wiley

ALERT

Summary of the April 1, 2016 NPRM: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services (WC Docket No. 16-106; FCC 16-39)

April 5, 2016

On April 1, the Federal Communications Commission (FCC) released a Notice of Proposed Rulemaking (NPRM) proposing to establish a new consumer privacy framework for broadband Internet access service providers (ISPs). The proposed rules would not apply to the privacy practices of web sites, apps, and other "edge services."

Importantly, the NPRM proposes protections for types of information beyond that traditionally considered "Customer Proprietary Network Information" (CPNI). In addition to providing guidance on the information that should be considered CPNI in the broadband context (*e.g.*, service plan and traffic information), the FCC proposes a new category of protected information, Customer Proprietary Information (CPI), including both CPNI and other personally identifiable information (PII) acquired by ISPs about their customers. The new transparency, control, and security rules proposed in the NPRM would apply to this broader category of information.

The NPRM proposes a three-tiered consent framework for ISP use and sharing of customer proprietary information.

- **Consent Implied:** No additional customer consent beyond creation of a customer-ISP relationship is needed for use of customer data necessary to provide broadband services, for marketing the type of broadband service purchased by a customer, and for certain other purposes consistent with customer expectations (*e.g.*, contacting public safety).

Authors

Bennett L. Ross
Partner
202.719.7524
bross@wiley.law

Practice Areas

Telecom, Media & Technology

- **Opt-out:** ISPs would be allowed to use (and share with affiliates) customer data to market other communications-related services unless the customer affirmatively opts out.
- **Opt-in:** All other uses and sharing of CPI would require express, affirmative "opt-in" consent from customers.

Among other matters, the NPRM also seeks comment on:

- **Transparency requirements for ISPs,** mandating notice to customers about how data is used and collected, and how privacy preferences can be changed;
- **New data security mandates for ISPs,** including requirements to adopt specified risk management practices, training, customer authentication, and corporate governance;
- **Federal data breach notification obligation for all telecommunications carriers**;
- **Specific business practices,** such as whether deep packet inspection, persistent tracking, and financial inducement should be prohibited or have heightened notice obligations;
- **Dispute resolution mechanisms,** including whether ISPs should be prohibited from compelling arbitration in customer agreements;
- **Alternative proposals for BIAS privacy frameworks,** which the FCC has received from industry associations and other organizations; and
- **The legal authority upon which the proposed rules would be based,** which is primarily Section 222 of the Communications Act, but also includes Sections 201, 202, 303(b), 303(r), 316, 705, and 706 of the Act.

Comments and Reply Comments on the NPRM will be due May 27 and June 27, 2016, respectively. The proposed rule changes and main tentative conclusions of the NPRM are summarized below.

* * *

1. Background

In the 2015 *Open Internet Order*, the FCC designated Broadband Internet Access Services (BIAS) as telecommunications services subject to the statutory provisions of Title II of the Communications Act of 1934, as modified by the Telecommunications Act of 1996. Section 222 of the Communications Act imposes a duty on telecommunications carriers to protect the confidentiality of proprietary information of their customers. In this proceeding, the FCC proposes to adapt its CPNI regime for application to broadband ISPs, and to build upon these existing rules to create new consumer privacy protections for broadband and other telecommunications services.

2. Discussion

The NPRM begins by setting the scope of its proposals through defining key terms. The NPRM then moves to its substantive proposals for consumer privacy protection, which the FCC says are "built upon the three foundations of privacy – transparency, choice, and security." Finally the NPRM addresses a number of other proposals and matters, including the FCC's legal authority to adopt the proposals put forth in the NPRM.

A. Scope of the Rule/Defining Key Terms

The FCC proposes several new definitions that apply to and set the scope of the substantive proposals contained in the NPRM. The FCC seeks comment on each of these definitions.

