these factors mitigate any potential competitive effects that might result from our proposed opt-in framework for disclosure of customer PI to third parties? What other factors counsel for or against it?

115. *Alternatives.* In the alternative, we seek comment whether an opt-out approval framework would be more appropriate for BIAS providers' (and their affiliates') use of customer PI for purposes other than marketing communications-related services, and for disclosure of customer PI to third parties, or for some subset of such activities. Are there reasons why such uses and disclosures of customer PI—or some subset of disclosures—should be subject to a more lenient standard of consent, such as opt-out approval? Why or why not? Would opt-out approval be an effective means of protecting customers from the harms that are attendant upon unknowing and unwanted third party disclosures, or from unexpected uses of their customer PI by their broadband providers? If so,

are there particular types of uses, data, or third parties for which a heightened standard of approval should be required?

d. Other Choice Frameworks

116. We have sought comment on one framework for approaching the types of control to give consumers over their customer PI. We also invite commenters to propose other frameworks for ensuring that broadband customers are given the ability to control the use and disclosure of their confidential information.

117. Are there other ways of differentiating between expected and unexpected uses and contexts for BIAS provider use of customers' PI that would be more useful? How should different types and contexts of information and usage be assigned different levels of required approval? Given the various types of information at issue, is there the risk that customers could be overwhelmed by choice and allow default options to stand? Would this militate towards requiring opt-in approval for more types of information? What approach, if any, best balances consumer benefits with minimizing regulatory burdens on broadband providers?

118. In particular, we seek comment whether certain types of ''highly sensitive'' customer information should be used by BIAS providers, even for the provision of the service, or shared with their affiliates offering communications-related services, only after receiving opt-in approval from customers. For example, the FTC has recognized certain types of information as particularly sensitive, including Social Security numbers and financial information, geo-location information, children's information, and health information. Given the highly sensitive nature of such information, customers may have an interest in ensuring that such data is not used without their prior, affirmative authorization. We seek comment on these issues. For example, location-based information—particularly mobile geo-location data—that reveals a customer's residence or current location is particularly sensitive in nature, and consumers may have a keen interest in safeguarding such data out of concerns for both safety and basic privacy. In the voice context, Congress recognized that use of ''call location information'' should not be used or disclosed without the ''express prior authorization of the customer.'' How should we consider treatment of location information in the broadband context? Likewise, we seek comment on what steps we could take to ensure knowing consent regarding the customer PI of children. Are there other types of information that we should treat as highly-sensitive and subject to opt-in protection? For example, should practices that involve using or sharing a customer's race or ethnicity, or other demographic information about a customer be subject to heightened privacy protections? Are there any types of information that BIAS providers should never use for purposes other than providing BIAS services?

119. We also seek comment on how to treat the content of communication, if we determine that it is covered by Section 222. The content of communications contain a wide variety of highly personal and sensitive information. Congress has also recognized that content of communications should be protected in all but the most exceptional circumstances. In addition to personal privacy implications, provider use of communications content raises competitive issues. A broadband provider may be able to glean competitively sensitive information from the contents of customers' communications. Would such conduct be prohibited under the Commission's general conduct rule prohibiting carriers from unreasonably interfering with or unreasonably disadvantaging end users' ability to select, access, and use broadband Internet access service or the lawful Internet content applications, services, or devices of their choice? We seek comment on whether the use or sharing, including with affiliates, of the content of customer communications should be subject to opt-in approval. We also seek comment on other approaches to the use of the content of customer communications, including how such approaches interact with our treatment of other types of information covered by Section 222.

120. Finally, we seek comment whether customers expect their BIAS providers to treat their PI differently depending on how the provider acquires it, and whether BIAS providers do and should treat such information differently. Should a broadband provider obtain some form of consumer consent before combining data acquired from third-parties with information it obtained by virtue of providing the broadband service?

2. Requirements for Soliciting Customer Opt-Out and Opt-In Approval

121. In this section, we seek comment on the appropriate procedures and practices for BIAS providers to obtain meaningful customer approval for the use or disclosure of customer PI. To that end, we first propose to require BIAS providers to solicit customer approval the first time that a BIAS provider intends to use or disclose the customer's PI in a manner that requires customer approval under our proposed rules. Second, we seek comment on the format of BIAS provider solicitations for customer approval, as well as the methods and formats by which customers may exercise their privacy choices. Specifically, we propose that BIAS providers must give customers a convenient and persistent ability to express their approval or disapproval of the use or disclosure of their information, at no cost to the customer. Third, we propose that a customer's choice must persist until it is altered by the customer, and that it should take effect promptly after the customer's expression of her choice. Fourth, we seek comment whether to apply the voice notice requirements specific to one-time usage of CPNI to BIAS providers' one-time usage of customer PI. We seek comment on these proposals, and reasonable alternatives thereto.

122. *Notice and Solicitation of Customer Approval Required Prior to Use or Disclosure of Customer PI.* To ensure that customers provide meaningful approval, we propose to require BIAS providers to solicit customer approval—subsequent to the point-of-sale—when a BIAS provider first intends to use or disclose the customer's proprietary information in a manner that requires customer approval. To ensure that customers' approval is fully informed, we propose to require BIAS providers to notify customers of the types of customer PI for which the provider is seeking customer approval to use, disclose or permit access to; the purposes for which such customer PI will be used; and the entity or types of entities with which such customer PI will be shared. We seek comment on this approach. Is there other information that a provider should be required to share as part of receiving opt-out or opt-in consent for the use or disclosure of customer information? For example, should a provider be required to share information about the arrangements it has made with third parties for the use of customer PI? If so, what information should they be required to share? We also seek comment on whether providers should be required to provide a link to the provider's privacy policy notice or other information when seeking approval for the use or sharing of customer PI. We are cognizant of the risk of information-overload if consumers are given more information than they need to make an informed

decision. We believe that our proposal, combined with the requirement to have a persistent and easily available longer privacy policy notice strikes the right balance, but we invite comment on whether there is other or different information that BIAS customers will need to make well informed opt-in and opt-out decisions. Also, while we believe that notice of a BIAS provider's privacy policies and customers' approval rights at the time of sale is necessary to help customers make an informed decision on which broadband service to purchase, such notice can often be too remote in time from when the information is actually used to give customers meaningful choice. Therefore, we believe that customers' informed approval requires notification and solicitation the first time that a BIAS provider will actually use or disclose a customer's PI. We seek comment on our proposal.

123. As the FTC has concluded, in order to be most effective, choice mechanisms that allow consumers control over how their data is used should be provided ''at a time and in a context that is relevant to consumers.'' We believe that providing notice and soliciting customer choice at this time may give customers useful information when it is most relevant to them, offsetting the risk that customers will be presented with so much information at the point of sale that they will not be able to meaningfully read and understand the privacy policies. Further, providing notice and soliciting choice before a provider wishes to use or disclose customer PI may also reduce the need for annual or other periodic notices. We seek comment on our proposal. Could notices upon use or disclosure contribute to ''notice fatigue'' over time, instead of lessening its impact at point of sale?

124. We also seek comment whether we should require BIAS providers to notify customers of their privacy choices and solicit customer approval at other prominent points in time. For example, should broadband providers be required to solicit customers' ''just-in-time'' approval whenever the relevant customer PI is collected or each time the broadband provider intends to use or disclose the relevant customer PI? What are the practical and technical realities of any such approaches? Are there any mobile-specific considerations that the Commission should consider in determining when the opportunity to provide customer approval should be given?

125. *Notice and Solicitation Methods.* We seek comment on how BIAS providers should notify customers of upcoming uses and disclosures of their PI, and solicit customer approval for those uses and disclosures. Should we permit each BIAS provider to determine the best method for soliciting customer approval, such as through email or another agreed upon means of electronic communication; separately by postal mail to the customer address of record; included on customer bills; or through some other method? Are there other technological solutions to providing customers notice that would minimize the burden on providers, and that would be equally or more efficient than these methods, such as, for example, a ''notification'' on the customer's device that accesses the broadband service? Alternatively, should we require BIAS providers to use a specific method or methods? We seek comment on any particular requirements that should apply for any of the above methods of soliciting approval.

126. *Customer Approval Methods.* We propose to require BIAS providers to make available to customers a clearly disclosed, easy-to-use method for the customer to deny or grant approval, such as through a dashboard or other user interface that is readily apparent and easy to comprehend, and be made available at no cost to the customer. We propose that such approval method should be persistently available to customers, such as via a link on a BIAS provider's homepage and mobile application, as well as any functional equivalents to them. We believe that this proposed requirement will directly and materially protect customer privacy by ensuring that customers have the ample opportunity to exercise their approval rights. Customers cannot effectively exercise their approval if the interface for expressing that choice is difficult to use, or if it is only rarely or sporadically available.

127. We seek comment on our proposal, and on any further requirements we should impose on the opportunity to grant or deny approval that may enhance customer comprehension. Should customers be given the ability to approve or disapprove uses within the text of the notice or solicitation, in addition to a dashboard or other persistent mechanism? And, given that some customers are unaccustomed to interacting with their provider via applications or the provider's homepage, should we require broadband providers to provide customers with the ability to provide customer approval via other written, electronic, or oral means, *e.g.,* through written correspondence, a toll-free number, or dedicated email address? How would such a requirement affect provider burdens?

128. We also seek comment on whether there are any mobile-specific considerations that we should consider in determining how the opportunity to provide customer approval should be given. For example, since mobile BIAS may be more accessible to children beyond parental supervision, are different approval methods necessary regarding consent of minors on mobile devices? Finally, we seek comment whether any of our proposed requirements are unnecessary or unlikely to aid customers.

129. *Effectiveness of Customer Choice.* We propose that approval or disapproval to use, disclose, or permit access to customer PI obtained by a broadband provider must remain in effect until the customer revokes or limits such approval or disapproval, and seek comment on this proposal. Are there particular considerations (for instance, with already-collected information) when customers disapprove of uses that they have previously approved, or vice versa? We also propose that BIAS providers must act upon customers' privacy choices ''promptly'' after customers provide or withdraw consent for the use or disclosure of their information. We seek comment whether it is necessary for the Commission to establish guidelines for what ''promptly'' means in this context. Why or why not? If so, we seek comment on what the guidelines and time frame might be. If a customer later reconsiders and changes his approval, how long should the provider be given to update this consent choice? Should the two lengths of time be the same? How does this proposal affect potential rules limiting data retention and requiring disposal of customer data? Would a customer's withdrawal of consent require disposal of her already-collected data immediately, after a period of time, or not at all?

130. *Notice Requirements for One-Time Usage of Customer PI.* Additionally, we seek comment on whether to apply or adapt the current voice notice requirements specific to one-time usage of CPNI to BIAS providers' one-time usage of customer PI. The current voice rules allow a more flexible process for providing notice and accepting consent, so long as the approval granted is for the limited purposes of the particular interaction, such as during the duration of a customer service call or during a real-time chat. Do these or some other requirements make sense in the broadband context? Do they make sense

as extended to all customer proprietary information?

3. Documenting Compliance With Proposed Customer Consent Requirements

131. In order to ensure that the requisite approval is clearly established before the use or disclosure of customer PI, and also that the approval can be demonstrated after the use or disclosure, we propose to require BIAS providers to document the status of a customer's approval for the use and disclosure of customer PI, and we seek comment on that proposal. We base our proposal on the existing rules governing safeguards on the use and disclosure of customer PI for voice telecommunications services. Specifically, we propose requiring BIAS providers to (1) maintain records on customer PI disclosure to third parties for at least one year, (2) maintain records of customer notices and approval for at least one year, (3) adequately train and supervise their personnel on customer PI access, (4) establish supervisory review processes, and (5) provide prompt notice to the Commission of unauthorized uses or disclosures. With these proposed rules, we seek to promote consumer confidence that BIAS providers are adequately protecting customers' PI, to provide clear rules of the road to BIAS providers about their obligations, and to maintain consistency with existing legal requirements and customer expectations. Are there any other or different requirements that we should adopt in order to ensure that providers document their compliance with our customer consent requirements? Should we require BIAS providers to file an annual compliance certification with the Commission, as is required under the current Section 222 rules? Are there alternative approaches to safeguard customers' proprietary information and boost customer confidence in the privacy of their customer PI that we should consider?

132. Finally, in addition to the above proposals, we seek comment on any other mechanisms or alternatives that would help document compliance with our proposed customer approval framework, boost customer confidence in BIAS provider safeguards of customer PI, and harmonize the proposed rules with existing legal requirements and customer expectations.

4. Small BIAS Providers

133. We seek comment on ways to minimize the burden of our proposed customer choice framework on small BIAS providers. In particular, we seek comment on whether there are any small-provider-specific exemptions that we might build into our proposed approval framework. For example, should we allow small providers who have already obtained customer approval to use their customers' proprietary information to grandfather in those approvals? Should this be allowed for disclosure to third parties? Should we exempt providers that collect data from fewer than 5,000 customers a year, provided they do not share customer data with third parties? Are there other such policies that would minimize the burden of our proposed rules on small providers? If so, would the benefits to small providers of any suggested exemptions outweigh the potential negative impact of such an exemption on the privacy interests of the customers who contract for the provision of BIAS with small providers? Further, were we to adopt an exemption, how would we define what constitutes a ''small provider'' for purposes of that exemption?

5. Harmonizing Customer Approval Requirements

134. We seek comment on whether we should take steps to harmonize the existing customer approval requirements for voice services with those requirements we have proposed for broadband providers to ensure that the privacy of customers' PI is protected, and that our regulations are competitively neutral, across all platforms. Are there aspects of the existing rules that should be more explicitly incorporated into our proposal, or eliminated to better comport with our proposal? Are there aspects of the proposed rules that should be applied in the voice context? Would harmonizing these rules benefit traditional voice subscribers? Would harmonizing our existing and proposed rules benefit providers who offer both services by clarifying and streamlining the customer approval requirements applicable to both types of services? In harmonizing the existing voice rules with our proposed rules for BIAS providers, how should we address voice services provided to large enterprise customers, which are currently not subject to the voice rules? Are there other changes that can be made to our rules that govern the marketing of service offerings that might improve them in the voice context? We also seek comment on how our reclassification of BIAS as a telecommunications service affects the obligations of voice carriers under our rules.

135. We also seek comment on whether we should adopt rules harmonizing the approval requirements we propose for BIAS customers with the approval requirements for use of subscriber information in Sections 631 and 338(i). We note that those provisions of the Act prohibit the use of the cable or satellite system to collect, use, or share personally identifiable information for purposes other than provision of the underlying services and other very limited purposes, absent the express written or electronic consent of the subscriber, except to provide the underlying service and for certain other very limited purposes.

D. Use and Disclosure of Aggregate Customer PI

136. Because of the complexity of the issues surrounding aggregation, de-identification, and re-identification of the data that BIAS providers collect about their customers, we propose to address separately the use of, disclosure of, and access to aggregate customer information. Consistent with reasonable consumer expectations, existing best practices guidance from the FTC and NIST, and Section 222(c)(3)'s treatment of aggregate CPNI, we propose to allow BIAS providers to use, disclose, and permit access to aggregate customer PI if the provider (1) determines that the aggregated customer PI is not reasonably linkable to a specific individual or device; (2) publicly commits to maintain and use the aggregate data in a non-individually identifiable fashion and to not attempt to re-identify the data; (3) contractually prohibits any entity to which it discloses or permits access to the aggregate data from attempting to re-identify the data; and (4) exercises reasonable monitoring to ensure that those contracts are not violated. We also propose that the burden of proving that individual customer identities and characteristics have been removed from aggregate customer PI rests with the BIAS provider.

137. Recognizing that aggregate, non-identifiable customer information can be useful to BIAS providers and the companies they do business with, and not pose a risk to the privacy of consumers, Section 222(c)(3) permits telecommunications carriers to use, disclose, or permit access to aggregate customer information—collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed—without seeking customer approval. Our proposed rule expands this concept to include all customer PI, and imposes safeguards to ensure that such information is in fact aggregated and non-identifiable, and that safeguards

have been put in place to prevent re-identification of this information.

138. We believe our multi-pronged proposal, grounded in FTC guidance, will give providers enough flexibility to ensure that as technology changes, customer information is protected, while at the same time minimizing burdens and maintaining the utility of aggregate customer information. Below we discuss and seek comment on each of the prongs of our proposed rule regarding the use and disclosure of aggregate customer PI. We also seek comment on whether we should extend our proposed rule to providers of voice telecommunications services. To the greatest extent possible, we ask that commenters ground their comments in practical examples: What kinds of aggregate, non-identifiable information do or can BIAS providers use and share?

139. *Not Reasonably Linkable.* In order to protect the confidentiality of individual customers' proprietary information, the first prong of our approach would require providers to ensure the aggregated customer PI is not reasonably linkable to a specific individual or device. Our proposal recognizes that techniques that once appeared to prevent re-identification of aggregate information have increasingly become less effective. It is also consistent with FTC guidance which recommends that companies take reasonable measures to ensure that the data is de-identified, and recommends that this determination should be based on the particular circumstances, including the available methods and technologies, the nature of the data at issue, and the purposes for which it will be used.

140. We seek comment on this proposal. Are the factors identified by the FTC well-suited to determining whether a BIAS provider has taken reasonable measures to de-identify data? Are there other factors that we should expect providers to take into account? Should we provide guidance on what we mean by linked and linkable information? NIST defines linked information as ''information about or related to an individual that is logically associated with other information about the individual,'' and linkable information as ''information about or related to an individual for which there is a possibility of logical association with other information about the individual.'' Should we adopt either or both of these standards? Are there other approaches we should use to decide whether information is reasonably linkable? For example, HIPAA permits covered entities to de-identify data through statistical de-identification, whereby a properly qualified statistician, using accepted analytic techniques, concludes that the risk is substantially limited that the information might be used, alone or in combination with other reasonably available information, to identify the subject of the information.

141. We seek comment on alternative approaches to this prong and the comparative merits of each possible approach. We also seek comment whether we should require BIAS providers to retain documentation that outlines the methods and results of the analysis showing that information that it has treated as aggregate information has been rendered not reasonably linkable.

142. *Public Commitments.* Prong two of our proposal would require BIAS providers to publicly commit to maintain and use aggregate customer PI in a non-individually identifiable fashion and to not attempt to re-identify the data. Such public commitments would help ensure transparency and accountability, and accommodate new developments in the rapidly evolving field of privacy science. This prong and the next are consistent with FTC guidance and the Administration's draft privacy bill recommending that companies publicly commit not to re-identify data and contractually prohibit any entity with which a company shares customer data from attempting to re-identify it. We seek comment on this proposal. Would this requirement help ensure that providers are protecting the confidentiality of customer PI? How could or should a BIAS provider satisfy the requirement to make a public commitment not to re-identify aggregate customer PI? For example, would a statement in a BIAS provider's privacy policy be sufficient?

