FCC Proposes Sweeping Privacy and Data Security Rules with Significant Potential Impact on the Broadband Ecosystem

Alysa Z. Hutnik, Jennifer Rodden Wainwright

April 8, 2016

On March 31, 2016, the Federal Communications Commission (FCC or Commission) voted along party lines (3-2) to launch a notice of proposed rulemaking (Notice or NPRM) to establish privacy rules for Broadband Internet Access Service (BIAS) providers. This rulemaking stems from the *2015 Open Internet Order* and proposes rules to apply Section 222 of the Communications Act of 1934, as amended (Communications Act or the Act), to BIAS. The proposed rules draw from a wide array of federal and state laws, rules, and other guidance, as well as industry best practices, and if adopted could impose prescriptive and complex privacy obligations that would be among the most extensive in the country.

The NPRM proposes to create a new subpart in the Code of Federal Regulations (Section GG, 47 C.F.R. § 64.7000 *et seq.*) for broadband privacy that would address customer proprietary information (PI), a category that includes both customer proprietary network information (CPNI) as well as personally identifiable information (PII). If adopted, the FCC's proposal would impose a privacy framework similar to, but in many respects more prescriptive than, existing voice telecommunications privacy rules. The proposal is designed to:

(1) Promote transparency through meaningful notice of privacy policies;

(2) Establish a robust customer choice framework for the use and disclosure of customer PI; and

(3) Protect customer PI from misappropriation, breach and unlawful disclosure through general and specific data security requirements and breach reporting obligations.

While the bulk of the proposed rules would be separate from the existing voice CPNI rules, the Commission also seeks comment on whether and how to "harmonize" its existing voice CPNI rules with the proposed rules. The Commission also seeks comment on whether and how to harmonize its cable and satellite privacy and data security rules with its proposed framework. Finally, while the Commission has stated that its proposals are not intended to regulate the privacy practices of edge services (e.g., web sites), the Commission seeks comment on whether to require BIAS providers to pass through their privacy and data security obligations (e.g., by contract) to third-party joint venture partners, independent contractors, operating system developers, and equipment manufacturers. Thus, the proceeding affects not only BIAS providers, but, potentially, telecom carriers, VoIP providers, cable providers, satellite providers, equipment manufacturers, and edge

services.

Initial comments on the NPRM are due on **May 27, 2016** and replies are due on **June 27, 2016**. We summarize the key proposals and questions below.

Table of Contents:

I. Background: Section 222 of the Communications Act

Section 222 was added to the Communications Act of 1996 to ensure the proper use of information necessary to facilitate the new competitive provider paradigm that replaced monopoly local phone service. In the *2015 Open Internet Order*, the FCC declined to forbear from applying Section 222 of the Communications Act to BIAS providers, but declined to impose its voice-centric rules implementing those statutory provisions to broadband, opting instead for a separate rulemaking for broadband-specific privacy rules. As interpreted by the Commission, Section 222 imposes numerous privacy and data security requirements on telecommunications carriers and interconnected VoIP providers.

- **General Standard.** According to the FCC, Section 222(a) establishes a general duty "to protect the confidentiality of proprietary information of, and relating to, other telecommunications carriers, equipment manufacturers, and customers, including telecommunications carriers reselling telecommunications service provided by a telecommunications carrier."

- **Carrier Proprietary Information.** Section 222(b) requires a telecommunications carrier that "receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service [to] use such information only for such purpose, and . . . not for its own marketing efforts."

- **Customer Proprietary Network Information (CPNI).** Section 222(c) sets forth the requirements related to CPNI, which is defined as "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone

toll service received by a customer of a carrier; except that such term does not include subscriber list information [i.e., information published in a phone book].” Except as required by law or with the approval of the customer, a carrier that receives or obtains CPNI may “only use, disclose, or permit access to individually identifiable customer proprietary network information 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, including the publishing of directories.” Section 222(c) also requires carriers to disclose CPNI, upon affirmative written request by the customer, to a designee of the customer. Moreover, Section 222(c) permits carriers to use, disclose, or permit access to aggregate customer information (so long as it provides such information to other carriers or persons of reasonable and nondiscriminatory terms).