Broadband Internet Access Service (BIAS). The FCC proposes to use the definition of Broadband Internet Access Service applied in the *2015 Open Internet Order*. Under this proposal, BIAS will 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." (¶ 29)

Affiliate. The FCC seeks comment on whether it should use its established definition of affiliate, meaning "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," or adopt a new definition. (¶ 30)

Customer. The FCC proposes 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. (¶ 31) This definition is broader than the definition used in the legacy CPNI rules, which applies only to current customers. The FCC seeks comment on whether the definition of customer should reflect the possibility of multiple broadband users on a single residential subscription. (¶ 34)

Customer Proprietary Network Information (CPNI). The FCC proposes to adopt the statutory definition of CPNI: "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," but the FCC asks whether there is a need for the second part of the definition dealing with telephone services) in the broadband context. (¶38)

The FCC seeks comment on several specific types of information that it considers CPNI in the broadband context, including (1) service plan information; (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. (¶¶ 41-47) The FCC asks whether other types of information should be considered CPNI, including: (1) port information; (2) application headers; (3) application usage; and (4) CPE information. (¶¶ 48-52)

Customer Proprietary Information (CPI or Customer PI). Section 222(a) of the Communications Act imposes on telecommunications carriers a duty "to protect the confidentiality of proprietary information of, and relating to, . . . customers." The FCC interprets this duty as extending beyond just CPNI, and therefore proposes to adopt a new defined term, "Customer Proprietary Information," which includes (1) customer proprietary network information (CPNI); and (2) personally identifiable information (PII) the BIAS provider acquires in connection with its provision of BIAS. (¶ 57) The FCC asks whether other categories of information should be included, and whether it should adopt harmonizing changes to legacy CPNI rules. (¶¶ 58-59)

*Personally Identifiable Information (PII).*The FCC proposes to define personally identifiable information as any information that is linked or linkable to an individual. (¶ 60) The FCC proposes 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. (¶ 61) The FCC proposes that PII would include, but not be limited to: name; Social Security number; date and place of birth; mother's maiden name; unique government identification numbers; 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). (¶ 62)

Content of Customer Communications. The FCC asks how it should treat the content of communications under Section 222, and whether there is a need for the FCC to provide heightened privacy protections for communications content beyond those contained in 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. (¶ 67)

Opt-Out and Opt-In Approval. The FCC proposes 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. (¶ 68) The FCC proposes 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 and before any use of, disclosure of, or access to such information. (¶ 69) The specific requirements for opt-out and opt-in notifications are detailed in the proposed rules.

Communications-Related Services. The FCC seeks comment on how best to define "communications-related services" (the use of CPI for marketing of which would require opt-out consent by customers) in the broadband context. (¶ 71) The current rules define the term to mean "telecommunications services, information services typically provided by telecommunications carriers, and services related to the provision or maintenance of customer premises equipment," and the FCC seeks comment on how it might narrow the scope of services covered by this definition. (¶ 72)

Aggregate Customer PI. The FCC 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. (¶ 74)

Breach. The FCC proposes 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," whether intentional or inadvertent. (¶ 75)

Other Definitions. The FCC asks whether there are other terms it should define or legacy definitions that should be revisited. Specifically it seeks comment on the appropriate definition of "customer premises equipment" in the age of Internet-connected devices. (¶ 79) It also seeks comment on changes that are needed to differentiate or harmonize legacy CPNI rules with the proposed broadband privacy rules. (¶ 80)

B. Privacy Notice Requirements

To promote transparency in privacy practices, the FCC proposes rules requiring Broadband ISPs to provide customers with clear and conspicuous notice of their privacy practices and to provide existing customers with advanced notice of material changes in their privacy policies. (¶ 82) The FCC seeks comment on each of these proposals, as well as standardizing the format of these notices, and on the specific information that must be provided in the notices. (¶ 82)