143. *Limits on Other Entities.* The third prong of our proposal would require providers to contractually prohibit any entity to which the BIAS provider discloses or permits access to the aggregate customer data from attempting to re-identify the data. This proposal presents a modern approach to the difficulties of ensuring the privacy of aggregate information, recognizing that businesses are often in the best position to control each other's practices. Researchers have argued that such contractual prohibitions are an important part of protecting consumers' privacy, because making data completely non-individually identifiable may not be possible or even desirable. We recognize that the categories of what can potentially be reasonably linkable information will continue to evolve, and we believe these contractual provisions provide a critical layer of privacy protection that remains constant regardless of changes in the technology.

144. *Reasonable Monitoring.* Related to the requirements for prong three, the fourth prong of our approach requires BIAS providers to exercise reasonable monitoring of the contractual obligations relating to aggregate information and to take reasonable steps to ensure that if compliance problems arise they are immediately resolved. This prong is a logical outgrowth of the previous prongs, and it is consistent with the 2012 FTC Privacy Report. We seek comment regarding the types of monitoring and remediation steps BIAS providers should be required to take to ensure that entities with which they have shared aggregate customer PI are not attempting to re-identify the data. What potential burdens and benefits would arise from this proposal?

145. *Alternatives.* Alternatively, we seek comment whether we should develop a list of identifiers that must be removed from data in order to determine that ''individual customer identities and characteristics have been removed.'' If we take such an approach, should it replace all, a portion of, or be in addition to our current proposal? HIPAA incorporates such a standard, and under this approach, a covered entity or its business associate may de-identify information by removing 18 specific identifiers. Under HIPAA, the covered entity must also lack actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information. We are aware of criticisms that the approach taken by HIPAA no longer provides the levels of protection previously assumed. One legal scholar, for example, argues that ''[t]he idea that we can single out fields of information that are more linkable to identity than others has lost its scientific basis and must be abandoned.'' Are such concerns valid? Were we to adopt a similar standard to that in HIPAA, what categories of identifiers would be relevant in the broadband context? And, given the wide variety of customer data to which BIAS providers have access by virtue of their provision of BIAS, is such a list even feasible? Is it likely that any list developed would be rendered obsolete by technological developments in the data re-identification field? How could we best ensure that the categories we identify remain adequate to prevent aggregate customer PI from being re-identified? Should we adopt a catch-all to address evolving methods of de-identification and re-identification of aggregate customer PI, and if so, how

would such a process work? We also seek comment whether, if we were to pursue such an approach, we should also adopt an ''actual knowledge'' standard, as HIPAA includes. How would the Commission enforce such a standard, and would it encourage willful ignorance on the part of broadband providers?

146. Are there any additional or alternative requirements we should adopt that might make aggregate customer information less susceptible to re-identification? If so, what are they, and why would they be preferable to the procedures we have proposed above? As commenters consider whether we should adopt each of the prongs of our proposed rule, and any proposed alternatives, we welcome comment on how providers would demonstrate compliance with each prong of the proposal, and of any alternative proposals. Are there specific record keeping requirements we should impose on providers to demonstrate compliance? We also seek comment on the costs and benefits of each prong and of all of them collectively. We invite proposals on how we could limit any burdens associated with compliance, particularly for smaller providers.

147. We also seek comment on how de-identified, but non-collective data should be treated under Section 222 and our rules. We note that there is an existing petition before the Commission that may address some of these issues. *See* Petition of Public Knowledge et al. for Declaratory Ruling Stating that the Sale of Non-Aggregate Call Records by Telecommunications Providers without Customers' Consent Violates Section 222 of the Communications Act, WC Docket No. 13–306 (filed Dec. 11, 2013). We do not believe that the use and disclosure of such information would fall under the exception for use and disclosure of aggregate customer data enumerated in Section 222(c)(3), because by definition aggregate data must be collective data. Do commenters agree? Does Section 222 require us to conclude that all CPNI should be considered individually identifiable unless it meets the definition of aggregate, *i.e.,* is both de-identified and collective? Does the use and disclosure of such information then fall under the general use and disclosure prohibitions of Section 222(c)(1)? Does Section 222(a) provide the Commission authority to adopt privacy protections regarding all such data that is customer PI? We seek comment whether de-identified but non-collective data should be subject to the proposed opt-out and opt-in customer consent requirements described above.

148. We seek comment on whether we should, for the sake of harmonization, apply our proposed rules for BIAS providers' use and disclosure of, and access to, aggregate customer proprietary information to all other telecommunications carriers. Likewise, should we adopt rules harmonizing the treatment of aggregate information by cable and satellite providers with the treatment of aggregate information by telecommunications carriers? We note that neither Section 222 nor the Commission's currently existing implementing rules explicitly restrict carriers' use of aggregate customer PI. However, as noted above, as technology has evolved, information that previously appeared to be aggregate may no longer be. We think this is true whether a company offers voice telephony or BIAS. Providers, researchers, and others make valuable use of aggregate customer information, but this use must comport with contemporary understandings of how to ensure the information is aggregate information and not re-identifiable. Accordingly, we ask commenters to explain whether our proposed rules should apply to all providers regardless of the technology used to provide service.

E. Securing Customer Proprietary Information

149. Strong data security protections are crucial to protecting the confidentiality of customer PI. As the FTC has observed, there is ''widespread evidence of data breaches and vulnerabilities related to consumer information,'' and such incidents ''undermine consumer trust, which is essential for business growth and innovation.'' Therefore, to protect confidential customer information from misappropriation, breach, and unlawful disclosure, we propose robust and flexible data security requirements for BIAS providers. We propose both a general data security requirement for BIAS providers and specific types of practices they must engage in to comply with the overarching requirement.

150. Our proposal to adopt a general standard and identify specific activities the provider must engage in to comply with that standard is informed by existing federal data security laws and regulations and proposed best practices that recognize that privacy and security are inextricably linked and require affirmative safeguards to protect against unauthorized access of consumer data. In proposing this two-step approach to data security we look to HIPAA and its implementing regulations, GLBA and its implementing regulations, the FTC's best practices guidance, FTC and FCC settlements of specific data security investigations, and state laws.

151. Specifically, we propose to require BIAS providers to protect the security and confidentiality of all customer proprietary information from unauthorized uses or disclosures by adopting security practices calibrated to the nature and scope of the BIAS provider's activities, the sensitivity of the underlying data, and technical feasibility. To ensure compliance with this obligation, we propose to require BIAS providers to, at a minimum, adopt risk management practices, institute personnel training practices, adopt customer authentication requirements, identify a senior manager responsible for data security, and assume accountability for the use and protection of customer PI when shared with third parties. In addition, we seek comment on whether we should also include data minimization, retention, and destruction standards in any data security regime we adopt. Finally, we seek comment on harmonizing the data security requirements for BIAS providers and those for voice providers, and on adopting harmonized data security requirements for cable and satellite providers.

1. General Standard

152. We believe that Section 222(a) requires BIAS providers to protect the security, confidentiality, and integrity of customer PI that such BIAS provider receives, maintains, uses, discloses, or permits access to from any unauthorized uses or disclosures, by adopting security practices appropriately calibrated to the nature and scope of the BIAS provider's activities, the sensitivity of the underlying data, and technical feasibility. We propose to adopt a rule codifying this obligation. We seek comment on this proposal.

153. Data security is one of the core principles of the FIPPs. The FIPPs call for organizations to protect personal information ''through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.'' As a result, numerous federal and state laws have adopted general data security requirements for the entities they cover. The Satellite and Cable Privacy Acts, for example, require cable and satellite operators to ''take such actions as are necessary to prevent unauthorized access to [personally identifiable] information by a person other than the subscriber or cable operator [or satellite carrier].'' HIPAA requires the adoption of security regulations to protect the integrity,

confidentiality, and availability of electronic health records that are held or transmitted by covered entities. Similarly, the Safeguards Rule, adopted by the FTC to implement GLBA, requires financial institutions under the FTC's jurisdiction to ''[i]nsure the security and confidentiality of customer information''; ''[p]rotect against any anticipated threats or hazards to the security or integrity of such information''; and ''[p]rotect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.''

154. Our proposal is also consistent with the approach that the FTC has taken in providing guidance on best practices for all companies under its jurisdiction, and in using the ''unfairness'' prong of Section 5 of the FTC Act in its enforcement work. The FTC has taken enforcement action in cases where companies have failed to take ''reasonable and appropriate'' steps to protect consumer data, including several dozen cases against businesses that failed to protect consumers' personal information. It is also worth noting that a number of states have enacted legislation requiring regulated entities to take reasonable measures to protect and secure personal data from unauthorized use or disclosure.

155. We seek comment on how we should interpret the terms ''security, confidentiality, and integrity'' in our proposed overarching data security requirement. For example, the HIPAA implementing rules define confidentiality as ''the property that data or information is not made available or disclosed to unauthorized persons or processes'' and integrity as ''the property that data or information have not been altered or destroyed in an unauthorized manner.'' Conversely, while the GLBA requires organizations to ''insure the security and confidentiality of customer records and information,'' it does not separately define the terms ''security'' and ''confidentiality.'' We seek comment whether we should define these terms and, if so, how we should define them. Are these terms already firmly established in the data security context and in other laws or should we rely on some other definition? Do these terms indicate three separate duties under Section 222, or are they all elements of the single, overarching duty under our proposed data security requirements? Further, to the extent that we determine that contents of customer communications may be considered CPNI, PII, or neither, how can we ensure that broadband providers appropriately protect such information?

2. Protecting Against Unauthorized Use or Disclosure of Customer PI

156. To ensure BIAS providers comply with our proposed overarching requirement to protect the security, confidentiality, and integrity of customer PI, we propose in this section to require every BIAS provider to:

- Establish and perform regular risk management assessments and promptly address any weaknesses in the provider's data security system identified by such assessments;
- Train employees, contractors, and affiliates that handle customer PI about the BIAS provider's data security procedures;
- Ensure due diligence and oversight of these security requirements by designating a senior management official with responsibility for implementing and maintaining the BIAS provider's data security procedures;
- Establish and use robust customer authentication procedures to grant customers or their designees' access to customer PI; and
- Take responsibility for the use of customer PI by third parties with whom they share such information.

157. This proposed data security framework is intended to be robust and flexible and to help ensure that BIAS providers protect the confidentiality of their customers' information, and enhance their customers' ability to effectively decide under what circumstances the BIAS provider should use and share customer confidential information. As discussed in more detail below, it is also consistent with a variety of federal laws and regulations, and best practices. We seek comment on this proposed framework.

158. In order to allow flexibility for practices to evolve as technology advances, while requiring the regulated entities to install protocols and safeguards that are available and economically justified, we propose not to specify technical measures for implementing the data security requirements outlined below. This follows the regulatory approaches taken at other federal agencies. We believe this approach will encourage BIAS providers to design security measures that can easily adapt to new and different technologies. We seek comment on this approach.

159. Are there additional data security obligations that would help to ensure the security, confidentiality, and integrity of customer PI? Are any of our proposed requirements not needed? We recognize that most BIAS providers already have robust data security measures in place. To what extent are some or all BIAS providers already engaged in these or other data security measures? What are the costs involved with each element of our proposal, and of any other proposed elements? Are there any costs or burdens unique to small entities? How would the security measures contemplated under our proposed rules impact small businesses? We also seek comment on whether there are alternative actions that BIAS providers could employ to meet the same goals.

160. We also seek comment whether we should establish safe harbors or convene stakeholders to establish best practices similar to NTIA's privacy multi-stakeholder processes. If we were to undertake a similar multi-stakeholder process, how could we facilitate the success of such a process? How could we ensure that any developed best-practices evolved over time?

161. Alternatively, we seek comment on whether we should prescribe specific administrative, technical, and physical conditions that must be included as part of a BIAS provider's plan to secure customer proprietary information. Would prescribing specific, technologically-motivated security measures unnecessarily limit additional protective measures that a BIAS provider would otherwise implement instead of, or in addition to, the prescribed measures? Would specific data security measures reduce BIAS providers' incentives to be more innovative with security or have an impact on competition, assuming BIAS providers compete on the level of security employed? How would having specific security measures help or hamper enforcement efforts? Below we invite comment on each of the areas that we propose to require BIAS providers to incorporate into their data security practices.

a. Risk Management Assessments

162. To help identify and protect against risks to the security, confidentiality, and integrity of customer PI, we propose requiring BIAS providers to establish and perform regular risk management assessments and promptly remedy any security vulnerabilities identified by such assessments. In combination with the other safeguards we propose today, we believe that regular risk management assessments will help enable BIAS providers to adequately protect customer PI from reasonably foreseeable risks to the data's security, confidentiality, and integrity. We propose to allow each BIAS provider to

determine the particulars of and design its own risk management program, taking into account the probability and criticality of threats and vulnerabilities that may impact the confidentiality of customer PI used, disclosed, or maintained by the BIAS provider. We seek comment on our proposal and rationale.

163. Our proposal aligns with the data security process established under GLBA, which requires financial institutions to perform risk assessments to ''[i]dentify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information'' in their possession. Similarly, under the Security Rule, implementing HIPAA, organizations must ''[i]mplement policies and procedures to prevent, detect, contain, and correct security violations,'' which includes a requirement for risk analysis. The HIPAA Security Rule also requires that, as part of the risk analysis, covered organizations ''conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization].'' We base our proposal on these well-established frameworks and seek comment on whether there are additional models or frameworks we should consider. Should we require technical audits such as penetration tests, given concerns about the adequacy of survey-based risk assessments? Are there any elements that would be inapplicable in the broadband context?

164. Alternatively, we seek comment whether we should specify the manner in which the risk management assessments should be designed and conducted instead of allowing the BIAS provider to determine the specifics. HIPAA risk analyses under the Security Rule must include: The scope of the analysis, data collection, identification and documentation of potential threats and vulnerabilities, assessment of current security measures, determination of the likelihood and potential impact of the threat occurrence, determination of the level of risk, and documentation of these efforts. We seek comment on whether we should follow a similar approach and impose specific risk management requirements on BIAS providers. Or, should we instead establish a safe harbor with specific criteria to be included in a risk management assessment in order to qualify for the safe harbor? Under either circumstance, what should the specific requirements be?

165. We also seek comment on whether we should define ''regular'' as part of the ''regular risk assessment'' requirement. If so, how often should we require BIAS providers to conduct risk assessments? Should the required frequency of risk assessment differ based on the sensitivity of the underlying information?

166. Finally, to ensure the effectiveness of the risk management assessments, we propose that a BIAS provider should be required to promptly remedy any data security vulnerabilities it identifies through such assessments. We seek comment on this proposal. Should we define ''promptly'' as part of the requirement to ''promptly address'' any weaknesses identified? If so, what would be a reasonable amount of time to qualify as ''promptly'' to adequately protect customers while allowing the BIAS provider an opportunity to react appropriately to the security risk at hand?

b. Employee Training To Protect Against Unauthorized Use or Disclosure of Customer PI

167. We also propose to require BIAS providers to protect against unauthorized uses or disclosures of customer PI by training their employees, agents, and contractors that handle customer PI on the data security measures employed by the BIAS provider and by sanctioning any such employees, agents, or contractors for violations of those security measures. Data security training is well recognized as a key component of strong data security practices. A training requirement is a well-established part of the Commission's treatment of CPNI for voice providers. The Commission adopted a personnel training safeguard as part of its original 1998 CPNI rules, requiring that carriers train all employees with access to customer records as to when they can and cannot access CPNI and that they maintain internal procedures for managing employees that misuse CPNI. In its data security consent orders, the Enforcement Bureau has also adopted training requirements to help ''ensure that consumers can trust that carriers have taken appropriate steps to ensure that unauthorized persons are not accessing, viewing or misusing their personal information.'' We seek comment on our proposal and our rationale.

168. Our proposal also aligns with the FTC's rules implementing GLBA, which requires staff training as part of a covered entity's security program as well as taking steps to ensure that their affiliates and service providers safeguard customer information in their care. The rules implementing HIPAA also require data security training, although those rules are focused on the employees of a covered entity and not its agents or contractors.

169. The existing training programs required by the HIPAA and GLBA rules do not specify all the topics that must be included under the training program, nor do they mandate the frequency or length of training. We seek comment whether we should follow this approach or provide further clarifications on the training process. We also seek comment whether we should require training be done on an annual basis or with some other specified frequency, or establish a minimum frequency. Are there additional entities to which these training requirements should apply?

c. Ensuring Reasonable Due Diligence and Corporate Accountability

170. To ensure that BIAS providers have a robust data security program that includes any requirements that we ultimately adopt, we propose requiring BIAS providers to designate a senior management official with responsibility for implementing and maintaining the BIAS provider's information security program to ensure that someone with authority in the company has personal knowledge of and responsibility for the BIAS provider's data security practices. As with the other data security requirements we propose, this proposal is firmly rooted in existing privacy regimes. For example, the HIPAA rules require each covered entity to designate a privacy official.

171. In fact, since the Commission first promulgated its CPNI rules, corporate oversight has been included as part of the data security requirements. As the Commission explained, having a corporate officer attest to having personal knowledge of the carrier's data security compliance is ''an appropriate and effective additional safeguard.'' We seek comment on our proposal to require BIAS providers to designate a senior management official to implement and maintain the provisions of the BIAS providers' data security procedures. We recognize that many BIAS providers currently have senior officials responsible for privacy and data security and seek comment on the burden of this requirement, in light of BIAS providers' existing management and compliance structures.

172. We also seek comment whether we should require additional information or verification measures as part of this requirement for oversight. For example, should we specify qualifications that a senior management

official should or must have to serve in this capacity? Are there any other specifications that we should or should not include as part of this requirement?

d. Customer Authentication Requirements for Access to Customer Proprietary Information

173. To honor customers' rights to access their personal information while ensuring that BIAS providers comply with their duty to safeguard confidential customer data, we propose to require BIAS providers to adopt robust customer authentication requirements. We seek comment on whether we should require providers to use, at a minimum, a multi-factor authentication before granting a customer access to the customer's PI or before accepting another person as that customer's designee with a right to access a customer's PI. We also propose to require BIAS providers to notify customers of account changes to protect against fraudulent authentication attempts. Relatedly, we also seek comment on the methods by which consumers should be allowed to access their customer PI and whether we should adopt rules requiring BIAS providers to correct inaccurate customer PI.

(i) Robust Authentication Requirements

174. In order to protect against unauthorized access to customer PI, we propose to require BIAS providers to adopt robust customer authentication and we seek comment on requiring the use of multi-factor authentication. We believe that customer authentication is a critical element in ensuring that the confidentiality of customers' PI is protected. We seek comment on our proposals.