- **Exceptions.** Section 222(d) includes a number of exceptions from the use, disclosure, and access restrictions above, including “(1) to initiate, render, bill, and collect for telecommunications services; (2) 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; (3) to provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if such call was initiated by the customer and the customer approves of the use of such information to provide such service; and (4) to provide call location information concerning the user of a commercial mobile service or the user of an IP-enabled voice service [in the event of an emergency].”

Over the last twenty years, the FCC has adopted a complicated suite of rules implementing Section 222, including notice and consent requirements, safeguards against pretexters, annual certification requirements, and data security breach notification obligations. Recently, the Commission significantly increased its enforcement efforts against providers for alleged violations of Section 222 and the Commission’s privacy rules. In addition, the Commission has used Section 201(b) of the Act, which prohibits “unjust and unreasonable” practices, to impose strong data security requirements on carriers. The Commission also has imposed significant privacy and data security requirements on carriers through consent decrees, creating a “common law of privacy” similar to the enforcement mechanisms that the Federal Trade Commission (FTC) has employed under Section 5 of the FTC Act. Apart from its traditional telecommunications privacy rules under Section 222, the Commission also has authority over the privacy and data security practices of cable (Section 631) and satellite (Section 338(i)) providers.

Together with other federal and state privacy and data security laws, rules, and guidelines, these voice-centric privacy provisions serve as the foundation for the Commission’s broadband privacy NPRM.

II. Definitions for Key Terms

The NPRM proposes specific definitions of more than a dozen unique terms for the purpose of “provid[ing] guidance to both broadband providers and customers regarding the scope of the [proposed] privacy protections.” The Notice seeks comment on these definitions and further asks whether any of the existing terms in the Commission’s CPNI rules should be modified in order to harmonize them with the proposed rules for BIAS providers. The key proposed definitions are as follows:

- **Customer Proprietary Information (PI).** The NPRM proposes that customer PI includes both (1) CPNI and (2) Personally Identifiable Information (PII), as defined below. The Commission

seeks comment on whether to adopt a single, unified definition of customer PI for use with its proposed broadband privacy rules and existing voice privacy rules.

- **Customer Proprietary Network Information (CPNI).** The Commission proposes to adopt the statutory definition of CPNI for use in the broadband context, i.e., "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 of a carrier." Consistent with its *2013 Mobile Device CPNI Declaratory Ruling,* the definition would include information that a BIAS provider causes to be collected and stored on customer devices, even where the information has not yet been transmitted to the provider's own servers (so long as the information was collected at the provider's direction). The NPRM proposes that the following specific examples would constitute CPNI in the broadband context:

  (1) Service plan information (including type of service, service tier, pricing, and capacity);

  (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.

  Unlike in the voice-CPNI context, the Commission tentatively concludes that the statutory exception for "subscriber list information" does not apply in the broadband context. The Commission seeks comment on this interpretation and asks whether CPNI should also include other types of information, such as port information, application headers, application usage information, and customer premises equipment (CPE) information.

- **Personally Identifiable Information (PII).** The NPRM proposes to define PII as "any information that is linked or linkable to an individual." Specific types of PII would include, but not be limited to, the following **30** data elements:

- Name
- Social security number
- Date and place of birth
- Mother's maiden name
- Physical address
- Email address or other online contact information
- Phone numbers
- Mac address or other unique
- Internet browsing history
- Traffic statistics
- Application usage data
- Current or historical geo-location
- Shopping records
- Medical and health information
- Account numbers and other account information,
- Biometric information
- Education information
- Employment information
- Information relating to family members
- Race
- Religion
- Sexual identity or orientation

device identifiers

- IP addresses
- Unique government identification numbers (e.g., driver's license, passport, taxpayer identification)
- Eponymous and non-eponymous online identities

including account login information

- Financial information (e.g., account numbers, credit or debit card numbers, credit history)
- Information identifying personally owned property (e.g., license plates, device serial numbers)