Privacy Notice Requirements. The FCC proposes rules that would require Broadband ISP privacy policies to give notice of (1) the Types of Customer PI collected and how it is used/disclosed; and (2) Customers' rights with respect to their proprietary information. Notices must be clear and comprehensible. (¶ 83) Notices must be made available to prospective customers at the point of sale, prior to purchase of BIAS (whether online, in person, or over the phone), and must be persistently available through the ISP's website and mobile app. (¶ 83) The FCC asks whether these rules are sufficient, or if it should adopt additional requirements, for example, to ensure privacy information is accessible to persons with disabilities. (¶ 84) The FCC asks about the types of information in should require in the disclosures, including whether it should require disclosure of the specific entities with which ISPs will share information, or just the categories of entities. (¶ 85) The FCC seeks comment on the burdens of compliance with these obligations. (¶ 89)

The FCC seeks comment on whether it should adopt a standardized approach and template for BIAS providers' privacy notices. (¶ 91) It asks whether such a standardized template should be adopted as a voluntary safe harbor for privacy notice requirements. (¶ 92) The FCC also seeks comment on whether it

should require BIAS providers to create a consumer-facing privacy dashboard that would allow customers to monitor and control the use of their proprietary information collected by the BIAS provider, request correction of inaccurate customer PI, and request deletion of any categories of customer PI the customer no longer wants the provider to maintain. (¶ 95)

Providing Notice of Material Changes in Privacy Policies. The FCC proposes 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. (¶ 96) These notices must be provided through email, on customer bills, and via a link on the BIAS provider's website. The notice must clearly and comprehensibly explain the changes to the privacy policies and the customer's rights regarding approval/denial of the collection and use of its proprietary information. (¶ 96) The FCC asks whether it should require the notice within a specified timeframe in advance of the changes, and if it needs to revisit its definition of a material change. (¶ 97) The FCC seeks comment on whether the 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. (¶ 100)

Mobile-Specific Considerations & Harmonizing Notices. The FCC seeks comment on whether there are any mobile-specific considerations to its proposed notice requirements. (¶ 102) The FCC also seeks comment on whether it should harmonize required privacy notices regarding the use of customer information for voice, video, and broadband services. (¶ 103)

C. Customer Consent for Use and Disclosure of Proprietary Information

The FCC proposes a three-tiered framework for obtaining customer consent for use and disclosure of proprietary information, distinguishing between uses of information for which no express consent is required, uses for which customers may opt-out, and uses prior to which Broadband ISPs must obtain express customer opt-in consent.

Customer Consent Not Required. The FCC seeks comment on how it should interpret and implement section 222(c)(1), which allows BIAS providers 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" without consent. (¶ 112) The FCC proposes to adopt rules permitting the disclosure of customer PI for marketing additional offerings without seeking further customer consent if the customer subscribes to that category of service from the BIAS provider. (¶ 114) The FCC asks whether it should adapt the section 222(d) statutory exceptions for disclosure to the broadband context, specifically exceptions allowing disclosure for call location and information for public safety, and allowing disclosure to protect against threats, vulnerabilities, and other unlawful conduct. (¶ 115, 116, 117).

Customer Consent Required. The FCC proposes to require BIAS providers to provide customers with notice and an opportunity to opt out before using customer PI, sharing customer PI with affiliates, and marketing communications-related services to the customer. (¶ 122). The FCC seeks comment on customers' expectations

and preferences regarding the use of customer PI. (¶ 123). The FCC asks whether the expectations and preferences here differ when compared to the expectations and preferences of customer PI for voice services. (¶ 125).

The FCC propose to require BIAS providers to obtain customer opt-in consent before sharing or disclosing customer PI for any other purpose, with the exception of the disclosures discussed above. (¶ 127) The FCC seeks comment as to whether BIAS providers benefit from using customer PI for purposes other than those associated with marketing communications-related services. (¶ 128) The FCC asks whether information disclosed to third parties falls outside of section 222's protections. (¶ 130) The FCC also seeks comment on the costs and benefits of its proposal (¶ 131), and the impact on the larger Internet ecosystem. (¶ 132)