175. We do not currently propose to require BIAS providers to adopt multi-factor authentication or, more granularly, specific types of multi-factor authentication methods, because we recognize that there is no perfect and permanent approach to customer authentication. Technology develops over time. Multi-factor authentication requires users to authenticate through multiple elements in order to prove one's identity, under the assumption that it is unlikely that an unauthorized actor will be able to succeed at more than one form of authentication. We understand that currently used authentication mechanisms vary by company, by industry, and often by the sensitivity of the underlying data. Types of authentication credentials currently fall into one of three categories: (i) Something people know, such as a password or a personal identification number (PIN); (ii) something people possess, such as a token or access key; and (iii) something people are, such as biometric information based on typing patterns or fingerprints. Multi-factor authentication typically combines at least two of these categories, requiring, for example, that users provide a password in addition to an access key code that is maintained on a separate device. As a result, multi-factor authentication is widely considered to be one of the most secure authentication methods currently available.

176. We seek comment on the advantages and disadvantages of requiring multi-factor authentication. Are there security risks associated with multi-factor authentication that we should take into account? How would consumers be affected by a multi-factor authentication requirement? What would be the additional costs imposed on BIAS providers and/or consumers? If a cell phone number or email address is used to provide new information after authentication, how can the provider be certain that neither has been compromised? Are there customers that would not be able to take advantage of a multi-factor authentication process based on lack of access to specific types of technology? If so, what alternatives should be available, and should we require providers to make these alternatives available? Would a multi-factor authentication requirement unduly burden small providers? How would a multi-factor authentication regime work for interactions that are off-line, *i.e.,* in-person access to customer PI via a face-to-face interaction at the BIAS provider's regional offices or via a telephone call? Are there specific issues with respect to multi-factor authentication and customers with disabilities that we should take into account?

177. We seek comment on other robust methods of customer authentication. FTC guidance encourages ''[c]ompanies engaged in providing data for making eligibility determinations [to] develop best practices for authenticating consumers for access purposes,'' and highlights the security work of the private sector such as Payment Card Institute Data Security Standards for payment card data, the Better Business Bureau, and the Direct Marketing Association that developed and implemented best practices for authenticating consumer accounts. Further, NIST's cybersecurity standards recommend authentication standards based on risk models, noting that ''the level of authentication required for online banking is likely to differ from that required to access an online magazine subscription.'' We seek comment on application of these authentication practices and standards to the relationship between BIAS providers and their customers, as well as the benefits and drawbacks of adopting any of these methods as requirements in the broadband context. Are there any authentication methods being used that we should discourage or even prohibit because they are outdated, present their own privacy or data security risks, are unworkable for people with certain types of disabilities, or for other reasons? For example, do authentication methods that rely on additional, less mutable, personal information, such as fingerprints or other biometric information, raise particular concerns in the case of a breach of that personal information or other scenarios? Would BIAS providers need to employ additional safeguards to secure this authentication-specific information? Should our rules prohibit BIAS providers from requiring their customers to provide biometric information as part of any authentication scheme?

178. We also seek comment on whether we should require password protection. Our existing voice rules rely on authenticating customers based on a password the customer must establish before seeking to obtain call-detail information over the telephone or via online access. These measures were implemented to address the problem of pretexting, where parties pretend to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications records.

179. However, given the frequency with which passwords are compromised due to phishing attacks, password database leaks, and reuse of passwords across multiple Web sites and service offerings, we have concerns whether a password is a sufficient safeguard when a customer requests access to customer PI over a customer-initiated phone call or via online access in the broadband context. We seek comment generally on the efficacy of password authentication in this context. If commenters agree that password protection should be part of a robust customer authentication mechanism, should we prescribe additional requirements, such as mandating the use of secret questions or character limitations on passwords? Or should we establish a particular standard with respect to password protection and leave it up to the provider to determine the best way to meet that standard?

180. We also seek comment whether we should adopt specific authentication

procedures for particular scenarios, as our existing Section 222 rules do with respect to customer authentication over a telephone call, or should instead adopt a flexible system like that which we propose for data security measures. If the former, what should such authentication procedures be, and under what scenarios should they be required? What are the advantages and disadvantages of each regime? What are the implications for BIAS providers of requiring a particular type of authentication measure? Would adopting a particular authentication model or practice stifle development of new technologies that may provide improved security, or possibly provide a specific target for bad actors to work around, in effect making the practice less effective as a security precaution? We also seek comment on how to ensure that any ultimate authentication requirement we adopt is flexible enough to incorporate and encourage the latest technological advances.

181. We also seek comment on whether there are other authentication methods that BIAS providers can employ to make the authentication process less cumbersome for consumers. For example, are there ways for BIAS providers to work with existing edge providers that already authenticate their users to simplify customer authentication? Allowing third-party credentials can save time and resources in managing identities for both customers and businesses. The benefits to organizations and individuals can be significant, but there is also a concern that these connections meant to improve security can create opportunities for increased tracking of users. We seek comment whether and how the proposed rules should and can accommodate such innovations.

182. Finally, we seek comment on whether we should harmonize the existing authentication requirements for voice providers with the authentication method we ultimately adopt for BIAS providers. Do the existing voice authentication rules, with their emphasis on passwords following a customer-initiated request, continue to be both relevant and effective? Should we update these rules to require robust customer authentication similar to what we propose for BIAS? Why or why not? Are there other steps we should take to harmonize the authentication requirements for voice and BIAS providers? Are there specific customer authentication rules we should adopt for cable and satellite providers in light of their obligation to prevent unauthorized access to a subscriber's personally identifiable information? In addition, we seek comment on whether we should adopt employee and contractor authentication requirements to permit access to customer PI. If so, what standards should we adopt?

(ii) Notification of Account Changes

183. We also propose requiring BIAS providers to notify customers of account changes, and attempted account changes, as an additional check against fraudulent account access. The change notification requirement we propose today is similar to the requirement under our existing Section 222 rules, which requires carriers to ''notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed.'' As the Commission explained in 2007, account change notification is an important tool that allows customers to monitor their accounts' security and protects customers from data thieves that might otherwise manage to circumvent a provider's authentication protections.

184. We recognize that notifying customers of account changes is a best practice already followed by many BIAS providers, as well as other companies operating in the broadband ecosystem. We seek comment, particularly those which are grounded on practical experience, on how our proposal for notification of account changes can be implemented with minimal burdens to customers and BIAS providers. How can we ensure that our proposal does not result in customer ''notice fatigue,'' lessening the usefulness of notices? Similarly, how can we ensure that notice requirement does not impose an undue burden on BIAS providers, particularly smaller providers? When sending an authentication notice, should BIAS providers be required to send the notification to another form of customer contact information than what is listed as the point of contact for any multi-factor authentication mechanism? What if a customer has only one means of being immediately notified (*i.e.,* a phone number but no email address)? How can BIAS providers be sure that they are sending the authentication notification to the correct customer and not the bad actor attempting to fraudulently authenticate the customer account? Are there other potential risks and benefits from this proposal we should consider?

185. We also propose to require BIAS providers to notify customers when someone has unsuccessfully attempted to access the customer's account or change account information. Providing such notice will alert the customer of possible data breach attempts. We seek comment on this proposal. Might it risk additional customer notice fatigue? Do the benefits outweigh the burdens?

186. We also seek comment on whether we should harmonize our account change notification requirements for voice and BIAS providers. Are there reasons that customer change notification regimes should be different for voice and BIAS providers? Should we have harmonized account change notification requirements for cable and satellite providers?

(iii) Right To Access and Correct Customer Data

187. We also seek comment on whether to adopt rules requiring BIAS providers to provide their customers with access to all customer PI in their possession, including all CPNI, and a right to correct that data. Access and correction rights are one of the FIPPs. We ask commenters to address how we can best balance the benefits of providing customers with access and the right to correct their personal information without imposing undue burdens on BIAS providers that collect such data.

188. As we consider these questions, we seek comment on the different forms that customer PI could take when collected and retained by broadband providers, and whether these different types of information may require different customer access regimes. For example, if BIAS providers possess customer PI in a machine-readable format, should they be required to provide customers with access to such data in a different form? What are the burdens likely to be associated with such a requirement? Are there certain sensitive classes of customer PI, such as search and browsing history or location data, that a BIAS customer should always have the ability to access? Alternatively, are there certain classes of customer PI that are inherently not sensitive, or fundamentally technical, thereby decreasing consumers' interest in obtaining disclosure of such data? Recognizing that there are economic costs associated with any disclosure regime, how should we take into account any competitive effects that may flow from the development of customer access rules applicable to broadband providers? We note that edge providers, data brokers, and other entities in the Internet ecosystem also collect, process, retain, and distribute large quantities of sensitive consumer data. Should we consider the restrictions, or lack thereof, that are

currently placed on edge providers or other entities in crafting rules for broadband providers?

189. We observe that, while the Cable and Satellite Privacy Acts explicitly provide a mechanism for subscribers to correct their personal information, Section 222 does not, and our current CPNI rules contain no such provision. How should this impact our assessment of whether to incorporate a right to correct customer PI into our broadband rules? What economic burdens or other risks would accompany application of this right to the information collected by broadband service providers? What are the data security risks that would attend customer access rights? On the other hand, what consumer protection benefits are likely to result from codifying a right to correct customer PI?

190. Relatedly, we recognize that Section 222(c)(2) grants the right of access to CPNI to ''any person designated by the customer.'' However, our existing CPNI rules do not currently contain any special provisions for voice customers to authorize third party access to their CPNI. Are such regulations necessary in the broadband context? If so, are they also necessary in the voice context? Should we harmonize our BIAS and voice services rules with respect to rights of access to customer PI?

191. If we do adopt rules requiring providers to make customer PI accessible to customers, should we also adopt rules requiring BIAS providers to give their customers clear and conspicuous notice of their right of access, along with a simple, easily accessible method of requesting their customer PI? How should such notice and access be structured? If we do adopt right of access rules, how should we ensure that customers with disabilities achieve the same level of access? If we do adopt such rules for BIAS providers, should we adopt rules harmonizing cable and satellite rights of access obligations under Sections 631 and 338(i)?

e. Accountability for Third Party Misuse of Customer PI

192. We seek comment on how best to ensure that the security, confidentiality, and integrity of customer PI is protected once a BIAS provider shares it with a third party and it is out of the BIAS provider's immediate control. Our goal is to promote customers' confidence that their information is secure not only with their BIAS provider, but also with anyone with whom the customer has provided approval for the BIAS provider to share his or her data. Consumers may be apprehensive about disclosing their personal information to BIAS providers if they cannot trust that their data will not be misused downstream. They may also be less likely to provide consent via an opt-out or opt-in mechanism if that information will no longer be protected in the recipients' hands. As the Commission has previously found, ''[i]n the absence of'' downstream safeguards, ''the important consumer protections enacted by Congress in Section 222 may be vitiated by the actions of agents.'' We believe that these risks are even greater in the broadband context than the voice telephony context because of the vast wealth of sensitive personal information handled by BIAS providers and exchanged through broadband Internet access services.

193. We believe that Section 222(a) requires BIAS providers to ensure the confidentiality of customer PI when shared with third parties. The Commission has held that ''a carrier's Section 222 duty to protect CPNI extends to situations where a carrier shares CPNI with its joint venture partners and independent contractors'' and has held carriers accountable for privacy violations of such third parties. Some economic literature suggests that holding a provider vicariously liable would maximize their incentives to ensure the data is protected. What are the benefits and drawbacks of holding providers accountable for the data security practices of its contractors, joint-venture partners, or any other third parties with which it contracts and shares customer PI? We seek comment on that approach. Is it too stringent? Should BIAS providers be held accountable for third party recipients' handling of customer PI for the entire lifecycle of the data or for a more limited duration?

194. Another way BIAS providers can help to ensure that third parties protect customer data shared by the BIAS provider is to obtain contractual commitments from third parties to safeguard such data prior to disclosing customer PI to those third parties. Such safeguards are a fundamental part of the best practices guidance the FTC provides to companies about data security practices. In the past, the Commission recognized that telecommunications services providers can protect against third party misuse through their own private contract arrangements. Should we follow that example here? Or, should we require BIAS providers to obtain specific contractual commitments from third party recipients of customer PI to ensure the protection of such data? If so, what should such contracts include? Should the third party commit to, for example, (1) limit the use and disclosure of customer PI to the specific purpose for which the provider shared the customer PI with the third party and to which the customer provided approval; (2) take precautions to protect the customer PI from unauthorized use, disclosure, or access; (3) train its employees on the provisions of its information security program and monitor compliance; (4) follow the same data security requirements that we adopt for BIAS providers; (5) follow the data breach notification procedures we adopt for BIAS providers; (6) notify the BIAS provider of any breach of security involving customer PI as expeditiously as possible and without unreasonable delay; (7) institute data retention limits and minimization procedures; and/or (8) document of compliance with these contractual commitments, including records of the use and/or disclosure of customer PI, as appropriate? What are the benefits and burdens of each of these options, in particular on small providers, and would the benefits of such obligations outweigh the burdens associated with compliance?

195. Relatedly, we seek comment on whether we should require mobile BIAS providers to use their contractual relationship with mobile device or mobile operating system (OS) manufacturers that manufacture the devices and hardware that operate on the mobile BIAS provider's network to obtain the contractual commitments described above. How do providers' contracts with device manufacturers and mobile OS manufacturers currently handle the treatment of customer PI? What would be the benefits and drawbacks of imposing security-specific obligations in those contracts?

196. Finally, we seek comment on other alternatives that we should consider regarding BIAS provider accountability for downstream privacy violations, as well as whether we should take any actions to either harmonize or distinguish our proposal from the existing voice CPNI rules.

f. Other Safeguards

197. In addition to the safeguards we propose above, we seek comment on whether there are other safeguards that BIAS providers should employ to protect against reasonably anticipated unauthorized use or disclosure of customer PI by the BIAS provider, its employees, agents, and contractors. For example, we seek comment on whether restricting access to sensitive data; setting criteria for secure passwords; segmenting networks; requiring secure access for employees, agents and

contractors; and keeping software patched and updated would be useful security measures to reduce the probability of threats. If so, should we require them? If not, what other security measures should we consider?

198. In addition we seek comment whether we should require or encourage BIAS providers to use standard encryption when handling and storing personal information. The FTC established best practices for maintaining industry-standard security, SSL encryption among them, which it considers to be a ''reasonable and appropriate'' step to secure user data. Should we mandate that customer PI be encrypted when stored by BIAS providers?

3. Factors for Consideration in Implementing Proposed Customer Data Security Measures

199. In determining how to implement the data security requirements outlined above, we believe that a BIAS provider should, at a minimum, take into account the nature and scope of the BIAS provider's activities and the sensitivity of the underlying data, and we propose to codify it as a rule. We derive our proposal from existing privacy statutes and frameworks, including the GLBA and the FTC's Privacy Framework. Our proposed approach also mirrors our existing CPNI rules for voice providers, which permit telecommunications carriers to individually determine the specific ''reasonable measures'' that will enable them to comply with the general duty to discover and protect against unauthorized access to proprietary information. We seek comment on our proposal.

200. We believe that Section 222(a) requires BIAS providers to, at a minimum, consider these factors when designing their safeguards to protect the confidentiality, integrity, and security of customer PI, and we seek comment on the inclusion of these factors and whether there are additional factors that we should consider. What are the benefits and drawbacks of such an approach to customers and BIAS providers? Would any of the factors discussed below not be considered ''reasonable'' in the broadband context? How does such an approach conform to existing industry standards? Does such an approach allow for sufficient innovation and flexibility as technology advances?

201. *Nature and Scope of BIAS Provider Activities.* We propose that any specific security measures employed by a BIAS provider should take into consideration the nature and scope of the BIAS provider's activities. We believe this sliding scale approach affords sufficient flexibility for small providers while still protecting their customers. The Commission has previously explained that ''privacy is a concern which applies regardless of carrier size or market share.'' However, we recognize that the same data security protections may not be necessary in all cases. For example, a small provider with only a few customers may not store, use, or disclose customer PI in the same manner as a large provider. In such a case, what constitutes a ''reasonable'' safeguard might be different.

202. *Sensitivity of Customer PI.* We also propose that the security measures a BIAS provider employs should consider the sensitivity of the underlying customer PI. This sliding scale approach follows the FTC's proposed Privacy Framework, which includes a recommendation for allowing consumers to access the data companies maintain on them, with the level of access ''proportionate to the sensitivity of the data and the nature of its use.'' Likewise, NIST also ranks the sensitivity of PII on different ''impact levels,'' ranging from low, moderate, or high, based on the effect of the disclosure of the underlying information. We seek comment on this proposal and our rationale for it.

4. Limiting Collection, Retention, and Disposal of Data

203. The more customer information that a BIAS provider maintains, and the more sensitive that information is, the stronger the data security measures a BIAS provider will need to employ to protect the confidentiality of that information. In this section, we seek comment on data minimization, including whether we should impose reasonable data collection and retention limits. We also seek comment on whether we should prescribe specific data destruction policies as part of any data retention limits.

a. Limiting Collection of Sensitive Customer Information

204. We seek comment on whether we should adopt rules limiting BIAS providers' collection of sensitive customer information, or providing customer control over the collection of such information. The FIPPs indicate that ''[o]rganizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).'' We recognize that while the Cable and Satellite Privacy Acts prohibit operators from using the cable or satellite systems to collect PII concerning any subscriber without the prior written or electronic consent of the subscriber concerned, Section 222 does not contain an analogous provision regarding the collection of customer information. Likewise, the Commission's existing privacy rules do not contain any blanket limitations on the ability of communications service providers to collect certain types of customer data.

205. We seek comment on whether we should adopt *ex ante* rules regulating the collection of customer data by broadband service providers. We recognize that declining data storage costs may mean that customer data, once collected, can be retained indefinitely. This in turn may present data security risks that impact a provider's obligation to protect customer data pursuant to Section 222(a).

206. We seek comment on the effect of unrestricted data collection practices on data security, as well as the relationship to the concept of privacy-by-design. If we do adopt rules restricting the types of data BIAS providers can collect, will there be negative societal consequences? For example, data collected in conjunction with other online services has yielded services such as spam filters that use a variety of data for ''machine learning.'' Are there particular types of customer data, such as health information, that a provider should be prohibited from collecting? Could such a requirement be implemented and operationalized without undue burden? Is it possible for a BIAS provider to reasonably distinguish between types of data that it collects such that it could comply with such a requirement?

b. Data Retention Limits

207. Similarly, we seek comment on whether we should require BIAS providers to set reasonable retention limits for customer PI. If so, what should those retention limits be? Data retention limits can also reduce the burden of data security. Limiting data retention is also one of the seven principles of the FIPPs. Many privacy-by-design regimes, where consumer privacy is built into every stage of product development, include data retention limitations as a fundamental part of their designs. FTC guidance emphasizes the importance of data retention limits, recommending that entities retain customer data only as long as necessary for the legitimate purpose for which it was collected with the caveat that retention periods ''can be

flexible and scaled according to the type of relationship and use of the data.''