- Other demographic information
- The fact of a disability and any additional information about a customer's disability
- Persistent online identifiers (e.g., unique cookies)

The Commission seeks comment on inclusion of these data elements in the definition of PII and asks whether there are other categories of linked or linkable information that should also be included in the definition. Further, the Commission seeks comment on whether it should harmonize its existing voice rules and proposed broadband rules to treat name, address, and telephone number information as customer proprietary information in the voice context (today, those data elements are not considered CPNI).

- **Customer Premises Equipment (CPE).** The Commission seeks comment on whether to adopt its current definition of CPE—i.e., "equipment employed on the premises of a person (other than a carrier) to originate, route, or terminate telecommunications"—in the broadband context, and whether this definition should include mobile devices and networked devices (including "Internet of Things" devices).
- **Content of Customer Communications.** The NPRM seeks comment on how best to define and treat the content of communications over BIAS, recognizing that several existing federal and state laws already protect such information (e.g., Electronic Communications Privacy Act (ECPA) and Section 705 of the Communications Act).
- **Aggregate Customer PI.** The NPRM proposes 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." The Commission notes that this definition is intended to encompass the "use of all aggregate customer PI and not just aggregate CPNI." It also seeks comment on whether this definition should apply to both BIAS and voice services.
- **Communications-Related Services and Related Terms.** The Commission seeks comment on the appropriate definition of "communications-related services." Under the current rules, using individually identifiable CPNI or disclosing/making available individually identifiable CPNI to agents and affiliates that provide communications-related services (for the purpose of marketing communications-related services) is subject only to opt-out consent requirements. The NPRM seeks comment on how best to narrow the scope of the term communications-related services "to align with consumer expectations about the extent to which BIAS providers use and share customer PI with communications-related affiliates" (i.e., to limit the circumstances in which opt-out approval would be sufficient). The Commission also proposes to narrow the definition of communications-related services in the voice context to exclude "Internet access" services, which have since those services are now classified as telecommunications services. Finally, the Commission asks whether it should harmonize the definition of communications-related services across BIAS and other telecommunications

services.

- **Customer.** Drawing on its conclusion in the *TerraCom/YourTel Notice of Apparent Liability*, the NPRM proposes to define "customer" broadly to include current and former paying and non-paying subscribers, as well as prospective subscribers ("applicants"). The Commission also seeks comment on whether it should further expand its definition of "customer" to protect broadband users who may not fall within the proposed definition of that term (i.e., minors, members of a group plan or individual users with a login), and whether it should harmonize its proposed definition of "customer" with its existing CPNI rules and the term "subscriber" under its cable and satellite privacy rules.

- **Breach.** The Commission proposes a broader definition of "breach" for purposes of reporting requirements under the broadband privacy rules. It proposes to define "breach" to mean "any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information." This definition differs from the existing Section 222 rules in two material respects: (1) there is no requirement of intent, and (2) it covers all customer PI, not just CPNI. With respect to its proposal not to include an intent requirement, the Commission explains its view that such a requirement "will ensure data breach notification in the case of inadvertent breaches that have potentially negative consequences for customers." Moreover, its proposal to require notification for breaches involving all customer PI would dramatically expand the potential scenarios in which notification would be required.

The Commission also proposes to revise its existing rules to clarify that those provisions apply only to telecommunications services other than BIAS, but seeks comment on whether to develop one uniform set of definition for both voice and broadband CPNI. The Commission also recognizes that any definitional changes may require revisions to the current CPNI rules, or additional definitions. For this reason, the Commission broadly asks how it should revise its existing CPNI rules.