Alternative Frameworks for Customer Choice. The FCC asks whether other frameworks exist that could better provide broadband customers control over their customer PI. (¶ 134) The FCC seeks comment on whether BIAS providers have a need to use or share certain types of "highly sensitive" customer data, such as Social Security numbers and health information. (¶ 136) The FCC also asks how to treat content of customer communications, should it determine it is covered by Section 222. (¶ 137)

Requirements for Soliciting Opt-Out and Opt-In Approval. The FCC proposes that after the point-of-sale, BIAS providers must solicit a customer's approval before it first intends to use or disclose the customer's PI. (¶ 140) The FCC seeks comment on how BIAS providers should make customers aware of upcoming uses and disclosures. (¶ 143) The FCC proposes that BIAS providers make available an "easy-to-use" method to grant or deny approval of PI disclosure. (¶ 144) The FCC also proposes that a customer's choice regarding disclosure remain in effect until the customer revokes their choice. (¶ 147) The FCC asks whether it should apply its voice notice requirements for one-time use of CPNI to BIAS providers. (¶ 148)

Documenting Compliance. The FCC proposes to require BIAS providers to document a customer's choice regarding disclosure of their customer PI in order to promote consumer confidence. (¶ 149) The FCC asks whether it should require BIAS providers to file an annual compliance certification. (¶ 149)

Small BIAS Providers. The FCC seeks comment on whether it should implement an exception to this consumer choice framework for small BIAS providers. (¶ 151)

D. Use and Disclosure of Aggregate Customer Proprietary Information

Standard for Use and Disclosure. The FCC proposes to allow BIAS providers to use and disclose aggregate customer PI so long as the BIAS 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; (4) exercises reasonable monitoring to ensure that those contracts are not violated." (¶ 154) BIAS providers can disclose collective data about a group or category of services or customers without customer approval given that such information does not generally present any privacy concerns. (¶ 155). The FCC seeks comment on

each prong this proposal and whether it should extend it to providers of voice telecommunications services. (¶ 156) Alternatively, the FCC asks whether it should develop a list of identifiers that must be removed from data in order to determine that individual identities and characteristics have been removed. (¶ 163)

E. Data Security

General Standard. The FCC proposes to require that BIAS providers protect the security, confidentiality, and integrity of customer PI that the 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. (¶ 170) The FCC seeks comment on its interpretation of the terms "security, confidentiality, and integrity" in this standard. (¶ 173)

Protecting Against Unauthorized Use or Disclosure. The Commission proposes that BIAS providers comply with five practices to best protect against the unauthorized use or disclosure of customer PI: (1) perform regular risk management assessments and promptly remedy any identified weaknesses; (2) train employees, contractors, and affiliates on the proper data security procedures for handling customer PI; (3) designate a senior management official to be responsible for setting and ensuring compliance with the data security procedures; (4) establish robust customer authentication procedures for customers; and (5) take responsibility for third party use of shared customer PI. (¶ 174) The FCC asks whether it should establish safe harbors or convene multistakeholder processes to develop best practices. (¶ 178) It also asks whether it should prescribe specific administrative, technical, and physical conditions that must be included in BIAS providers' security plans. (¶ 179)

Risk Management Assessments. The FCC proposes to require BIAS providers to establish and regularly perform risk management assessments to protect against data security threats and vulnerabilities. (¶ 180) The FCC seeks comment on whether it should determine the specifics of the risk management assessments or whether the BIAS provider should determine the specifications in accordance with a safe harbor that the FCC establishes. (¶ 182) The FCC also seeks comment on how "regularly" BIAS providers should conduct assessments and how "promptly" BIAS providers should address perceived threats and vulnerabilities. (¶ 183, 184)

Employee Training. The FCC proposes to require BIAS providers to train employees, agents, and contractors on proper data security measures and sanction any employee, agent, or contractor who does not comply with the set measures. (¶ 185) The FCC asks whether it should provide additional clarifications for the training process and other training requirements. (¶ 187)