208. The FTC recommends that data retention periods should be based on the underlying nature of protected information, suggesting that data relating to children should have a shorter retention period than data relating to adults. The Cable and Satellite Privacy Acts require entities to destroy personal data if the information is no longer necessary for the purpose for which it was collected, and the Video Privacy Protection Act requires records with protected information to be destroyed as soon as practicable. While these limits are often contextually based on what is ''reasonable'' for a particular use or industry, there are circumstances where long term retention of customer data is unlikely to be reasonable. Should we adopt rules harmonizing data retention requirements for telecommunications carriers with those provided for cable and satellite providers under Sections 631 and 338(i)?

209. We seek comment whether it would be appropriate to apply any of these standards in the broadband context. Why or why not? Are there other data retention policies utilized by industry that we should look to as a guide? We also seek comment whether we should adopt a specific timeframe or a flexible standard for data retention by BIAS providers. For example, should we adopt a specific retention period for customer data upon termination of the broadband service and the carrier-customer relationship (*i.e.,* a former customer)? Should the same data retention standard apply to a BIAS provider's retention of customer PI for existing customers? What should be the appropriate retention period if someone merely completes the information form for a service but does not obtain that service?

210. Should we adopt different data retention limits for different categories of data? If so, how should we define those categories of data, and what would those retention periods be? For example, should a separate standard exist for data that has been de-identified? In addition, how could we ensure any retention periods are sufficiently flexible to accommodate requests from law enforcement or legitimate business purposes?

211. On the other hand, we recognize that some data retention can be beneficial. Historic data can be useful to individuals and serve broader social goals. For example, as the FTC Staff Report on Privacy explains, data retention limits could limit innovation by requiring the destruction of data that could be used in the future to develop new products that can potentially benefit customers. We seek comment on whether and how our rules should take into account these potential benefits of data retention.

c. Destruction of Customer Proprietary Information

212. We also seek comment whether we should implement specific measures for BIAS providers when disposing of customer PI. Alternatively, we seek comment whether we should establish a general data destruction requirement but allow industry to determine best practices for data disposal in this area. What types of data destruction practices do BIAS providers currently abide by? What are the current industry standards, if any?

213. We seek comment on whether we should adopt data destruction requirements and, if so, how sensitive data should be disposed of when it is no longer needed. Should we follow the model laid out by the Fair and Accurate Credit Transactions Act (FACTA), which requires the proper disposal of information contained in consumer reports and records? Under the FTC disposal rule, which implements FACTA with respect to companies under the FTC's jurisdiction, companies must ''tak[e] reasonable measures to protect against unauthorized access to or use of [consumer] information in connection with its disposal.'' The rule offers a non-exhaustive list of such reasonable measures that includes burning, pulverizing, or shredding paper so that they are unreadable and cannot be practicably reconstructed and destroying or erasing electronic media such that it cannot be practicably read or reconstructed. Should we take a similar approach here? Several states have also enacted laws regarding the disposal of records that contain personal information. Should we look to any such state laws for guidance?

214. We also seek comment on the potential costs and correlating burdens of imposing such requirements. Would the requirements be particularly costly or burdensome for small BIAS providers? Could the costs of a data destruction program be absorbed by the BIAS provider or would any additional cost be passed on to customers? Is there a meaningful way to quantify the privacy benefits to consumers to justify any additional costs or benefits? Is there a way for BIAS providers to ensure that a customer's data has been properly disposed of and communicate that to the customer? If we adopt data destruction requirements for BIAS providers, should we also adopt them for voice providers?

F. Data Breach Notification Requirements

215. In order to encourage providers to protect the confidentiality of customer proprietary information, and to give consumers and law enforcement notice of failures to protect such information, in this section, we propose data breach notification requirements for BIAS providers and providers of other telecommunications services. The importance of customer and law enforcement notification in the event of a data breach is widely recognized. Our existing Section 222 rules impose data breach obligations on voice providers; 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have adopted data breach notification laws; and the FTC has repeatedly testified in support of federal data breach legislation. The rules we propose today seek to incorporate the lessons learned from existing and proposed data breach notification frameworks, while addressing the extensive sets of customer data available to providers of telecommunications services, and our role in helping to identify and protect against network vulnerabilities.

216. We propose and seek comment on specific data breach notification requirements for providers of telecommunications services. We think harmonizing these requirements is a common-sense approach to ensuring that customers of all telecommunications services, the Commission, and other federal law enforcement receive timely notice of data breaches of customer PI. We structure these proposals with the goal of ensuring that affected customers, the Commission, and other federal law enforcement agencies receive timely notice of data breaches so they can take appropriate action to mitigate the impact of such breaches and prevent future breaches. Specifically, we propose that in the event of a breach carriers shall:

- Notify affected customers of breaches of customer PI no later than 10 days after the discovery of the breach, subject to law enforcement needs, under circumstances enumerated by the Commission.
- Notify the Commission of any breach of customer PI no later than 7 days after discovery of the breach.
- Notify the Federal Bureau of Investigation (FBI) and the U.S. Secret Service (Secret Service) of breaches of customer PI reasonably believed to relate to more than 5,000 customers no

later than 7 days after discovery of the breach, and at least 3 days before notification to the customers.

217. We discuss and seek comment on each of these proposals in detail below, but as an initial matter we seek comment on our proposals generally. Below, we first discuss our requirements for notifying customers and federal law enforcement of data breaches. We also seek comment on what information should be provided to customers and law enforcement as part of the data breach notification, whether we should impose record keeping requirements with respect to data breach notification, and whether we should, in fact, harmonize our voice and broadband data breach notification rules, and on whether we should adopt harmonizing rules for cable and satellite providers. Finally, we seek comment on appropriate breach notification requirements in response to a breach of data received by a third party.

1. Customer Notification

218. We propose to require BIAS providers and other telecommunications carriers to notify customers of breaches of customer PI no later than 10 days after discovery of the breach, absent a request by federal law enforcement to delay customer notification. Recognizing the harms inherent in over-notification, we propose to adopt a trigger to limit breach notification in certain circumstances. We seek comment on this proposal.

219. We seek comment on under what circumstances BIAS providers should be required to notify customers of a breach of customer PI. For consistency and to minimize burdens on breached entities, we look to other federal statutes and other jurisdictions as a basis for determining when it is appropriate to notify, or not notify, consumers of a breach of customer PI. Various state regulations employ a variety of triggers to address this challenge. We seek comment on whether some of these state requirements would also effectively serve our purpose. For example, some states do not require disclosure if, after an appropriate investigation, the covered entity determines that there is not a reasonable likelihood that harm to the consumers will result from the breach. Should we require breach reporting based on the likelihood of misuse of the data that has been breached or of harm to the consumer? If so, how would broadband providers, and the Commission, determine the likelihood of misuse or harm? If we adopted such a standard, is it necessary to clarify what is meant by ''misuse'' or ''harm''? Is it necessary to also require the provider to consult with federal law enforcement when determining whether there is a reasonable likelihood of harm or misuse?

220. Alternatively, should the requirement to notify customers of a breach be calibrated to a particular type of misuse or harm? Should it be calibrated to the sensitivity of the information? If we allow time for an appropriate investigation, how much time should providers have before they need to make their determination or disclose the breach to customers? If the provider determines that harm to the customer is likely to occur, how quickly thereafter would the provider need to notify the customer of the breach? Are there other triggers we should consider, such as the number of affected consumers? Should different triggers apply to different types of customer PI? Are there other factors that we should consider before requiring breach notifications? What are the potential enforcement and compliance implications associated with this approach?

221. Our existing Section 222 rule does not specify how quickly affected customers must be notified of a data breach involving CPNI. Instead it requires that seven full business days pass after notification to the FBI and the Secret Service before the carrier may notify customers or disclose the breach to the public. Notifying affected customers no later than 10 days following discovery of the breach will allow customers to take any measures they need to address the breach in as timely a manner as possible. We seek comment on this proposal and on potential alternatives.

222. Consistent with our current Section 222 rules, our proposed rules allow federal law enforcement to direct a provider to delay customer notification if notification would interfere with a criminal or national security investigation. We seek comment on this proposal. Should we delay customer notification in every—or in any—instances because of the potential for such notification to interfere with an investigation? The Commission adopted the staggered notification system at the request of federal law enforcement. But, is that still an approach recommended by law enforcement and other stakeholders? Our current Section 222 rules allow carriers to notify affected customers sooner than otherwise required in order to avoid immediate and irreparable harm, but only after consultation with the relevant investigating agency. Should we include such an exception in any new rules?

223. Instead of requiring customer notification of a data breach within a specific period of time, should we adopt a more flexible standard for the timing of customer notification? For example, many state data breach statutes impose an ''expeditiously as practicable'' or ''without unreasonable delay'' standard instead of a set timeframe for reporting. What are the benefits and drawbacks to such an approach? If we were to adopt such a standard, should we provide guidance on what would be considered a ''reasonable'' delay? Under such an approach, how could the Commission ensure that both federal law enforcement agencies and customers are notified in a timely manner? Could the Commission effectively enforce these requirements with such an approach? Should the Commission consider establishing any exceptions to this requirement? Or, should breaches of voice customer PI be distinguished from breaches of broadband customer PI for the reporting requirement? What would the impact of this requirement be on small providers?

224. Although we propose to require notice to customers only after discovery of a breach, we seek comment on whether we should require notice when the telecommunications carrier discovers conduct that would reasonably lead to exposure of customer PI. Should any such requirement be adopted in addition to or in place of a requirement to provide notice upon discovery of a breach?

225. *Content of customer data breach notification.* We propose to require that the customer data breach notice include basic information about the breach sufficient to convey an understanding of the scope of the breach, any harm that might result, and whether customers should take action in response. Specifically we propose to require that a carrier's notification to affected customers include the following:

- 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 provider 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

• Information about national credit-reporting agencies and the steps customers can take to guard against identity theft, including any credit monitoring or reporting the telecommunications provider is offering customers affected by the breach of security.

226. We seek comment on this proposal and potential alternatives. The existing Section 222 breach notification rule does not specify the content of customer notification. In 2007, the Commission declined to do so, leaving the contents to the discretion of carriers to tailor the language and method to the circumstances. Although we continue to believe that breached entities should have discretion to tailor the language and method of notification to the circumstances, we believe that it is appropriate to specify the above as a baseline of fundamental information that should be provided to affected individuals to ensure customers receive an adequate level of protection. Does our proposal include the information that customers will likely need in order to take measures to address a breach and its ramifications? Is there additional information that we should require providers to include in their data breach notifications to customers? Should any of the proposed content requirements be revised, and should any be removed? Should content requirements vary based on the type of information breached, the number of customers affected, the extent of economic harm, if any, or other factors? If so, how should the requirements vary?

227. *Method of customer data breach notification.* In order to inform customers about breaches, we propose that the telecommunications carrier should provide written notification to the customer's address of record, email address, or by contacting the customer by other electronic means using contact information the customer has provided for such purposes. This framework ensures that customers receive prompt notification in the manner in which they expect to be contacted by their telecommunications carriers. In 2007, the Commission chose not to specify the method by which carriers would notify their affected customers of a breach. Our proposal is consistent with the HIPAA breach rule and many state breach notification rules that specify that notification can be by mail, by email, or by other electronic means using contact information the customer has provided. Service providers should be in the best position to know how to reach their customers with important notifications and should have already established how to communicate important notifications to their customers. We seek comment on our proposal, and whether a more specific notification method is necessary or desirable to protect customers.

2. Notification to Federal Law Enforcement and the Commission

228. In order to ensure that law enforcement has timely notice to conduct confidential investigations into data breaches, we propose to require telecommunications providers to notify the Commission no later than seven days after discovering any breach of customer PI, and to notify the FBI and the Secret Service no later than seven days after discovery a breach of customer PI reasonably believed to have affected at least 5,000 customers. With regard to federal law enforcement notification, we further require that such notifications occur at least three days before a provider notifies its affected customers, except as discussed above. We seek comment on our proposal.

229. Our proposal, which aims to balance the importance of data breach notifications with the administrative burdens on telecommunications carriers and law enforcement agencies from excessive reporting, is consistent with many state statutes requiring notice to state law enforcement authorities, proposed federal legislation, and the Executive Branch's legislative proposal, each of which require law enforcement notification of large breaches. We do not want over-reporting to the FBI and the Secret Service to impose an excessive burden on their resources. We seek comment on our proposed threshold of 5,000 affected customers before a provider must report a data breach to the FBI and the Secret Service. Should we have a threshold for such reporting? If so, is 5,000 affected customers the correct threshold? For example, although a slightly different context, we note that some states have a minimum threshold of 10,000 affected customers for reporting to the consumer reporting agencies. We observe that our proposed threshold would reduce the burden on existing voice telecommunications carriers, which are currently required to report *all* breaches to the FBI and Secret Service. Does the proposed reporting threshold meet the needs of law enforcement and provide adequate safeguards? We also seek comment on whether other or different federal law enforcement agencies should receive data breach notification reports from providers. In addition to other federal law enforcement agencies, we also seek comment about whether we should require telecommunications carriers to report breaches to relevant state law enforcement agencies. What are the benefits and drawbacks of this proposal, particularly for small providers?

230. We propose to require providers to give the Commission notice of all data breaches, not just those affecting 5,000 or more customers. As the agency responsible for regulating telecommunications services, we have a responsibility to know about problems arising in the telecommunications industry. Breaches affecting smaller numbers of customers may not cause the same law enforcement concerns as larger breaches because they may be less likely to reflect coordinated attacks on customer PI. They may, however, provide a strong indication to Commission staff about existing data security vulnerabilities that Commission staff can help providers address through informal coordination and guidance. They may also shed light on providers' ongoing compliance with our rules. We invite commenters to explain whether the Commission should be notified of all data breaches. Are there reasons that the Commission should not be notified of all data breaches? How much of an incremental burden is associated with notifying the Commission of all data breaches as opposed to only notifying customers of all data breaches?

231. We also propose that notification to federal law enforcement, when required, should be made no later than seven days after discovery of the breach, and at least three days before notification of a customer. We seek comment on this proposal and on potential alternative approaches. Will the proposed time-frames for reporting to law enforcement agencies be effective? The Commission's existing rule provides that such notification must be made ''[a]s soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach.''

232. Although we propose to require notice to law enforcement only upon discovery of a breach, we seek comment on whether we should require notice when the telecommunications provider discovers conduct that would reasonably lead to exposure of customer PI. Should any such requirement be adopted in addition to or in place of a requirement to provide notice upon discovery of a breach? Is such a requirement overly-broad to achieve our purposes? Would such a duty help protect customers against breaches and against the effects of being unaware that their information has been breached? If we do adopt such a requirement, should we require that the provider reasonably

believe that the potential breach could affect a certain number of customers?

233. *The method and content of data breach notification to federal law enforcement.* We propose to extend our existing Section 222 requirements for both the method and substance of the data breach notification to federal law enforcement agencies to include notice to the Commission, and to impose the same obligations on BIAS providers. Our current breach notification rule requires that voice providers notify the FBI and Secret Service ''through a central reporting facility'' to which the Commission maintains a link on its Web site. We believe that the information currently submitted through the FBI/Secret Service reporting facility is sufficient, and that the same information should be reported under the rule we propose here. We seek comment on our proposal. Are there any additional or alternative categories of information or methods of communication that should be included in these disclosures? To protect individuals' privacy, we do not propose requiring that any personal information about individuals be included in breach reports submitted to the Commission or to other governmental entities. Are there any reasons such personal information should be included, and how could we ensure that any such requirement would be consistent with our goal of protecting the privacy of individuals? Alternatively, should we affirmatively prohibit customer PI from being included in reports submitted to the Commission or other governmental entities?

3. Record Retention

234. We propose to extend our existing Section 222 record retention requirements regarding data breaches to BIAS providers. Currently, voice providers are required to maintain a record of any discovered breaches and notifications to the FBI, the Secret Service, and customers regarding those breaches for a period of at least two years. This record must include, if available, the date that the carrier discovered the breach, the date that the carrier notified the Secret Service and the FBI, a detailed description of the CPNI that was breached, and the circumstances of the breach. As with the rest of our proposal, we propose to extend this requirement to include a detailed description of the customer PI that was breached. We seek comment on this proposal.

235. We seek comment on how telecommunications carriers subject to our existing Section 222 rules have found the current Section 222 requirement to work in practice. What have been the costs for compliance with this provision? Is any of the information that we propose to be retained unnecessary? Are there additional categories of information that should be retained? We also seek comment whether this requirement has proved useful to law enforcement needs. We seek comment on other potential alternatives. What are the benefits and drawbacks of any alternative approaches?

4. Harmonization

236. We seek comment on our proposal to apply new data breach notification requirements to both voice and BIAS providers. Both BIAS providers and providers of voice telephony receive sensitive information from customers, including about usage of the service provided. When this information is compromised, customers may suffer substantial financial, privacy-related, and other harms. Accordingly, we ask commenters to explain whether our proposed rules should apply equally to all providers of telecommunications services. We are interested in understanding any efficiencies gained or potential problems caused by harmonizing the data breach notification rules across technologies. Are there any reasons that BIAS providers and other telecommunications carriers should have different notification requirements for breaches of customer PI? If so, what requirements should we adopt in the BIAS and voice contexts? We also seek comment on whether we should adopt harmonizing rules for cable and satellite providers.

5. Third-Party Data Breach Notification

237. As a final matter, we seek comment on how our rules should treat data breaches by third parties with which a BIAS provider has shared customer PI. Should we require BIAS providers to contractually require third parties with which they share customer PI to follow the same breach notification rules we adopt for BIAS? Are such contractual safeguards necessary to ensure that third-party breaches are discovered and the relevant parties notified on a timely basis? Should we permit BIAS providers and third parties to determine by contract which party will provide the notifications required under our rules when there is a third-party breach? Where third parties are contractually obligated to provide these notifications, should BIAS providers be required to provide notifications of their own? Could such dual notifications confuse or overwhelm consumers, or would they rather help consumers better understand the circumstances of a breach and hold their providers accountable for their data management practices? Which approach best serves the needs of law enforcement? Are there alternative approaches to third-party data breach notification that we should consider?

G. Practices Implicating Privacy That May Be Prohibited Under the Act

238. We seek comment on whether there are certain BIAS provider practices implicating privacy that our rules should prohibit, or to which we should apply heightened notice and choice requirements. In particular, we propose to prohibit the offering of broadband services contingent on the waiver of privacy rights by consumers, and seek comment on whether practices involving (1) the offering of higher-priced broadband services for heightened privacy protections, (2) the use of deep packet inspection (DPI) for purposes other than network management, and (3) persistent identifiers should be prohibited or subject to heightened privacy protections. On what statutory basis could we rely to prohibit such practices? We seek comment on whether such practices are consistent with preserving customer choice, protecting the confidentiality of customer proprietary information, and the public interest. We also seek comment on the restrictions imposed on carriers' use of proprietary information in Section 222(b).