III. Providing Meaningful Notice of Privacy Policies

To promote transparency, the Commission lays out a number of proposals that would require BIAS providers to "provide customers with clear, conspicuous, and understandable information about their privacy practices." Most importantly, the Commission proposes to require BIAS providers to post privacy notices at the point of sale and on an on-going basis on the BIAS provider's homepage, mobile application, and any functional equivalent. Moreover, the FCC provides specific direction on the content, form, timing, and placement of those notices, as well as rules for notice of material changes to BIAS provider's privacy policies. Finally, the Commission seeks comment on ways to harmonize its proposed requirements with notice requirements for providers of voice and video services.

A. Privacy Notice Requirements

The NPRM proposes that BIAS providers provide notice of their privacy policies, and proposes requirements for the content, form, timing, and placement of those notices.

- **Content.** NPRM proposes that a BIAS provider's privacy notice must include the following information:

  (1) **The types of customer PI collected and how this information is used and disclosed,** including the categories of entities that will receive customer PI from the BIAS

provider and the purposes for which the information will be used by those entities; and

(2) **The customer's rights with respect to their PI,** including instructions for how to opt-in or opt-out of consent for certain data uses, an explanation 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 services, and an explanation that the customer's opt-out or opt-in decision is valid until the customer affirmatively revokes it.

The Commission seeks comment on these proposals and asks whether other information should be included in the disclosures, including, for example, information concerning BIAS providers' data security practices. The Notice also asks whether the rules should require BIAS providers to disclose specific information about each individual third party with whom a customer's PI has been shared, similar to California's Shine the Light law.

- **Form.** To ensure that customers understand the content of the privacy notice, the Commission proposes to require that such notices be:

  (1) Comprehensible and not misleading;

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

  (3) Completely translated into another language if any portion of the notice is translated into that language.

  The NPRM also asks whether and how 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." Alternatively, the Commission asks whether a standardized disclosure should be adopted as a voluntary safe harbor. The NPRM further seeks comment on other approaches the Commission could take to simplify privacy policy notices (e.g., a layered notice that includes a plain-language disclosure policy in addition to a more in-depth disclosure).

- **Timing and Placement.** The Commission also proposes that customers receive timely and "persistent" notice of a BIAS provider's privacy policies. To that end, the notice must:

  (1) Be made available to prospective customers at the point of sale, prior to the purchase of BIAS, and

  (2) Be made persistently available on the provider's homepage, mobile app, and any functional equivalent.

  The Commission seeks comment on whether it should require BIAS providers to create a "consumer-facing privacy dashboard" that would give consumers a streamlined view of how their customer PI is being collected, used and disclosed to third parties, and would allow consumers to change their privacy preferences.

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

The Commission proposes to require that a BIAS provider give advance notice to existing customers of any material changes to the provider's privacy policies. The notice would be required to:

- 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; 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;
- 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; and
- Have all portions of the notice translated into another language if any portion of the notice is translated into that language.

The Commission seeks comment on the appropriate timeframe for providing the notice, what would constitute a "material" change triggering the notice requirement, and the burden that these proposals would place on BIAS providers, particularly small providers.

C. Mobile-Specific Considerations Harmonizing Existing Requirements for Voice, Video and Broadband

The Commission also seeks comment on whether to treat fixed and mobile services differently. Although the Commission states as a general matter that it "do[es] not see a justification for treating fixed and mobile BIAS differently," it acknowledges that there may be some technical and logistical differences between the two types of services such that adjustments to the notice rules may be appropriate for mobile BIAS. Thus, the NPRM seeks comment on what, if any, accommodations would be appropriate mobile BIAS, and if separate, mobile-specific requirements should be adopted as well.

D. Harmonizing Existing Requirements for Voice, Video and Broadband

The NPRM asks whether it should harmonize its notice rules across voice, video, and broadband services. The Commission also seeks comment on whether it should harmonize privacy policy notice requirements for voice, video and broadband services. Additionally, recognizing that some providers offer bundled packages of voice, video and/or broadband services, the Commission asks whether it should allow such providers to provide a single notice of privacy policies, and in doing so "reconcile the types of information that are required to be in consumer privacy notices across voice, video, and broadband Internet access platforms."