239. We encourage commenters who suggest heightened notice and choice requirements for certain practices to describe the consent regime that they propose, explain why it is appropriate for the practice at issue, and identify the statutory authority that supports such requirements. For instance, would requiring carriers to ''refresh'' opt-in or opt-out consent periodically for certain practices be appropriate? Should more prominent notice or specific prescribed text be required in certain instances? Should we work with interested stakeholders to develop privacy best practices guidelines and create a ''privacy protection seal'' that BIAS providers could display on their Web sites to indicate compliance with those guidelines? For any alternatives commenters propose, we ask that they also comment on the benefits and burdens of their proposals, particularly for small providers. Are there certain types of practices for which a notice-and-choice regime is insufficient to protect consumer privacy? Why or why not? What are viable alternatives to

notice and choice and what are their associated benefits and burdens, particularly for small providers? Are there ways that the Commission can encourage BIAS providers to engage in privacy-by-design practices to build privacy protections into new or existing systems and products?

240. *Service Offers Conditioned on the Waiver of Privacy Rights.* We propose to prohibit BIAS providers from making service offers contingent on a customer surrendering his or her privacy rights. The FTC has raised concerns about these kinds of arrangements by broadband providers, noting that ''[w]hen consumers have few options for broadband service, the take-it-or-leave-it approach [to privacy] becomes one-sided in favor of the service provider.'' In such situations, the FTC found, for example, that ''the service provider should not condition the provision of broadband on the customer's agreeing to . . . allow the service provider to track all of the customer's online activity for marketing purposes.'' We seek comment on our proposal to prohibit these types of arrangements, and on alternative approaches we might take to protect broadband consumers from potentially coercive service offerings. Notwithstanding their risks, are there countervailing consumer benefits associated with these types of offers to provide BIAS?

241. *Financial Inducement Practices.* We also seek comment on whether business practices that offer customers financial inducements, such as lower monthly rates, for their consent to use and share their confidential information, are permitted under the Communications Act. Certain broadband providers, including AT&T, have begun to experiment with these types of business models. For example, AT&T's Gigapower fiber-to-the-premises (FTTP) service currently offers consumers a ''Premiere'' pricing option, which, in exchange for a rate that is roughly $30 off of the standard $100 monthly subscription fee, allows AT&T to use ''individual Web browsing information,'' including search and browsing history ''to tailor ads and offers to [customers'] interests.'' AT&T has reportedly indicated that since its debut, a substantial majority of its Gigapower customers have elected to participate in the discounted Internet Preferences program.

242. We recognize that it is not unusual for consumers to receive perks in exchange for use of their personal information. In the brick-and-mortar world, loyalty programs that track consumers purchasing habits and provide rewards in exchange for that information are common. In the broadband ecosystem, ''free'' services in exchange for information are common. However, it is not clear that consumers generally understand that they are exchanging their information as part of those bargains.

243. Notwithstanding the prevalence of such practices in other contexts, the FTC and others have argued that these business models unfairly disadvantage low income or other vulnerable populations who are unable to pay for more expensive, less-privacy invasive service options. Others have warned that these types of financial inducements could become ''coercive tools to force consumers to give up their statutory rights.'' We seek comment on these concerns. What is the current impact on low-income consumers and others of business practices that offer financial inducements in return for customers' consent to their broadband providers using and sharing confidential information? What is likely to be the impact if such practices become more wide-spread among broadband providers?

244. Given these concerns, Should we adopt rules concerning the use of such practices by BIAS providers? Should the offering of such practices be subject to the opt-out or opt-in frameworks we propose above? Our proposed rules require BIAS providers to allow customers to deny or withdraw approvals at any time and require that a denial or withdrawal will not affect the provision of any services to which the customer subscribes. Are these principles consistent with allowing financial inducements? If we were to allow financial inducements, how should a rule allowing withdrawal of approval work? Should such practices be subject to heightened notice and choice requirements, and, if so, what requirements? Section 222(c)(1) prohibits providers from using or disclosing individually identifiable CPNI for purposes other than providing the telecommunications service, absent customer approval. We seek comment whether a customer's approval to use or disclose his or her proprietary information in exchange for financial incentives is meaningful if customers' broadband choices are limited by lack of competition, switching costs, or financial hardship. Does simply offering such practices violate providers' baseline duty under Section 222(a) to protect the confidentiality of customers' proprietary information? Should BIAS providers be prohibited from engaging in such practices?

245. Despite the risks discussed above, some have argued that consumers stand to benefit from the sale of personal information collected by entities such as ISPs and other telecommunications companies. In light of these potential consumer benefits, should we accept that, upon being fully informed about the privacy rights they are exchanging for a discounted broadband price, consumers can and should be allowed to enter into such bargains? Are there any baseline privacy protections with which providers should be required to comply? If instances arise where it appears that the providers is offering subscribers financial inducements to waive their privacy rights the value of which far exceed the value to the provider of the customer's data, how should we evaluate such offers?

246. *Deep Packet Inspection.* We seek comment whether the use of DPI for purposes other than providing broadband services, and reasonable management thereof, should be prohibited or otherwise subject to a heightened approval framework. DPI involves analyzing Internet traffic beyond the basic header information necessary to route a data packet over the Internet. DPI is used by network operators to gather information about the contents of a particular data packet, and may be used for reasonable network management, such as some tailored network security practices. In addition, DPI has been used by network providers in order to serve targeted advertisements. DPI has also been used by network providers to identify and block specific packets.

247. The FTC has found that the use of DPI by Internet service providers for marketing purposes raises unique privacy concerns. Noting that broadband providers are uniquely situated as a ''gateway'' to the Internet, the FTC has found that ''ISPs are thus in a position to develop highly detailed and comprehensive profiles of their customers—and to do so in a manner that may be completely invisible.'' The 2012 FTC Privacy Report also noted that switching costs and a lack of competitive options for broadband service may inhibit consumers' ability to avoid these practices, should they wish to do so. As a result, the FTC voiced ''strong concerns about the use of DPI for purposes inconsistent with an ISP's interaction with a consumer,'' and called for express consumer consent requirements, or more robust protections, as a precondition for their use.

248. We seek comment whether BIAS providers' use of DPI for purposes other

than providing broadband services, or as required by law, should be prohibited. Should such practices be subject to either the opt-out or opt-in requirements we have proposed above, or heightened approval requirements? For what purposes do broadband providers engage in DPI? What would be the benefits and drawbacks of prohibiting the use of DPI for purposes other than providing BIAS? What would be the costs to consumers and BIAS providers of such a prohibition?

249. Under what authority could the Commission regulate or prohibit DPI practices? For example, do such practices violate a provider's duty to protect the confidentiality of customer information under Section 222(a)? Do such practices violate a provider's duties under Section 705? We also seek comment about the extent to which adoption of encryption technology would mitigate privacy concerns regarding broadband provider use of DPI. What types of information that may be learned by BIAS providers' use of DPI are encrypted, and what types are not encrypted? To what extent does an end user have control over the use of encryption? How, if at all, should the extent of BIAS competition and switching costs for BIAS be taken into account in addressing the impact of DPI on consumer privacy protection?

250. *Persistent Tracking Technologies.* We seek comment whether the use of persistent tracking technologies should be prohibited, or subject to opt-out or opt-in consent. Under our proposed rules, certain types of information used in persistent tracking technologies, such as unique identifiers, would be considered both CPNI and PII. The use of persistent tracking technologies may allow network operators to obtain detailed insight into their customers' Internet usage. For example, UIDH, injected by carriers into the HTTP header of a data packet, allow BIAS providers to repackage and use customer data for targeted advertising purposes. Unlike cookies, which are located in a web browser and may be controlled locally, UIDH are injected by carriers at the network level, thereby preventing customers from removing them directly. The Enforcement Bureau recently entered into a consent decree with a carrier that used UIDH without obtaining informed consent from its customers. As part of the Consent Decree, the carrier paid a fine and agreed to obtain opt-in approval from its customers before sending UIDH to third-party Web sites.

251. We seek comment on what other technologies can be used by BIAS providers to track broadband users and their devices, either by storing information (*e.g.,* cookies), collecting partially unique information (*e.g.,* fingerprinting) or associating information at the network level (*e.g.,* UIDH). Do these technologies pose a privacy risk to BIAS customers and, if so, what are the best ways to protect customers' private information and enhance customer control?

252. We seek comment on whether the use of persistent tracking technologies may expose BIAS customers to unique privacy harms, and as such, whether the Commission should prohibit BIAS providers from employing such practices to collect and use customer PI and CPNI. Alternatively, should the use of persistent tracking technologies be subject to opt-in or opt-out consent? Do customers understand how BIAS providers are using this technology such that notice and the opportunity to approve such uses is ''informed''? How do BIAS providers use the information gleaned from such technologies? What are the benefits to customers of such technology, if any? What would be the benefits and drawbacks to prohibiting such practices, or subjecting their use to opt-in or opt-out approval? Under what authority could the Commission prohibit BIAS providers' deployment of such technologies? Does the use of such technology violate BIAS providers' duty to protect the confidentiality of customer information, with or without customer approval? Does it violate any other provisions of the Communications Act?

253. *Section 222(b).* We also seek comment on how best to interpret and apply in the BIAS context the limitations imposed by Section 222(b) on carriers receiving proprietary information from other carriers for the purposes of providing telecommunications services. Under Section 222(b), a ''telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts.'' The Commission has previously interpreted this section as applying specifically to carriers' propriety information. Should we understand this section as protecting information about all of the traffic that a BIAS provider receives from another provider from being used by the receiving BIAS provider for any purpose other than the provision of the telecommunications service? Should we understand this provision to be referring only to information that is proprietary to a telecommunications carrier, or to all three types of proprietary information referred to in Section 222(a)—''proprietary information of or relating to telecommunications carriers, equipment manufacturers and customer proprietary information?'' What are the privacy implications of the different readings of this provision?

254. *Other.* Lastly, we seek comment whether there are other uses or disclosures of customer PI, other than those we have here described, that should be prohibited or subject to heightened notice and choice requirements. If so, what are they, and why should they be prohibited or subject to more stringent notice and choice requirements? On what authority could we act to prohibit such practices?

H. Dispute Resolution

255. We seek comment on whether our current informal complaint resolution process for alleged violations of the Communications Act is sufficient to address customer concerns or complaints with respect to the collection, use, and disclosure of customer information covered by our proposed rules. At present, customers who experience privacy violations may file informal complaints through the Consumer Inquiries and Complaints Division of the Consumer & Governmental Affairs Bureau. Are these mechanisms adequate? If not, we seek comment on whether BIAS providers currently do or should provide other optional, impartial, and efficient dispute resolution mechanisms. Such programs, if structured fairly and operated efficiently, could help customers resolve privacy complaints more quickly and with less cost than formal complaints to the Commission or private litigation. However, if procedures are not carefully structured, BIAS providers could use dispute resolution programs to disadvantage customers and deny them the full panoply of due process rights they would receive through formal legal processes.

256. BIAS providers are of course free to offer arbitration as a method of dispute resolution. Arbitration can be a useful tool in the dispute resolution toolkit, but it may not suitable for all situations. We seek comment on whether to prohibit BIAS providers from compelling arbitration in their contracts with customers. In the *2015 Open Internet Order,* we agreed with the observation that ''mandatory arbitration, in particular, may more frequently benefit the party with more resources and more understanding of the dispute procedure, and therefore should not be

adopted.'' We further discussed how arbitration can create an asymmetrical relationship between large corporations that are repeat players in the arbitration system and individual customers who have fewer resources and less experience. Just as customers should not be forced to agree to binding arbitration and surrender their right to their day in court in order to obtain broadband Internet access service, they should not have to do so in order to protect their private information conveyed through that service.

257. We additionally seek comment on any other dispute resolution proposals we should consider in conjunction with this rulemaking, including whether and how to harmonize such proposals with our existing voice CPNI framework. To the extent we should adopt any dispute resolution requirements, we seek comment on how to ensure access to dispute resolution for customers with disabilities. For all dispute resolution proposals, we seek comment on the benefits and burdens of such proposals—in particular the burdens such proposals would place on small providers—and any reasonable alternatives that could alleviate associated burdens.

I. Preemption of State Law

258. Consistent with the Commission's approach to the current Section 222 rules, we propose to preempt state laws only to the extent that they are inconsistent with any rules adopted by the Commission. The states are very active participants in ensuring their citizens have robust privacy and data security protections, and we do not intend to curtail their work. However, the Commission is tasked with implementing the requirements of Section 222, and as the Commission has previously found, 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.' ''

259. We observe that the Commission has interpreted this limited exercise of its preemption authority to allow states to craft laws regarding the collection, use, disclosure, and security of customer data that are more restrictive than those adopted by the Commission, provided that regulated entities are able to comply with both federal and state laws. Our proposal is consistent with the approach adopted by the Commission in prior CPNI Orders, and is in line with the Commission's goal of allowing states to craft their own laws related to the use of personal information, including CPNI. Therefore, as the Commission has done in previous CPNI orders, we propose to preempt inconsistent state laws on a case-by-case basis, without the presumption that more restrictive state requirements are inconsistent with our rules. We seek comment on this proposal, and on any alternative approaches we may take to state laws governing customer PI collected by BIAS providers and addressed by our proposed rules. Specifically, we seek comment on whether broader application of our preemption authority is warranted, or, alternatively, whether we should decline to preempt state law in this area altogether. We seek comment on the benefits and risks presented by these competing approaches to preemption.

J. Other Proposed Frameworks and Recommendations

260. Various stakeholders have publicly proposed BIAS privacy frameworks and recommendations for us to consider. These include frameworks offered by a coalition of industry associations that includes a number of BIAS providers (Industry Framework), New America's Open Technology Institute (OTI Framework), Public Knowledge (PK Framework), the Electronic Privacy Information Center (EPIC Framework), the Information Technology and Innovation Foundation (ITIF), and Digital Content Next (Digital Content Framework). Like the proposals in this Notice, all of the stakeholder proposals include components that would impose transparency, choice, and security obligations on confidential consumer information collected by BIAS providers, and we have incorporated some of their recommendations in to our own. However, we recognize that our consideration of how best to ensure BIAS providers protect the confidentiality of their customers' information could also benefit from feedback on these alternative proposals as a whole. We therefore describe each proposed framework briefly in turn, and seek comment on their proposals, as additions to or substitutes for our own.

261. In addition to seeking comment on each of these sets of proposals, we seek comment on how these separate proposals correspond with our proposed framework. Are there aspects of them that should be incorporated into our proposal? We note that there is broad agreement about the importance of transparency, choice, and data security, but in other ways some of the proposals appear to be inconsistent with each other. How should those inconsistencies be resolved? Does our definition of key terms, including CPNI, customer PI, and personally identifiable information, account for the scope of protections and obligations contemplated under these proposals, given possible discrepancies in how those terms are defined between different frameworks?

262. *Industry Framework.* The Industry Framework proposes four principles that we should consider when adopting privacy rules: (1) Transparency; (2) respect for context/consumer choice; (3) data security; and (4) data breach notification. The proponents of the Industry Framework also recommend that any privacy rules we adopt should be limited to prohibiting unfair and deceptive practices, as outlined in the FTC's Policy Statements. They also argue that any such privacy rules should (and lawfully can) only apply to telecommunications service providers in the provision of telecommunications service, and only to CPNI that is made available by virtue of the customer-carrier relationship. They also contend that any such rules should not apply to any information that has been de-identified, aggregated, or does not otherwise identify a known individual.

263. The proponents of the Industry Framework also recommend a general approach of setting privacy or security goals, rather than methods by which those goals are to be achieved, and suggests that we should, beyond issuing rules, provide additional guidance on interpreting the privacy framework through workshops or reports, and encourage and support industry guidelines. They also recommend harmonizing the existing CPNI guidelines with any BIAS guidelines we adopt and that we should adopt more flexible standards than are currently part of the Section 222 rules.

264. The Industry Framework also details more specific principles to which it believes BIAS providers should adhere. First, the Industry Framework specifies that BIAS providers should give notice that is neither deceptive nor unfair that describes the collection, use, and sharing of CPNI with third parties. Second, the Industry Framework recommends requiring BIAS providers to provide consumer choice where the failure to do so would be deceptive or unfair. However, the Industry Framework specifies that consumers need not be given a choice when their information will be used for product or service fulfillment, fraud prevention, compliance with law, responses to government requests, network

management, first-party marketing, and affiliate sharing where the affiliate relationship is reasonably clear to consumers. Third, the Industry Framework recommends that BIAS providers maintain a CPNI data security program that has reasonable protections to prevent unauthorized access, use, or disclosure, concomitant with the nature and scope of the company's activities, the sensitivity of the data, and the size and complexity of the company's data operation. Fourth, the Industry Framework recommends requiring BIAS providers to notify customers of data breaches when a breach is likely to cause substantial harm to customers and failure to notify would be unfair or deceptive, with providers having the flexibility to determine how and when to provide notice. We seek comment on these proposals.

265. *OTI Framework.* The OTI Framework begins by recommending that we adopt a broad definition of CPNI in the broadband context, which would include subscriber location information; sites visited; specification of connected devices; and time, amount, and type of Internet traffic. The OTI Framework also proposes that the definition of CPNI should be expanded ''where appropriate'' to account for ''new risks in broadband context,'' and that we should define (and presumably protect) ''proprietary information'' as defined in the *TerraCom NAL.* With that proposed definition in place, the OTI Framework makes several specific policy recommendations on (1) notice and consent, (2) disclosure of CPNI to customers, (3) data security and breach notification, (4) complaint process, and (5) differential privacy protections based on price. In the matters of notice and consent, the OTI Framework recommends that we require BIAS providers to give accurate and reasonably specific notice of uses of information and of any third parties to whom the information will be disclosed. The OTI Framework proposes opt-in consent for all non-service-related uses of CPNI. The OTI Framework also appears to suggest that we provide rules or other guidance on how BIAS providers might disclose CPNI to customers, as required under Section 222(c)(2). The OTI Framework also recommends required data breach notification similar to the existing CPNI rules. The OTI Framework proposes a formal complaint process for violations of the privacy rules similar to the processes for wireline and wireless telephony. Finally, the OTI Framework proposes prohibiting BIAS providers from charging subscribers for the baseline privacy protections specified in the OTI Framework. We seek comment on these proposals.

266. *PK Framework.* In its proposed privacy framework, Public Knowledge recommends that we restate and adopt the framework of the *2007 CPNI Order,* which it argues would include finding all PII within the scope of CPNI, not implementing a safe harbor rule, and requiring carriers to improve data security protections of their own accord as new precautions become available, without requiring additional rulemaking. Public Knowledge proposes that BIAS providers, and not customers, bear the burden of ensuring privacy protections, while allowing customers to engage in privacy-enhancing practices themselves. In particular, this means that the availability of customer-initiated protections like encryption and VPNs does not absolve BIAS providers from protecting the information of customers who do not purchase or deploy those solutions. Public Knowledge also recommends that we prohibit BIAS providers from interfering with customers' privacy enhancing tools and techniques, such as blocking tracking software or clearing it from caches.

267. The PK Framework also includes recommendations on two particular practices: Deep packet inspection and differential privacy protections based on discounts or other inducements. With regard to deep packet inspection, the PK Framework suggests that consent to use or disclose CPNI does not mean consent to use or disclose communications content. Public Knowledge further recommends that we prohibit ''*any* provider under *any* circumstances from using DPI or other tools to view the content of subscriber traffic.'' With regard to differing privacy protections, the PK Framework recommends prohibiting BIAS providers from ''coercing consent'' from customers by charging fees or withholding functionality of services that a subscriber ''reasonably believes are included as part of the purchase of [BIAS].'' However, the PK Framework does not recommend a categorical prohibition on inducements to consent, though it cautions that some ''discounts'' and ''services'' may be disguised coercive tools, and that discounts could have a disparate impact against the privacy of lower-income customers.

268. Finally, the PK Framework recommends that we seek comment on supplementing the privacy and competition protections of Section 222 with rules based on our authority over cable and wireless providers. With regard to privacy, the PK Framework recommends enhancing cable privacy rules under Section 631 and wireless privacy under Section 303(b) to ensure that protections based in Section 222 can be equally applied in those contexts. With regard to competition, the PK Framework recommends supplementing competition-enhancing rules derived from Section 222 with authority from Section 628 and Section 303(b), to prevent anticompetitive uses of customer information in wireless and video services, including over-the-top video services. We seek comment on these proposals.

269. *EPIC Framework.* EPIC makes five recommendations for privacy rules. First, it argues that the rules should apply the FIPPs, as outlined in the HEW Report and the Consumer Privacy Bill of Rights. Second, it recommends data minimization requirements, including rules limiting the collection of data, requiring the disposal or de-identification of data that is no longer needed, and requiring reasonable data retention and disposal policies. EPIC opposes mandatory data retention and recommends data be retained for the shortest period possible. Third, the EPIC Framework recommends we promote privacy enhancing technologies such as ''Do Not Track'' mechanisms. Fourth, the EPIC Framework argues that all Internet-based service providers obtain opt-in consent for the use or disclosure of consumer data.

270. EPIC also recommends that the rules incorporate its Code of Fair Information Practices for the National Information Infrastructure, which itself incorporates several principles and recommendations, including: Protecting the confidentiality of electronic communications; limiting data collection; requiring explicit consent for service provider disclosure; requiring providers to disclose data collection practices; prohibiting payment for routine privacy protection, and allowing charges only for ''extraordinary'' privacy protection; appropriate security policies; and an enforcement mechanism. We seek comment on these proposals.

271. *ITIF Recommendations.* In a paper on broadband privacy, ITIF makes a number of recommendations, beginning with a recommendation that we forbear from the application of Section 222 to BIAS. Alternatively, ITIF recommends that we declare the privacy policies of BIAS providers as non-common carrier services, thus allowing the FTC to exercise jurisdiction over their privacy practices. ITIF's third proposal is that we limit rules to those which correspond as much as possible

to the FTC's past privacy enforcement in this area. ITIF suggests that any fines enforcing such rules be tied to actual consumer harm and amplified when the harm was intentional. The ITIF Recommendations also suggest that we should support and encourage the continued formation of industry best practices; the development of experiments with pricing around new uses of consumer data; and the use, disclosure, and sharing of aggregate and de-identified customer data. We seek comment on these proposals.

272. *Digital Content Framework.* Digital Content Next stresses the importance of respecting consumers' expectations within the context of the interaction, as well as providing consumers with transparency and choice. The Digital Content Framework further recommends that, in the context of BIAS providers, the contrast between the amount of information collected and the customers' expectations of how that information is to be used suggests that service providers should be held to a higher standard than other participants in the online ecosystem.

273. Digital Content Next recommends we require broadband providers to provide consumers with transparency and meaningful choice, particularly when information is used outside of consumer expectations and outside of the context in which the information was initially given. Digital Content Next more specifically suggests that we follow the pattern of our existing Section 222 rules, allowing opt-out approval for marketing services similar to the providers' and requiring opt-in approval for broader marketing or advertising. The Digital Content Framework further recommends that the choice mechanisms should be clear, easy to use, and persistent, suggesting that they could take the form of account settings set up by the provider, or the recognition of signals sent by a device or a browser. Digital Content Next also recommends we work with self-regulatory bodies, the FTC, and BIAS providers on developing business practices and technologies, including how to account for customers' privacy choice mechanisms across multiple devices and in cross-device tracking. We seek comment on these proposals.

274. *Other.* Finally, we seek comment on any alternative approaches we can take to protect customer privacy, preserve customer control, and promote innovation, as well as the benefits and burdens associated with any such alternatives.

K. Multi-Stakeholder Processes

275. We seek comment on whether there are specific ways we should incorporate multi-stakeholder processes into our proposed approach to protecting the privacy of customer PI. The Department of Commerce's 2010 Green Paper recommended use of multi-stakeholder processes to clarify how the FIPPs should be applied in particular commercial contexts. Since then, the Department of Commerce through NTIA has convened multi-stakeholder processes on several topics, including mobile application transparency, facial recognition technology, and unmanned aircraft systems. The Administration's Privacy Bill of Rights also incorporates multi-stakeholder processes into its framework. We seek comment on what lessons have been learned from the multi-stakeholder processes that NTIA has convened on behalf of the Department of Commerce. Would such processes be useful in developing guidelines and best practices relating to these proposed rules? Above we have sought comment on whether aspects of our proposed rules, such as notice language or security standards would benefit from a multi-stakeholder process such as that conducted by NTIA. Would a similar process be useful to address the privacy practices of broadband providers more generally, or in other specific areas? If so, how should the process be managed and governed? Should such processes serve as a supplement or an alternative to further rulemaking?

III. Legal Authority

276. In this section, we discuss and seek comment on our statutory authority to adopt the rules we propose in this Notice and for any other rules that we may conclude, as a result of this proceeding, to be in the public interest. Since the enactment of the Communications Act of 1934, there has been an expectation that providers of communications services have obligations to protect both the security and the privacy of information about their customers. We intend our proposed rules to be primarily grounded in Section 222. However, we believe that we can also find support in other sections of the Communications Act, including Sections 201 and 202 of the Communications Act, which prohibit telecommunications carriers from engaging in unjust, unreasonable, or unreasonably discriminatory practices; Section 706 of the Telecommunications Act of 1996, as amended (1996 Act), which requires the Commission to use regulating methods that remove barriers to infrastructure investment; and Section 705 of the Communications Act, which restricts the unauthorized publication or use of communications. Taken together, these statutory provisions give us the authority and responsibility to ensure that telecommunications carriers and other service providers protect the confidentiality of private customer information and give their customers control over the carriers' use and sharing of such information.

277. The Act gives us the authority to prescribe rules that may be necessary in the public interest to carry out the Communications Act, and our authority to adopt rules to interpret and implement Section 222's provisions is well established. We welcome comment on the legal framework we offer below for this proceeding and invite commenters to offer their own legal analysis on whether the rules we propose, the alternatives on which we seek comment, and the recommendations that commenters make are consistent with and supported by the statutory authority upon which we rely, or on other statutory authority, including, for example, Sections 631 and 338(i) of the Communications Act. To the extent that commenters offer alternate proposals, we welcome explanations of the extent to which such proposals are consistent with and authorized by Section 222 or other relevant statutory provisions. We focus our discussion in this legal authority section on some of the most significant issues in this proceeding, but we also invite commenters to offer analysis of the Commission's legal authority on all of the rules we propose today.

A. Section 222 of the Communications Act

278. In the sections above, we seek comment on adopting rules that require telecommunications carriers, including providers of BIAS, to protect, and to provide their customers with notice, choice, and data security with respect to their customer PI. As described in more detail below, we believe that these proposals are fully supported by Section 222, and invite comment on that issue.

279. Congress added Section 222 to the Communications Act in 1996. Section 222, entitled ''Privacy of customer information,'' established a new statutory framework governing carrier use and disclosure of customer proprietary network information and other customer information obtained by carriers in their provision of telecommunications services. Fundamentally, Section 222 obligates telecommunications carriers to protect

the confidentiality of proprietary information, including proprietary information about their customers, and in furtherance of that obligation it requires carriers to seek approval before using or sharing customer proprietary network information. When we reclassified BIAS as a telecommunications service, we determined that forbearance from Section 222 would not serve the public interest because of the importance of ensuring that BIAS customers have strong privacy protections.

280. We recognize that earlier Commission decisions focused primarily on Section 222(c)'s protection of CPNI, and could be read to imply that CPNI is the only type of customer information protected. However, those decisions simply did not need to address the broader protections offered by Section 222(a), and we do not so limit ourselves here. The focus of the earliest decisions implementing Section 222 was generally on the restrictions on use and sharing of individually identifiable CPNI in particular, especially from the perspective of introducing competition into the telecommunications market and replacing the CPNI rules that the Commission had adopted before the 1996 Act, which were focused on protecting independent enhanced service providers and equipment suppliers from discrimination by incumbent local exchange carriers. The duty to secure the confidentiality of customer information beyond CPNI would not have been as substantial a concern in the years before it became so common for information to be stored electronically. In 2007, the Commission strengthened its rules governing secure handling of CPNI in order to address problems that had been identified regarding the advertising and sale of personal telephone records, which are indisputably CPNI, and in doing so acknowledged the general mandate to protect confidentiality in 222(a).

281. Today, when telecommunications services are provided by myriad carriers, and when customers' sensitive information is typically held in digital form that could pose security risks if not managed properly, we believe that Section 222(a) should be understood to mean what it says and that it should not be so narrowly construed. More recently, the Commission made clear its view that the set of customer information protected by Section 222(a) is broader than CPNI in the 2014 *TerraCom NAL,* and reiterated that view in the *2015 Lifeline Reform Order*.

282. In this Notice, we now propose rules that we believe are necessary to implement carriers' obligation to protect customer information that is not CPNI, and we seek comment here specifically on our proposal that subsection (a) of Section 222 provides authority for the Commission to adopt such rules. Furthermore, we understand that the phrase ''protect the confidentiality'' means more than preventing unauthorized access; confidentiality includes the concept of trust, and consumers rightfully expect that information that their BIAS providers acquire by virtue of providing BIAS should be used and shared only for expected purposes. Indeed, we believe that each of the core privacy principles we seek to uphold in this proceeding—transparency, choice, and security—is built into the authority granted by Section 222.

283. *Transparency.* We have often exercised our authority under Section 222 to describe the types of notice that would be necessary to constitute ''approval'' under Sections 222(c)(1), (c)(2), and (d)(3). Without adequate disclosure, consumers cannot truly be held to have approved any given use or sharing of their information. Furthermore, we believe that adequate disclosure of privacy and security practices is necessary to protect the confidentiality of proprietary information of and relating to customers. Disclosure helps to ensure that consumers, and not only service providers, can assign the appropriate weight to the privacy of their information compared to the value of allowing the service provider to use or share the information. We also tentatively conclude that adequate transparency is necessary to ensure that BIAS providers' practices are just, reasonable, and not unreasonably discriminatory, and that disclosures are in fact a necessary part of providing just and reasonable service. Finally, we believe that transparency obligations do not constitute unconstitutionally compelled speech under the First Amendment, and we seek comment on that issue.

284. *Choice.* Customer approval is a key component of the privacy framework of Section 222, and a core part of our existing CPNI rules. Our proposed rules for BIAS providers draw from this framework, requiring customer approval for many uses, but permitting that approval to be granted in an opt-out framework for many uses where an opt-in approval requirement may be overly burdensome. This framework, in the context of our existing rules, was successfully adopted after the Tenth Circuit found an earlier set of rules with fewer opt-out options to be insufficiently supported by the record at the time. The rules we propose here, like the existing CPNI rules, are intended to directly advance both the substantial public interest in consumer privacy as well as Section 222's mandate to protect customer confidentiality, while not being more extensive than necessary to serve those interests, according to the criteria of *Central Hudson.* For customers to be able to protect their privacy, they must have a way to easily locate and exercise their options, and they must be able to give or withhold their consent for uses of their information not directly related to the provision of their service. These proposed rules correspond with well-established rules in the voice context, and allow for a number of uses with no additional approval, or opt-out or opt-in approval, from customers, imposing no more restrictions than are necessary to protect customer privacy and control.

285. *Data Security and Breach Notification.* Section 222 leaves no doubt that every telecommunications carrier has a duty to protect its customers' proprietary information. The Commission has referred specifically to Section 222(a) as imposing security obligations on telecommunications carriers and providing authority to the Commission to adopt security-focused rules, and we have implemented security and data breach obligations on CPNI under the more specific auspices of Section 222(c). We believe that the same authority justifies the revised breach notification requirements we propose in this Notice, including the requirement that carriers notify customers, law enforcement, and the Commission of breaches of customer PI that is not CPNI. We also do not believe that such breach notification requirements, which are common in other sectors and in many states, constitute unjustified compelled speech that implicates the First Amendment.

B. Additional Statutory Authority

286. We also believe that our proposals find support in a number of other statutory provisions, which provide authority to protect against unjust, unreasonable, and unreasonably discriminatory practices; interception or divulgence of communications; and the untimely deployment of advanced telecommunications services. An additional source of authority includes our particular authority over wireless licensees.

1. Sections 201–202 of the Communications Act

287. In the *2015 Open Internet Order,* we interpreted Section 201 and 202 in the broadband Internet access services context through our adoption of the ''no-unreasonable interference/disadvantage'' standard. That standard, which is codified in our rules at Section 8.11, ''is specifically designed to protect against harms to the open nature of the Internet.'' Of particular relevance for the proceeding initiated by this Notice, we found that ''practices that fail to protect the confidentiality of end users' proprietary information, will be unlawful if they unreasonably interfere with or disadvantage end user consumers' ability to select, access or use broadband services, applications, or content.'' Against that backdrop, we seek comment on how our interpretation of Sections 201 and 202 in the broadband Internet access services context should inform rules adopted in this proceeding to address consumer privacy and security.

288. We also note that Section 5 of the Federal Trade Commission Act declares that unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce are unlawful. There is a distinct congruence between practices that are unfair or deceptive and many practices that are unjust, unreasonable, or unreasonably discriminatory. Indeed, both Commissions have found that Section 201 of the Communications Act and Section 5 of the FTC Act can be read as prohibiting the same types of acts or practices, and the FTC has a rich body of precedent, in enforcement actions and consent orders, that measures privacy and data-security practices against the unfair-or-deceptive standard. Although the FTC lacks statutory authority to prevent common carriers from using such unfair or deceptive acts or practices, we seek comment on the extent to which Section 5 of the FTC Act and the FTC's precedents may inform our consideration of whether practices by common carriers are unjust or unreasonable.

2. Section 705 of the Communications Act

289. Section 705 of the Communications Act has been in place since the adoption of the Communications Act in 1934. Section 705(a) establishes that providers of communications services by wire and radio have obligations not to ''divulge or publish the existence, contents, substance, purport, effect, or meaning'' of communications that they carry on behalf of others. We believe that Section 705 can thus provide a source of authority for rules protecting the privacy of customer information, including the content of their communications. Do commenters agree? To what extent do Section 705, as well as provisions of Title 18 of the United States Code, currently limit the practices of BIAS providers? To what extent might it be necessary for the Commission to use its authority to interpret and implement Section 705 to protect subscribers to BIAS services?

3. Section 706 of the Telecommunications Act of 1996

290. Section 706(a) of the Telecommunications Act of 1996 directs the Commission to take actions that ''shall encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans.'' To do so, the Commission may utilize, ''in a manner consistent with the public interest, convenience, and necessity, price cap regulation, regulatory forbearance, measures that promote competition in the local telecommunications market, or other regulating methods that remove barriers to infrastructure investment.'' In addition, Section 706(b) provides that the Commission ''shall take immediate action to accelerate deployment of such capability by removing barriers to infrastructure investment and by promoting competition in the telecommunications market,'' if it finds after inquiry that advanced telecommunications capability is not being deployed to all Americans in a reasonable and timely fashion. In *Verizon* v. *FCC,* the DC Circuit upheld the Commission's transparency rule as authorized pursuant to Section 706. In doing so, it upheld the Commission's judgment that Section 706 constitutes an independent source of affirmative statutory authority to regulate BIAS providers. The Commission reaffirmed that view in the *2015 Open Internet Order*.

291. We believe that rules governing the privacy and security practices of BIAS providers, such as those discussed in this Notice, would be independently supported by Section 706. We also believe that the proposed transparency, choice, and security requirements further align with the virtuous cycle of Section 706, since they have the potential to increase customer confidence in BIAS providers' practices, thereby boosting confidence in and therefore use of broadband services, which encourages the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans. We seek comment on this analysis.

4. Title III of the Communications Act

292. Section 303(b) of the Act directs the Commission to, ''as public convenience, interest, or necessity requires,'' ''[p]rescribe the nature of the service to be rendered by each class of licensed stations and each station within any class.'' Section 303(r), furthermore, directs the Commission to make rules and regulations, and prescribe restrictions and conditions, to carry out the Act. In addition, 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.'' To the extent that BIAS is provided by licensed entities providing mobile BIAS, these provisions would appear to support adoption of rules such as those we consider in this proceeding. We seek comment on this conclusion.

IV. Procedural Matters

A. Ex Parte Rules

293. This proceeding shall be treated as a ''permit-but-disclose'' proceeding in accordance with the Commission's *ex parte* rules. Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with rule 1.1206(b). In proceedings governed by rule 1.49(f) or for which the Commission has made available a

method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (*e.g.,* .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

B. Accessible Formats

294. 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).

C. Paperwork Reduction Act

295. This NPRM seeks comment on potential new or revised information collection requirements. If the Commission adopts any new or revised information collection requirements, the Commission will publish a notice in the **Federal Register** inviting the public to comment on the requirements, as required by the Paperwork Reduction Act of 1995, Public Law 104–13 (44 U.S.C. 3501–3520). In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107–198, see 44 U.S.C. 3506(c)(4), the Commission seeks specific comment on how it might ''further reduce the information collection burden for small business concerns with fewer than 25 employees.''

D. Contact Person

296. For further information about this proceeding, please contact Sherwin Siy, FCC Wireline Competition Bureau, Competition Policy Division, Room 5–C225, 445 12th Street SW., Washington, DC 20554, (202) 418–2783, *sherwin.siy@fcc.gov.*

V. Ordering Clauses

297. Accordingly, *it is ordered,* pursuant to Sections 1, 2, 4(i)–(j), 201(b), 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(b), 222, 303(b), 303(r), 316, 338(i), 605, and 1302, that this Notice of Proposed Rulemaking *is adopted.*

298. *It is further ordered* that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, *shall send* a copy of this Notice of Proposed Rulemaking, including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

Initial Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA), the Commission has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on a substantial number of small entities by the policies and rules proposed in this Notice of Proposed Rulemaking (NPRM or Notice). Written public comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments on the Notice provided on the front page of this item. The Commission will send a copy of the Notice, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).