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

One of the Commission's central concerns with regard to broadband privacy is ensuring that consumers have a choice as to how their information is used. To address this concern, the NPRM proposes and seeks comment on a series of rules outlining the types of approval required for a BIAS provider to use and disclose customer PI; the requirements for soliciting customer opt-out and opt-in

approval of use and disclosure; and how BIAS providers can document their compliance with the proposed customer consent requirements. The Commission further seeks comment on how these proposals would impact small BIAS providers and whether it should take steps to harmonize existing rules with its proposals for new rules.

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

In the NPRM, the Commission sets forth a proposed three-tiered framework for obtaining valid consent from a customer to use and/or disclose his or her PI. This approval framework generally tracks the existing consent framework for voice services. The proposed framework is as follows:

- **Implied Approval and Statutory Exceptions.** The NPRM proposes that BIAS providers would always be permitted to use or share customer PI in order to provide broadband services, and for certain other purposes that make sense within the context of the providers' relationships with their customers, without additional approval from the customer (e.g., marketing services within the category of services to which the customer already subscribes). The Commission seeks comment on the appropriate scope of activities that should be included in this category, as well as the Commission's interpretation that BIAS providers would be permitted to use customer PI without customer approval "for the purpose of marketing additional BIAS offerings in the same category of service (e.g., fixed or mobile BIAS) to the customer." The Commission further proposes to apply the statutory exemptions for permissible CPNI use under Section 222(d) to BIAS providers (e.g., billing and collections, protection of the carrier's property, caller location information during an emergency, or inside wiring installation, maintenance, and repair services). The FCC also proposes to allow telecommunications carriers to use or disclose calling party phone numbers to help protect customers from abusive, fraudulent, or unlawful robocalls, and seeks comment on whether to allow other providers, such as interconnected VoIP providers, to do the same.

- **Opt-Out Approval.** The NPRM proposes that BIAS providers (or their affiliates that provide communications-related services) could use customer PI to market other communications-related services subject to opt-out approval from the customer. The Commission proposes to define "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." Unlike the existing voice CPNI rules, the proposed definition would not be subject to a 30-day waiting period before becoming effective. The Commission seeks comment on whether to relax or tighten this proposal, particularly with respect to disclosing information to affiliates.

- **Opt-In Approval.** The NPRM proposes to require BIAS providers to obtain opt-in approval from their customers before sharing customer information with non-communications-related affiliates or third parties or before using customer information themselves (or through their communications-related affiliates) for any purpose other than those described in the above two mechanisms. The NPRM proposes to define "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 . . . before any use of, disclosure of, or access to such information." Notably, the Commission seeks comment on the

effect the proposed opt-in 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."

In addition to providing feedback on the FCC's proposed framework, commenters are also invited to propose their own frameworks for ensuring that customers have the ability to control the use and disclosure of their confidential information.

Finally, the Commission seeks comment on whether there are certain types of "highly sensitive" customer information used by BIAS providers that warrant heightened protections, and the appropriate protective measures for the content of customer communications.

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

The Commission proposes to require BIAS providers to obtain meaningful customer approval, subsequent to the point of sale, when they actually intend to first use or disclose customer PI "in a manner that requires customer approval." Specifically, the proposal would require a BIAS provider to notify the customer of the following information:

(1) The types of customer PI for which the provider seeks approval to use, disclose, or permit access to;

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

(3) The entity or types of entities with which the customer PI will be shared.

While the Commission does not propose a specific method through which a BIAS provider could notify subscribers, it asks commenters to weigh in on a number of potential notice and solicitation methods, including email or other electronic communications, postal mail, or others.

With regard to customer approval methods, the NPRM proposes 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] should be persistently available to customers." Finally, the Commission seeks comment on whether a customer's approval or disapproval should remain in effect until the customer revokes such approval or disapproval, and the effects of a revocation.