A. Need for, and Objectives of, the Proposed Rules

2. In this NPRM, we propose to apply the traditional privacy requirements of the Communications Act to the most significant communications technology of today: broadband Internet access service. Our approach can be simply stated: *First,* consumers must be able to protect their privacy, which requires transparency, choice, and data security. *Second,* BIAS providers are the most important and extensive conduits of consumer information and thus have access to very sensitive and very personal information that could threaten a person's financial security, reveal embarrassing or even harmful details of medical history, or disclose to prying eyes the intimate details of interests, physical presence, or fears. But, *third,* the current federal privacy regime does not now comprehensively apply the traditional principles of privacy protection to these 21st Century telecommunications services provided by broadband networks. That is a gap that must be closed, and this NPRM proposes a way to do so by securing what Congress has commanded—the ability of every telecommunications user to protect his or her privacy.

3. Privacy protects important personal interests. Not just freedom from identity theft or financial loss but also from concerns that intimate, personal details should not become grist for the mills of public embarrassment or harassment or the basis of opaque, but harmful judgments, such as discrimination. The power of modern broadband networks is that they allow consumers to reach from their homes (or cars or sidewalks) to the whole wide world instantaneously. The accompanying concern is that those broadband networks can now stand over the shoulder of every subscriber who surfs the web, sends an email or text, or even walks down a street carrying a mobile device. Absent legally-binding principles, those networks have the ability and incentive to use and share extensive and personal information about their customers. The protection of privacy thus both protects individuals and encourages use of broadband networks.

B. Legal Basis

4. The legal basis for any action that may be taken pursuant to the Notice is contained in Sections 1, 2, 4(i)–(j), 201(b), 222, 303(r), 338(i), 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(b), 222, 303(r), 338(i), 605, and 1302.

C. Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply

5. 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 proposed rules, if adopted. 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 Small Business Administration (SBA).

1. Total Small Entities

6. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe here, at the outset, three comprehensive small entity size standards that could be directly affected herein. As of 2014, according to the SBA, there were 28.2 million small businesses in the U.S., which represented 99.7% of all businesses in the United States. Additionally, a ''small organization is generally any not-for-profit enterprise which is independently owned and operated and not dominant in its field''. Nationwide, as of 2007, there were approximately 1,621,215 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 local governmental jurisdictions are small.

2. Broadband Internet Access Service Providers

7. The proposed rules would apply to broadband Internet access service providers (BIAS providers). The Economic Census places these firms, 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 $25 million or less. These are labeled non-broadband. According to Census Bureau data for 2007, there were 3,188 firms in the first category, total, that operated for the entire year. Of this total, 3144 firms had employment of 999 or fewer employees, and 44 firms had employment of 1000 employees or more. For the second category, the data show that 1,274 firms operated for the entire year. Of those, 1,252 had annual receipts below $25 million per year. Consequently, we estimate that the majority of broadband Internet access service provider firms are small entities.

8. 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 IRFA describes the universe of small entities that our action might affect, we discuss in turn several different types of entities that might be providing broadband Internet access service. 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 Initial Regulatory Flexibility Analysis.

3. Wireline Providers

9. *Wired Telecommunications Carriers.* 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. According to Census Bureau data for 2007, there were 3,188 firms in this category, total, that operated for the entire year. Of this total, 3,144 firms had employment of 999 or fewer employees, and 44 firms had employment of 1000 employees or more. Thus, under this size standard, the majority of firms can be considered small.

10. *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 size standard under SBA rules is for Wired Telecommunications Carriers. Under that size standard, such a business is small if it has 1,500 or fewer employees. According to Commission data, 1,307 carriers reported that they were incumbent local exchange service providers. Of these 1,307 carriers, an estimated 1,006 have 1,500 or fewer employees and 301 have more than 1,500 employees. Consequently, the Commission estimates that most providers of local exchange service are small entities that may be affected by rules adopted pursuant to the Notice.

11. *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 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, 1,307 carriers reported that they were incumbent local exchange service providers. Of these 1,307 carriers, an estimated 1,006 have 1,500 or fewer employees and 301 have more than 1,500 employees. Consequently, the Commission estimates that most providers of incumbent local exchange service are small businesses that may be affected by our proposed rules.

12. *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 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, 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 and 186 have more than 1,500 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. In addition, 72 carriers have reported that they are Other Local Service Providers. Of the 72, seventy have 1,500 or fewer employees and two have more than 1,500 employees. Consequently, 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 that may be affected by our proposed rules.

13. 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.

14. *Interexchange Carriers.* Neither the Commission nor the SBA has developed a small business size standard specifically for providers of interexchange services. 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, 359 carriers have reported that they are engaged in the provision of interexchange service. Of these, an estimated 317 have 1,500 or fewer employees and 42 have more than 1,500 employees. Consequently, the Commission estimates that the majority

of IXCs are small entities that may be affected by our proposed rules.

15. *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 our proposed rules.

16. *Other Toll Carriers.* Neither the Commission nor the SBA has developed a size standard 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 size standard under SBA rules is for Wired Telecommunications Carriers. Under that size standard, such a business is small if it has 1,500 or fewer employees. According to 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 and five have more than 1,500 employees. Consequently, the Commission estimates that most Other Toll Carriers are small entities that may be affected by rules adopted pursuant to the Notice.

4. Wireless Providers—Fixed and Mobile

17. The broadband Internet access service provider category covered by these proposed rules may cover multiple wireless firms and categories of regulated wireless services. Thus, to the extent the wireless services listed below are used by wireless firms for broadband Internet access service, the proposed actions may have an impact on those small businesses as set forth above and further below. 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.

18. *Wireless Telecommunications Carriers (except Satellite).* Since 2007, the Census Bureau has placed wireless firms within this new, broad, economic census category. Under the present and prior categories, the SBA has deemed a wireless business to be small if it has 1,500 or fewer employees. For the category of Wireless Telecommunications Carriers (except Satellite), census data for 2007 show that there were 1,383 firms that operated for the entire year. Of this total, 1,368 firms had employment of 999 or fewer employees and 15 had employment of 1000 employees or more. Since all firms with fewer than 1,500 employees are considered small, given the total employment in the sector, we estimate that the vast majority of wireless firms are small.

19. *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.

20. *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.

21. *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.

22. *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.

23. 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.

24. *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.

25. 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.

26. 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.

27. *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.

28. 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.

29. *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.

30. *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.

31. *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.

32. *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.

33. *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.

34. *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.

35. *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.

36. 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.

37. 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

38. *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.

39. 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 2007 show that there were a total of 570 firms that operated for the entire year. Of this total, 530 firms had annual receipts of under $30 million, and 40 firms had receipts of over $30 million. Consequently, we estimate that the majority of Satellite Telecommunications firms are small entities that might be affected by our action.

40. 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 Bureau data for 2007 show that there were a total of 1,274 firms that operated for the entire year. Of this total, 1,252 had annual receipts below $25 million per year. Consequently, we estimate that the majority of All Other Telecommunications firms are small entities that might be affected by our action.

6. Cable Service Providers

41. Because Section 706 requires us to monitor the deployment of broadband using any technology, we anticipate that some broadband service providers may not provide telephone service. Accordingly, we describe below other types of firms that may provide broadband services, including cable companies, MDS providers, and utilities, among others.

42. *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.

43. *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.

44. *Cable System Operators.* The Communications Act of 1934, as amended, 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.'' The Commission has determined that an operator serving fewer than 677,000 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 ten 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, and therefore we are unable to estimate more accurately the number of cable system operators that would qualify as small under this size standard.

7. All Other Telecommunications

45. The Census Bureau defines this industry as including ''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. 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 this category; that size standard is $32.5 million or less in average annual receipts. According to Census Bureau data for 2007, there were 2,383 firms in this category that operated for the entire year. Of these, 2,346 firms had annual receipts of under $25 million and 37 firms had annual receipts of $25 million or more. Consequently, we estimate that the majority of these firms are small entities that may be affected by rules adopted pursuant to the Further Notice.

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

46. This Notice of Proposed Rulemaking proposes and/or seeks comment on several regulations that could affect small providers, including (1) the provision of meaningful notice of privacy policies; (2) customer approval requirements for the use and disclosure of customer PI; (3) the use and disclosure of aggregate customer PI; (4) the security of customer proprietary information; (5) data breach notification; (6) other practices implicating privacy; and (7) dispute resolution.

47. *Meaningful Notice of Privacy Policies.* As discussed above, this Notice proposes to require BIAS providers to provide meaningful notice of privacy policies. The Notice proposes rules and/or seeks comment on the content, location, timing, and formatting of different types of privacy notices. In order to promote transparency and inform all BIAS customers of their privacy choices and security, these proposed rules will apply to small providers as well as large providers. The Notice seeks comment on alternative ways of achieving these goals. The Notice seeks comment on the compliance costs of these proposals for small providers. The Notice also seeks comment on whether to harmonize these proposals with existing regulations regarding voice CPNI, and whether such harmonization can reduce compliance burdens.

48. *Customer Approval Requirements.* As discussed above, this Notice proposes to require BIAS providers to obtain customer approval in order to use, access, or disclose customer proprietary information. This Notice proposes and/or seeks comment on (1) the contexts in which BIAS providers need to seek opt-out and opt-in consent for uses of customer information; (2) the requirements BIAS providers must meet to ensure that customers can easily learn about and effectively express their choices; (3) the ways in which BIAS providers should document their compliance with customers' choices. In order to protect the privacy choices of all BIAS customers, these proposals will apply to small providers as well as large providers. The Notice seeks comment on the effects of these proposals on small providers, as well as whether and how to harmonize these proposals with existing regulations regarding voice CPNI.

49. *Use and Disclosure of Aggregate Customer PI.* As discussed above, this Notice proposes rules and seeks comment on BIAS provider use, access, and disclosure of aggregate customer PI. Our proposed rules would allow BIAS providers, including small providers, to use, access, and disclose aggregate customer PI if the provider (1) determines that the aggregated customer PI is not reasonably linkable to a specific individual or device; (2) publicly commits to maintain and use the aggregate data in a non-individually identifiable fashion and to not attempt to re-identify the data; (3) contractually prohibits any entity to which it discloses or permits access to the aggregate data from attempting to re-identify the data; and (4) exercises reasonable monitoring to ensure that those contracts are not violated. In order to promote all customers' privacy interests in the transparency, choice, and security of how their data is used, these proposals will apply to small providers as well as large providers. We also seek comment on alternative approaches to handling aggregate customer PI, as well as the burdens our proposed rules would place on small providers.

50. *Securing Customer Proprietary Information.* As discussed above, this Notice proposes rules and seeks comment on requiring BIAS providers to protect the security and confidentiality of customer PI by adopting security practices calibrated to the nature and scope of the BIAS provider's activities, the sensitivity of the underlying data, and technical feasibility. These proposals include requiring BIAS providers to protect against unauthorized use or disclosure of customer PI by (1) conducting risk management assessments; (2) training employees to protect against reasonably anticipated unauthorized use or disclosure of customer PI; (3) ensuring reasonable due diligence and corporate accountability; and (4) requiring customer authentication for access to customer proprietary information. We seek comment on how to hold BIAS providers accountable for third party misuse of customer PI and whether we should impose reasonable data collection, retention, and disposal rules. In order to protect the security of all BIAS customers' private information, these proposals will apply to small providers as well as large providers. We also seek comment on alternative approaches to securing customer PI, the burdens the proposed rules would place on small providers, and whether to harmonize our security proposals with existing regulations for voice CPNI.

51. *Data Breach Notification Requirements.* As discussed above, the Notice proposes rules and seeks comment on requiring telecommunications providers to give customers, the Commission, and other law enforcement notice when a breach of customer PI has occurred. In addition, the Notice proposes to harmonize the existing voice CPNI data breach rules with these proposed rules for BIAS provider data breaches. These proposals include (1) requiring telecommunications providers to notify customers within ten days after the discovery of a data breach, subject to law enforcement needs, under circumstances enumerated by the Commission; (2) the necessary content of a customer data breach notification; (3) requiring telecommunications providers to notify the Commission within seven days, and to notify the Federal Bureau of Investigation and the U.S. Secret Service, in the event of a data breach affecting more than 5,000 customers, within seven days; (4) two-year record retention rules for data breaches; and (5) seeking comment on how to address third party data breaches. In order to promote transparency and security for all telecommunications customers, these proposed rules will apply to small providers as well as large providers. The Notice also seeks comment on alternative data breach notification approaches as well as the burdens that our proposals will have on small providers.

52. *Other Practices Implicating Privacy.* As discussed above, the Notice seeks comment on whether there are certain BIAS provider practices implicating privacy that our rules should prohibit, or to which we should apply heightened notice and choice requirements. In particular, the Notice proposes to prohibit service offers conditioned on the waiver of privacy rights. The Notice also seeks comment on how to address (1) financial inducement practices; (2) deep packet inspection for purposes other than

network management; and (3) persistent tracking technologies. In order to protect the privacy of all BIAS customers, any such rules may be applied to small providers as well as large providers. In the course of seeking comment on these subjects, the Notice seeks comment on alternative approaches and burdens to small providers.

53. *Dispute Resolution.* As discussed above, the Notice seeks comment on whether the Commission's current informal complaint resolution process is sufficient or if BIAS providers should offer additional dispute resolution mechanisms for broadband privacy disputes. In order to promote all customers' privacy interests in the transparency, choice, and security of how their data is used, any such resulting rules may apply to small providers as well as large providers. The Notice seeks comment as well on alternative approaches as well as the burdens any approaches would have on small providers.

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

54. 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.''

55. The Commission expects to consider the economic impact on small providers, as identified in comments filed in response to the Notice and this IRFA, in reaching its final conclusions and taking action in this proceeding. Moreover, in formulating these rules, we seek to provide flexibility for small providers whenever possible, by setting out standards and goals for the providers to reach in whichever way is most efficient for them.

56. *Definitions.* As discussed above, in proposing definitions to accompany these proposed rules we seek comment on alternative formulations, including alternatives that could reduce burdens on small providers. We seek comment on alternative definitions of the terms affiliate; customer; CPNI; customer PI; opt-out and opt-in approval; communications-related services; breach; and other terms and ask how such alternatives could affect the benefits and burdens to small providers. In addition to these requests for comment, we seek comment generally on alternative definitions that would reduce burdens on small providers.

57. *Providing Meaningful Notice of Privacy Policies.* As discussed above, we seek comment on alternative approaches to our proposed privacy notice rules that would alleviate burdens on small providers. In particular, we seek comment on notice practices currently in use and industry best practices, in order to develop efficient and effective options. We seek comment on the compliance burden associated with our proposed rules and alternatives that would alleviate the burden on small providers in particular. We seek comment on whether a privacy policy safe harbor rule would ease the regulatory burden on small providers. We also seek comment on other alternatives for simplifying and standardizing privacy notices and whether these approaches, such as the creation of a privacy dashboard, could alleviate burdens on small providers. For notices of material changes to privacy policies, we specifically seek comment on burdens, compliance costs, and alternatives for small providers.

58. *Customer Approval Requirements for the Use and Disclosure of Customer PI.* As discussed above, we seek comment on alternative customer approval rules that could alleviate burdens on small providers while preserving the ability of all BIAS customers to have meaningful choices in the use and disclosure of their personal information. Choice is a critical component of protecting the confidentiality of customer proprietary information. We seek comment on ways to minimize the burden of our proposed customer choice framework on small BIAS providers. In particular, we seek comment on whether there are any small-provider-specific exemptions that we might build into our proposed approval framework. For example, should we allow small providers who have already obtained customer approval to use their customers' proprietary information to grandfather in those approvals? Should this be allowed for third parties? Should we exempt providers that collect data from fewer than 5,000 customers a year, provided they do not share customer data with third parties? Are there other such policies that would minimize the burden of our proposed rules on small providers? If so, would the benefits to small providers of any suggested exemptions outweigh the potential negative impact of such an exemption on the privacy interests of the customers of small BIAS providers? Further, were we to adopt an exemption, how would we define what constitutes a ''small provider'' for purposes of that exemption?

59. *Use and Disclosure of Aggregate Customer PI.* As discussed above, we seek comment on alternative approaches to the use and disclosure of aggregate customer PI that could alleviate burdens on small BIAS providers. In particular, we seek comment on an approach to aggregate customer PI that is similar to that used by HIPAA, and whether such an approach would be less burdensome to small BIAS providers. We also ask that as commenters consider whether we should adopt each of the prongs of our proposed rule, and any proposed alternatives, that they also consider how we could limit any burdens associated with compliance, particularly for small providers.

60. *Securing Customer Proprietary Information.* As discussed above, we seek comment on alternative approaches to secure customer proprietary information that could alleviate burdens on small BIAS providers. We propose that any specific security measures employed by a BIAS provider take into consideration the nature and scope of the BIAS provider's activities, because we believe that this sliding scale approach will afford sufficient flexibility for small providers while still protecting their customers. The Commission has previously explained that ''privacy is a concern which applies regardless of carrier size or market share.'' However, we recognize that the same data security protections may not be necessary in all cases. For example, a small provider with only a few customers may not store, use, or disclose customer PI in the same manner as a large provider. In such a case, what constitutes ''reasonable'' safeguards might be different. We seek comment on current data security practices in the industry and alternative structures that can build on current best practices to alleviate burdens. We seek comment on alternatives to our proposed rule on account change notifications that could reduce burdens on small providers. When discussing whether to require multi-factor authentication or contractual data security commitments from third party recipients of customer PI, we seek comment on the burdens such proposals could place on small providers and alternatives that could reduce such burdens. We also ask that comments

and proposals regarding data destruction discuss potential burdens for small providers.

61. *Data Breach Notification Requirements.* As discussed above, we seek comment on alternative approaches to data breach notifications that could alleviate burdens on small providers. In particular we propose a threshold of 5,000 affected customers for breach notification of the Federal Bureau of Investigation and U.S. Secret Service, and seek comment on how such a threshold could benefit or burden small providers. We also seek comment on record retention rules and alternatives that could reduce compliance burdens.

62. *Other Practices Implicating Privacy.* As discussed above, in seeking comment on whether to prohibit specific practices implicating privacy, we also seek comment on how proposals and alternatives can alleviate burdens on small providers. In particular, when seeking comment on whether heightened notice and choice requirements are necessary for some practices, we specifically ask commenters to address the burdens of their proposals on small providers, and alternatives to reduce such burdens.

63. *Dispute Resolution.* As discussed above, in seeking comment on potential approaches to dispute resolution, we also seek comment on how proposals and alternatives can benefit or burden small providers.

F. Federal Rules That May Duplicate, Overlap, or Conflict With the Proposed Rules

None.

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.

Proposed Rules

For the reasons discussed in the preamble, the Federal Communications Commission proposes to revise Part 64 of Title 47 of the Code of Federal Regulations 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.

Subpart U—Customer Proprietary Network Information

■ 2. Amend § 64.2003 as follows:

■ a. Redesignate paragraphs (d) through (r) as indicated in the table below:

Old paragraph	New paragraph
(d)	(e)
(e)	(f)
(f)	(g)
(g)	(i)
(h)	(j)
(i)	(k)
(j)	(l)
(k)	(m)
(l)	(n)
(m)	(p)
(n)	(q)
(o)	(r)
(p)	(s)
(q)	(t)
(r)	(u)

■ b. Add new paragraphs (d), (h), and (o), and revise newly redesignated paragraphs (c), (j), (k), (l), (r), and (s) to read as follows:

§ 64.2003 Definitions.

* * * * *

(c) *Affiliate.* The term ''affiliate'' has the same meaning given such term in Section 3 of the Communications Act of 1934, as amended, 47 U.S.C. 153.

(d) *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.

* * * * *

(h) *Customer proprietary information.* The term ''customer proprietary information'' or ''customer PI'' means:

(1) Customer proprietary network information; and

(2) Personally identifiable information (PII) a carrier acquires in connection to its provision of telecommunications service.

* * * * *

(j) *Customer premises equipment (CPE).* The term ''customer premises equipment (CPE)'' has the same meaning given to such term in Section 3 of the Communications Act of 1934, as amended, 47 U.S.C. 153.

(k) *Information services typically provided by telecommunications carriers.* The phrase ''information services typically provided by telecommunications carriers'' means only those information services (as defined in Section 3 of the Communication Act of 1934, as amended, 47 U.S.C. 153) that are typically provided by telecommunications carriers, such as voice mail services. Such phrase ''information services typically provided by telecommunications carriers,'' as used in this subpart, shall not include retail consumer services provided using Internet Web sites (such as travel reservation services or mortgage lending services), whether or not such services may otherwise be considered to be information services.

(l) *Local exchange carrier (LEC).* The term ''local exchange carrier (LEC)'' has the same meaning given to such term in Section 3 of the Communications Act of 1934, as amended, 47 U.S.C. 153.

* * * * *

(o) *Personally Identifiable Information.* The term ''personally identifiable information'' or ''PII'' means any information that is linked or linkable to an individual.

* * * * *

(r) *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 an entity that provides interconnected VoIP service, as that term is defined in § 9.3 of this chapter, and shall exclude an entity that provides broadband Internet access service, as that term is defined in § 8.2 of this chapter.

(s) *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.

* * * * *

■ 3. Revise § 64.2011 to read as follows:

§ 64.2011 Data breach notification.

(a) *Customer notification.* A telecommunications carrier must notify affected customers of covered breaches of customer PI no later than 10 days after the discovery of the breach, subject to law enforcement needs.

(1) A telecommunications carrier required to provide notification to a customer under this paragraph may provide such notice by any of the following methods:

(i) Written notification, sent to the postal address of the customer provided by the customer for contacting that customer;

(ii) Email or other electronic means using information provided by the

customer for contacting that customer for data breach notification purposes.

(2) The customer notification required to be provided under this section 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 used, disclosed, or accessed, or reasonably believed to have been used, disclosed, or accessed, by a person without or exceeding authorization as a part of the breach of security;

(iii) Information that 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) Information about the national credit-reporting agencies and the steps customers can take to guard against identity theft, including any credit monitoring or reporting the telecommunications carrier is offering customers affected by the breach of security.

(3) If a federal law enforcement agency determines that the notification to customers required under this paragraph would interfere with a criminal or national security investigation, such notification shall be delayed upon the written request of the law enforcement agency for any period which the law-enforcement agency determines is reasonably necessary. A law enforcement agency may, by a subsequent written request, revoke such delay or extend the period set forth in the original request made under this paragraph by a subsequent request if the law enforcement agency determines that further delay is necessary.

(b) *Commission notification.* A telecommunications carrier must notify the Federal Communications Commission of any breach of customer PI no later than seven days after discovering such breach. Such notification shall be made electronically by means of a reporting system that the Commission makes available on its Web site.

(c) *Federal law enforcement notification.* A telecommunications carrier must notify the Federal Bureau of Investigation (FBI) and the U.S. Secret Service (Secret Service) whenever a breach is reasonably believed to have compromised the customer PI of more than 5,000 individuals, no later than seven (7) days after discovery of the breach, and at least three (3) days before notification to the affected customers. Such notification shall be made through a central reporting facility. The Commission will maintain a link to the reporting facility on its Web site.

(d) *Recordkeeping.* A telecommunications carrier must maintain a record of any breaches of security discovered and notifications made to customers, the Commission, the FBI, and the Secret Service pursuant to this section. The record must include, if available, dates of discovery and notification, a detailed description of the customer PI that was the subject of the breach, and the circumstances of the breach. Telecommunications carriers shall retain such records for a minimum of 2 years.

■ 4. Add subpart GG to part 64 as follows:

Subpart GG—Privacy of BIAS Customer Information

Sec.

§ 64.7000 Definitions.

(a) *Aggregate customer proprietary information.* The terms ''aggregate customer proprietary information'' or ''aggregate customer PI'' means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.

(b) *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.

(c) *Broadband Internet Access Service (BIAS).* The term ''broadband Internet access services'' or ''BIAS'' has the same meaning given such term in § 8.2(a) of this chapter.

(d) *Broadband Internet access service provider.* The term ''broadband Internet access service provider'' or ''BIAS provider'' means a person or entity engaged in the provision of BIAS.

(e) *Customer.* The term ''customer'' means:

(1) A current or former, paying or non-paying, subscriber to a broadband Internet access service; or

(2) An applicant for a broadband Internet access service.

(f) *Customer proprietary information.* The term ''customer proprietary information'' or ''customer PI'' means:

(1) Customer proprietary network information; and

(2) Personally identifiable information (PII) a BIAS provider acquires in connection to its provision of BIAS.

(g) *Customer proprietary network information.* The term ''customer proprietary network information (CPNI)'' has the same meaning given to such term in the Communications Act of 1934, as amended, 47 U.S.C. 222(h)(1).

(h) *Opt-in approval.* The term ''opt-in approval'' means a method for obtaining customer consent to use, disclose, or permit access to the customer's proprietary information that requires that the BIAS provider obtain affirmative, express consent from the customer allowing the requested usage, disclosure, or access to the customer PI, consistent with the requirements set forth in § 64.7002 of this subpart.

(i) *Opt-out approval.* The term ''opt-out approval'' means a method 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 BIAS provider's request for consent consistent with the requirements set forth in § 64.7002 of this subpart.

(j) *Personally Identifiable Information.* The term ''personally identifiable information'' or ''PII'' means any information that is linked or linkable to an individual.

§ 64.7001 Notice requirements for providers of broadband Internet access services.

(a) *Providing notice of privacy policies.* A BIAS provider must clearly and conspicuously notify its customers of its privacy policies. The notice must:

(1) Specify and describe:

(i) The types of customer PI that the BIAS provider collects by virtue of its provision of broadband service;

(ii) How the BIAS provider uses, and under what circumstances it discloses, each type of customer PI that it collects; and

(iii) The categories of entities that will receive the customer PI from the BIAS provider and the purposes for which the customer PI will be used by each category of entities.

(2) Advise customers of their opt-in and opt-out rights with respect to their own proprietary information, and provide access to a simple, easy-to-access method for customers to provide or withdraw consent to use, disclose, or provide access to customer PI for purposes other than the provision of BIAS. Such method shall be persistently available and made available at no additional cost to the customer.

(3) Explain that a denial of approval to use, disclose, or permit access to customer PI for purposes other than providing BIAS will not affect the provision of any services to which the customer subscribes. However, the provider may provide a brief description, in clear and neutral language, describing any consequences directly resulting from the lack of access to the customer PI.

(4) Explain that any approval, denial, or withdrawal of approval for the use of the customer PI for any purposes other than providing BIAS is valid until the customer affirmatively revokes such approval or denial, and inform the customer of his or her right to deny or withdraw access to such PI at any time. However, the notice must also explain that the provider may be compelled to disclose a customer's PI when such disclosure is provided for by other laws.

(5) Be comprehensible and not misleading.

(6) Be clearly legible, use sufficiently large type, and be displayed in an area so as to be readily apparent to the customer; and

(7) Be completely translated into another language if any portion of the notice is translated into that language.

(b) *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 BIAS, whether such purchase is being made in person, online, over the telephone, or via some other means; and

(2) Be made persistently available via a link on the BIAS provider's homepage, through the BIAS provider's mobile application, and through any functional equivalent to the provider's homepage or mobile application.

(c) *Material changes in a BIAS provider's privacy policies.* A BIAS provider must provide existing customers with advanced notice of material changes to the BIAS provider's privacy policies. Such notice must:

(1) Be clearly and conspicuously provided through each of the following means:

(i) Email or another electronic means of communication agreed upon by the customer and BIAS provider;

(ii) On customers' bills for BIAS; and

(iii) Via a link on the BIAS provider's homepage, mobile application, and any functional equivalent.

(2) Provide a clear, conspicuous, and comprehensible explanation of:

(i) The changes made to the BIAS provider's privacy policies, including any changes to what customer PI the BIAS provider collects, and how it uses, discloses, or permits access to such information;

(ii) The extent to which the customer has a right to disapprove such uses, disclosures, or access to such information and to deny or withdraw access to the customer PI at any time; and

(iii) The precise steps the customer must take in order to grant or deny access to the customer PI. The notice must clearly explain that a denial of approval will not affect the provision of any services to which the customer subscribes. However, the provider may provide a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to the customer PI. If accurate, a provider may also explain in the notice that the customer's approval to use the customer's PI may enhance the provider's ability to offer products and services tailored to the customer's needs.

(3) Explain that any approval or denial of approval for the use of customer PI for purposes other than providing BIAS is valid until the customer affirmatively revokes such approval or denial.

(4) Be comprehensible and not misleading.

(5) Be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to customers.

(6) Have all portions of the notice translated into another language if any portion of a notice is translated into that language.

§ 64.7002 Customer approval requirements.

Except as described in paragraph (a) of this section, a BIAS provider may not use, disclose, or provide access to customer PI except with the approval of a customer.

(a) *Approval for use, disclosure, or permitting access inferred.* A customer is considered to have provided approval for the customer's BIAS provider to use, disclose, or permit access to customer PI for the following purposes:

(1) In its provision of the broadband Internet access service from which such information is derived, or in its provision of services necessary to, or used in, the provision of such broadband service.

(2) To initiate, render, bill and collect for broadband Internet access service, and closely related services, *e.g.,* tech support related to the broadband Internet access services.

(3) To protect the rights or property of the BIAS provider, or to protect users of the broadband Internet access service and other BIAS providers from fraudulent, abusive, or unlawful use of the broadband Internet access service.

(4) To provide any inbound marketing, referral, or administrative services to the customer for the duration of the interaction, if such interaction was initiated by the customer and the customer approves of the use of such information to provide such service.

(5) To support queries by Public Safety Answering Points and other authorized emergency personnel pursuant to the full range of NG911 calling alternatives (including voice, text, video and data); to 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 to 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 by law.

(b) *Approval for use inferred.* A BIAS provider may use customer PI for the purpose of marketing additional BIAS offerings in the same category of service (*e.g.,* fixed or mobile BIAS) to the customer, when the customer already subscribes to that category of service from the same provider, without further customer approval.

(c) *Notice and solicitation required.* Except as described in paragraph (a) of this section, a BIAS provider must solicit customer approval, as provided for in paragraphs (e) and (f) of this section, when it intends to first use, disclose, or provide access to the customer's proprietary information and in so doing must clearly and conspicuously disclose:

(1) The types of customer PI for which it is seeking customer approval to use, disclose or permit access to;

(2) The purposes for which such customer PI will be used; and

(3) The entities or types of entities to which it intends to disclose or provide access to such customer PI.

(d) *Method for solicitation for customer approval.* A BIAS provider must make available a simple, easy-to-access method for customers to provide or withdraw consent at any time. Such method must be clearly disclosed, persistently available, and made available at no additional cost to the

customer. The customer's action must be given effect promptly after the decision to provide or withdraw consent is communicated to the BIAS provider.

(e) *Opt-Out approval required.* Except as otherwise provided in paragraph (a) of this section, a BIAS provider must obtain opt-out or opt-in approval from a customer to:

(1) Use customer PI for the purpose of marketing communications-related services to that customer; and

(2) Disclose or permit access to customer PI to its affiliates that provide communications-related services for the purpose of marketing communications-related services to that customer.

(f) *Opt-In approval required.* Except as otherwise provided, a BIAS provider must obtain customer opt-in approval to use, disclose, or permit access to customer PI.

(g) *Use and disclosure of aggregate customer PI.* A BIAS provider may use, disclose, and permit access to aggregate customer PI other than for the purpose of providing BIAS and for services necessary to, or used in, the provision of BIAS, if the BIAS provider:

(1) Determines that the aggregated customer PI is not reasonably linkable to a specific individual;

(2) Publicly commits to maintain and use the aggregate customer PI in a non-individually identifiable fashion and to not attempt to re-identify such information;

(3) Contractually prohibits any entity to which it discloses or permits access to the aggregate customer PI from attempting to re-identify such information; and

(4) Exercises reasonable monitoring to ensure that those contracts are not violated.

For purposes of this section, the burden of proving that individual customer identities and characteristics have been removed from aggregate customer PI rests with the BIAS provider.

§ 64.7003 Documenting compliance with customer approval requirements.

A BIAS provider must implement a system by which the status of a customer's approval to use, disclose, and provide access to customer PI can be clearly established both prior to and after its use, disclosure, or access. A BIAS provider must:

(a) Train its personnel as to when they are and are not authorized to use, disclose, or permit access to customer PI and have an express disciplinary process in place.

(b) Maintain a record of all instances where customer PI was disclosed to or accessed by third parties for at least one year. The record must include a description of the specific customer PI that was disclosed to or accessed by third parties, a list of the specific third parties who received the customer PI, and the basis for disclosing or providing access to such information to third parties.

(c) Maintain a record of all customer notifications, whether oral, written, or electronic, for at least one year.

(d) Establish a supervisory review process regarding the provider's compliance with the rules in this subpart.

(e) Provide written notice to the Commission within five days of the discovery of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly; or the provider used, disclosed, or permitted access to customer PI subject to opt-in approval requirements without first having received opt-in approval. Such notice must be submitted even if the provider offers other methods by which customers may opt-out. The notice shall include:

(1) The provider's name;

(2) A description of the opt-out mechanism(s) at issue and the problem(s) experienced, if relevant;

(3) A description of:

(i) Any customer PI used, disclosed, or accessed without opt-out or opt-in approval;

(ii) With whom or by whom such customer PI has been used, disclosed, or accessed;

(iii) For what purposes such customer PI was used, disclosed, or accessed; and

(iv) Over what period of time such customer PI was used, disclosed, or accessed;

(4) The remedy proposed and when it will be or was implemented; and

(5) A copy of the notice provided contemporaneously to customers.

§ 64.7004 Service offers conditioned on the waiver of privacy rights.

A BIAS provider is prohibited from conditioning offers to provide broadband Internet access service on a customer's agreement to waive privacy rights guaranteed by law or regulation. A BIAS provider is further prohibited from discontinuing or otherwise refusing to provide broadband Internet access service due to a customer's refusal to waive any such privacy rights.

§ 64.7005 Data security requirements for broadband Internet access service providers.

(a) *Data security requirements.* A BIAS provider must ensure the security, confidentiality, and integrity of all customer PI the BIAS provider receives, maintains, uses, discloses, or permits access to from any unauthorized uses or disclosures, or uses exceeding authorization. At minimum, this requires a BIAS provider to:

(1) Establish and perform regular risk management assessments and promptly address any weaknesses in the provider's data security system identified by such assessments;

(2) Train employees, contractors, and affiliates that handle customer PI about the BIAS provider's data security procedures;

(3) Designate a senior management official with responsibility for implementing and maintaining the broadband provider's information security measures;

(4) Establish and use robust customer authentication procedures to grant customers or their designees' access to customer PI; and

(5) Notify customers of account changes, including attempts to access customer PI, in order to protect against fraudulent authentication.

(b) A BIAS provider may employ any security measures that allow the provider to reasonably implement the requirements set forth in this section, and in doing so must take into account, at minimum:

(1) The nature and scope of the BIAS provider's activities;

(2) The sensitivity of the customer proprietary information held by the BIAS provider.

§ 64.7006 Breach notification.

(a) *Customer notification.* A BIAS provider must notify affected customers of covered breaches of customer PI no later than 10 days after the discovery of the breach, subject to law enforcement needs.

(1) A BIAS provider required to provide notification to a customer under this subsection may provide such notice by any of the following methods:

(i) Written notification, sent to the postal address of the customer provided by the customer for contacting that customer; or

(ii) Email or other electronic means using information provided by the customer for contacting that customer for data breach notification purposes.

(2) The customer notification required to be provided under this section 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 used, disclosed, or accessed, or reasonably believed to have been used,

disclosed, or accessed, by a person without or exceeding authorization as a part of the breach of security;

(iii) Information that the customer can use to contact the BIAS provider to inquire about the breach of security and the customer PI that the BIAS provider 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) Information about the national credit-reporting agencies and the steps customers can take to guard against identity theft, including any credit monitoring or reporting the telecommunications carrier is offering customers affected by the breach of security.

(3) If a federal law enforcement agency determines that the notification to customers required under this subsection would interfere with a criminal or national security investigation, such notification shall be delayed upon the written request of the law enforcement agency for any period which the law enforcement agency determines is reasonably necessary. A law enforcement agency may, by a subsequent written request, revoke such delay or extend the period set forth in the original request made under this paragraph by a subsequent request if the law enforcement agency determines that further delay is necessary.

(b) *Commission notification.* A BIAS provider must notify the Federal Communications Commission of any breach of customer PI no later than seven days after discovering such breach. Such notification shall be made electronically by means of a reporting system that the Commission makes available on its Web site.

(c) *Federal law enforcement notification.* A BIAS provider must notify the Federal Bureau of Investigation (FBI) and the U.S. Secret Service (Secret Service) whenever a breach is reasonably believed to have compromised the customer PI of more than 5,000 customers, no later than seven (7) days after discovery of the breach, and at least three (3) days before notification to the affected customers, whichever comes first. Such notification shall be made through a central reporting facility. The Commission will maintain a link to the reporting facility on its Web site.

(d) *Recordkeeping.* A BIAS provider must maintain a record of any breaches of security discovered and notifications made to customers, the Commission, the FBI, and the Secret Service pursuant to this section. The record must include, if available, dates of discovery and notification, a detailed description of the customer PI that was the subject of the breach, and the circumstances of the breach. BIAS providers shall retain such records for a minimum of 2 years.

§ 64.7007 Effect on state law.

The rules set forth in this subpart shall preempt state law only to the extent that such state laws are inconsistent with the rules set forth herein. The Commission shall determine whether a state law is preempted on a case-by-case basis, without the presumption that more restrictive state laws are preempted.

[FR Doc. 2016–08458 Filed 4–19–16; 8:45 am]

BILLING CODE 6712–01–P