C. Documenting Compliance with Proposed Customer Consent Requirements

The Commission proposes to require BIAS providers to document their compliance with customer consent requirements by:

(1) Maintaining records on customer PI disclosure to third parties for at least one year,

(2) Maintaining records of customer notices and approval for at least one year,

(3) Adequately training and supervising their personnel on customer PI access,

(4) Establishing supervisory review processes, and

(5) Providing prompt notice to the Commission of unauthorized uses or disclosures.

The Commission also asks whether it should require BIAS providers to file an annual certification of compliance with the proposed rules, similar to the annual CPNI certification required for voice

services under the existing Section 222 rules.

D. Small BIAS Providers

The Commission seeks comment on how the proposed customer notice requirements would impact small BIAS providers. It further seeks comment on a number of potential accommodations for small providers, including grandfathering in existing approvals for use of customer PI and exempting providers that collect data from fewer than 5,000 customers per year and do not share customer data with third parties.

E. Harmonizing Customer Approval Requirements

As with many of its proposed rules, the Commission asks whether it should harmonize its existing CPNI approval requirements for voice services—and its existing approval requirements for cable and satellite providers—with its proposed approval requirements in the broadband context.

V. Use and Disclosure of Aggregate Customer PI

The Commission proposes "to allow BIAS providers to use, disclose, and permit access to aggregate customer PI if the provider" complies with the following:

> (1) The providers determines that the aggregated customer PI is not reasonably linkable to a specific individual or device. In determining whether data has been properly de-identified, the Commission seeks comment on whether it should rely on guidance established by the FTC, National Institute of Standards and Technology (NIST), or other federal agencies and/or statutory regimes;
>
> (2) The provider publicly commits to maintain and use the aggregate data in a non-individually identifiable fashion and to not attempt to re-identify the data. The Commission seeks comment as to how a provider could satisfy this requirement and whether it would help ensure that providers are protecting the confidentiality of customer PI;
>
> (3) The provider contractually prohibits any entity to which it discloses or permits access to the aggregate data from attempting to re-identify the data; and
>
> (4) The provider exercises reasonable monitoring to ensure that those contracts are not violated. The Commission seeks comment on 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.

The Commission has also invited commenters to set forth alternative or additional proposals for requirements that might make aggregate customer information less susceptible to re-identification, and asks whether it should harmonize its proposal with its existing privacy rules.

VI. Securing Customer Proprietary Information

The NPRM notes that "[s]trong data security protections are crucial to protecting the confidentiality of customer PI." To that end, the Commission proposes both a general data security requirement for BIAS providers and specific types of practices they must engage in to "protect confidential customer information from misappropriation, breach and unlawful disclosure." It's proposal draws from a wide variety of sources, including the Health Insurance Portability and Accountability Act (HIPAA) Security Rule for health information, the Gramm-Leach-Bliley Act (GLBA) for financial information, FTC best practices, FTC and FCC settlements, and state laws.

A. General Standard

The NPRM proposes to codify the Commission's interpretation that under Section 222(a) of the Act, BIAS providers are obligated 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." The FCC seeks comment on its definitions of the terms security, confidentiality, and integrity in its proposed general standard.

B. Protecting Against Unauthorized Use or Disclosure of Customer PI

To ensure compliance with the general security standard discussed above, the NPRM proposes the following specific practices with which every BIAS provider would be required to comply:

- **Risk Management Assessments.** BIAS providers would be required to establish and perform regular risk management assessments and promptly remedy any weaknesses in the provider's data security system identified by such assessments. The NPRM proposes to allow each BIAS provider to determine the particulars of and design of its own risk management program.
- **Employee Training.** The NPRM proposes to require BIAS providers to train employees, contractors, and affiliates that handle customer PI about the BIAS provider's data security procedures, and to sanction any such employees, agents or contractors for violations of those measures.
- **Reasonable Due Diligence and Corporate Accountability.** BIAS providers would be required to ensure due diligence and oversight of the proposed security requirements by designating a senior management official with responsibility for implementing and maintaining the BIAS provider's data security procedures.
- **Customer Authentication and Notification of Account Changes.** The Commission proposes that BIAS providers establish and use robust customer authentication procedures to grant customers or their designees access to customer PI, including a requirement to notify customers of account changes to protect against fraudulent authentication attempts. It seeks comment on whether the Commission 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, and the advantages and disadvantages of such a mechanism. The NPRM also asks whether it should harmonize the existing call detail disclosure protections for voice providers with its proposed authentication rules, and whether it should adopt specific rules for cable and satellite providers.
- **Right to Access and Correct Customer PI.** Separately, the Commission asks whether it should 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. If it adopts such rules, it asks whether it should 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 PI. The Commission also asks whether it should harmonize its existing rules with its proposal.
- **Accountability for Third Party Misuse of Customer PI.** The Commission proposes to

require BIAS providers to take responsibility for the use of customer PI by third parties with whom they share such information, including joint venture partners and independent contractors. To that end, it seeks comment on whether a provider should be held vicariously liable for privacy violations by third parties with whom the provider shares customer PI. Alternatively, the Commission seeks comment on whether BIAS providers should obtain contractual commitments from third parties to safeguard data prior to disclosing customer PI, either through private agreements or Commission-mandated contracting standards. The Commission further seeks comment on whether it should require mobile BIAS providers to obtain similar commitments in their contracts with mobile device or mobile operating system manufacturers.

While the NPRM proposes to allow providers 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, it proposes to require providers, at a minimum, to take into account the nature and scope of the BIAS provider's activities and the sensitivity of the underlying data.

C. Limiting Collection, Retention, and Disposal of Data

Without laying out any specific proposals, the NPRM seeks comment on whether the Commission should adopt rules that would regulate or limit BIAS providers' collection of data, require providers to set reasonable retention limits for customer PI, and impose specific measures for BIAS providers when disposing of customer PI.

VII. Data Breach Notification Requirements

In the NPRM, the Commission proposes data breach notification requirements that are significantly more extensive than existing data breach requirements for voice service, and would apply to both voice and BIAS providers. Specifically, under the proposal, upon discovery of a "breach" (which is defined more broadly than under the voice CPNI rules) carriers and BIAS providers would be required to:

- 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; and
- 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.

With respect to these general proposals, the NPRM seeks comment on what information should be included in a breach notification, whether the Commission should impose recordkeeping requirements with respect to data breach notification, whether it should adopt a more flexible timeframe for notifications (e.g., as "expeditiously as practicable"), and whether the Commission should harmonize its voice and broadband data breach notification rules.

A. Customer Notification of a Breach

As proposed in the NPRM, the 10-day customer notice requirement would apply to both BIAS providers and other telecommunications providers. The Commission proposes to adopt a trigger to limit breach notification in certain circumstances, and seeks comment on what the appropriate trigger should be (e.g., likelihood of misuse of the data or the number of affected consumers).

- **Content of Customer Data Breach Notification.** The NPRM proposes to require that a carrier's breach notification to affected customers include the following information:

  (1) The date, estimated date, or estimated date range of the breach;

  (2) 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;

  (3) 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;

  (4) Information about how to contact the Federal Communications Commission and any state regulatory agencies relevant to the customer and the service; and

  (5) 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.

- **Method of Customer Data Breach Notification.** The Commission also proposes to require carriers to "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."

B. Notification to Federal Law Enforcement and the Commission

The NPRM would heighten the existing data breach notification rules by requiring carriers to notify the Commission of all data breaches, in addition to notifying law enforcement (i.e., the FBI and Secret Service). As explained above, the proposal would limit the law enforcement notification requirement only to breaches that affect 5,000 or more customers.

The Commission seeks comment on whether there are certain breaches for which no Commission notification requirement should be imposed, and whether the 5,000 customer limit is the appropriate threshold for the FBI notification requirement. In addition, the Commission asks if it should adopt a notification requirement when a carrier "discovers conduct that would reasonably lead to exposure of customer PI."

C. Record Retention

The Commission proposes to require BIAS providers 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 (consistent with the existing Section 222 record retention requirements for voice providers). To that end, the Commission seeks comment from telecommunications carriers about how the existing rules work in practice, including costs of compliance and if any of the information retained is unnecessary.

D. Harmonization with Existing Rules

The Commission asks whether its proposed data breach notification rules should apply equally to all providers of telecommunications services, or if there are reasons that BIAS providers and other telecommunications carriers should have different notification requirements for breaches of customer PI. It further seeks comment on whether to adopt harmonizing rules for cable and satellite providers.

E. Third-Party Data Breach Notification

The NPRM seeks comment on how the Commission's rules should treat data breaches by third parties with which a BIAS provider has shared customer PI. For example, the Commission asks whether BIAS providers should be required to contractually bind third parties to the same breach notification rules adopted for BIAS, or if BIAS providers and third parties should be permitted to determine by contract which party will provide the required notification if there is a third-party breach.

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

The Commission proposes and seeks comment on whether it should adopt rules that prohibit or apply heightened notice and choice requirements to certain BIAS practices related to privacy.

Specifically, the NPRM proposes to "prohibit the offering of broadband services contingent on the waiver of privacy rights by consumers." Further, it seeks comment on whether to prohibit or impose heightened privacy protections for the following practices: (1) offering higher-priced broadband services for heightened privacy protections; (2) using deep packet inspection (DPI) for purposes other than network management; and (3) using persistent tracking technologies.

Finally, the NPRM seeks comment on how to interpret the requirements of Section 222(b), which relates to carrier PI. Specifically, it asks whether it should understand this provision 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 a purpose other than the provision of the telecommunications service," or only to the three types of proprietary information referred to in Section 222(a) (i.e., proprietary information relating to carriers, equipment manufacturers, and customers).

IX. Miscellaneous Issues

The NPRM also seeks comment on a number of other proposals and issues.

- **Prohibiting Binding Arbitration Clauses in Customer Contracts.** The Commission seeks comment on the appropriate dispute resolution mechanisms to address customer complaints regarding the collection, use and disclosure of customer information. Notably, the NPRM asks whether the Commission should prohibit BIAS providers from compelling arbitration in their contracts with customers.

- **State Law Preemption.** The NPRM proposes that the Commission would "preempt state laws only to the extent they are inconsistent with any rules adopted by the Commission." It further proposes that preemption would occur "on a case-by-case basis, without the presumption that more restrictive state requirements are inconsistent with [the FCC's] rules." The Commission seeks comment on whether to apply its preemption authority more broadly in this context, or whether it should decline to preempt state laws altogether.

- **Multi-stakeholder Processes.** The Commission also seeks comment on a number of other

publicly proposed BIAS privacy frameworks and recommendations, including those from industry and public advocacy organizations. It further asks whether it should "incorporate multi-stakeholder processes into [its] proposed approach to protecting the privacy of customer PI," similar to efforts by other agencies such as the National Telecommunications and Information Administration.

- **Legal Authority.** The Commission seeks comment on its authority to adopt its proposed rules, including its authority under Sections 201, 202, 222, and 705 and Title III of the Communications Act, and Section 706 of the 1996 Telecommunications Act.

X. Conclusion

If adopted, these rules would represent perhaps the most sweeping and prescriptive privacy and data security rules at either the federal or state level, particularly if the Commission harmonizes its proposed BIAS privacy rules with its privacy and data security rules for voice, cable video, and satellite services. Further, because of their scope, these rules may also have an indirect impact far beyond BIAS services themselves, particularly for application-layer services, equipment manufacturers, and other third parties that interact or contract with BIAS providers.

Kelley Drye's Communications and Privacy & Information Security practice groups are well-versed in privacy law at the federal and state level, and stand ready to help interested parties understand the potential scope of these rules and how to get involved in the proceeding. Should you have any questions, please contact any of the attorneys listed in the margin.