Due Diligence and Corporate Accountability. The FCC proposes to require BIAS providers to designate a senior management official who is responsible for ensuring that the provider's data security program is both implemented and maintained. (¶ 188) The FCC seeks comment on the feasibility of this proposal in light of a BIAS provider's current practice and organization and compliance structure. (¶ 189)

Customer Authentication. The FCC proposes to require BIAS providers to implement and maintain a customer authentication process for a customer's access to the customer's PI. (¶ 191) The FCC also seeks comment on the advantages and disadvantages of multifactor authentication, and other forms of customer authentication. (¶ 194, 195, 199) The FCC asks whether a required customer authentication process should be password protected. (¶ 196)

The FCC seeks comment on whether it should require BIAS providers to notify consumers of account changes and attempted account changes. (¶ 201) The FCC also seeks comment on whether BIAS providers should provide customers with access and correction rights to all customer PI retained by the BIAS provider. (¶ 205) The FCC seeks comment on the type of data that a BIAS provider would possess and whether customer access should vary by type of data. (¶ 206)

Accountability for Third Party Misuse. The FCC seeks comment on how to best protect customer PI when the BIAS provider shares the data with a third party. (¶ 210) The FCC asks whether BIAS providers are vicariously liable for a third party's violation. (¶ 211) It also seeks comment on whether BIAS providers should obtain contractual commitments from third parties to ensure that customer PI is adequately protected. (¶ 212) Specifically, the FCC asks whether it should require mobile BIAS providers to seek contractual commitments related to data collection and use from mobile device and operating system manufacturers. (¶ 213)

Other Safeguards. The FCC seeks comment on whether there are additional safeguards that it has not addressed. (¶ 215) The FCC also asks if it should require that BIAS providers comply with other safeguards, such as using standard encryption. (¶ 216)

Factors for Consideration in Implementing Data Security Measures. The FCC proposes that, at a minimum, BIAS providers implement data security measures based on the "nature and scope of the BIAS provider's activities and the sensitivity of the underlying data." (¶ 217)

Limiting Data Collection, Retention, and Disposal.The FCC asks whether its rules should limit the amount and type of customer PI that BIAS providers may collect.(¶ 222).The FCC seeks comment on unrestricted data collection and whether there are certain types of data that BIAS provider should be unable to collect.(¶ 224) The FCC also asks whether BIAS providers should set retention limits for customer PI.The FCC seeks comment on whether retention periods should be set by the category of data.(¶ 225, 226)The FCC seeks comment on whether it should draft and implement a data destruction requirement and, in doing so, use states' record disposal laws for guidance.(¶ 231)

F. Data Breach Notification

The FCC proposes to require all telecommunications carriers to notify customers, the FCC, and Federal law enforcement agencies within specified time periods after discovering a breach of customer PI.

Customer Notification. The FCC proposes to require BIAS providers and other telecommunications carriers to notify customers of breaches of customer PI within 10 days after discovery of the breach. The FCC seeks

comment on what circumstances should trigger notification and whether it should borrow from state law in this respect. (¶¶ 236-37)

The FCC seeks comment on an alternative, more flexible standard for the timing of customer notifications, such as "as expeditiously as practicable" or "without unreasonable delay," and asks whether there should be any exceptions to this requirement. (¶ 241) The FCC also seeks comment on whether a provider should be required to provide notice when it discovers conduct that would reasonably lead to exposure of customer PI. (¶ 242)

The FCC proposes that customer notifications include the following information about the breach: the date or date range; a description of the customer PI involved; information that the customer can use to contact the provider; information about how to contact the FCC and appropriate state regulatory agencies; and information about national credit-reporting agencies and steps customers can take to guard against identity theft. (¶ 243) The FCC also proposes to require providers to provide written notification to the customer's address, email address, or by contacting the customer by other electronic means provided by the customer. (¶ 245)

Notification to Federal Law Enforcement and the Commission. The FCC proposes to require telecommunications providers to notify the Commission within seven days of discovery of a breach, and notify the FBI, and the Secret Service no later than seven days after discovery of a breach reasonably believed to have affected at least 5,000 customers. The FCC further proposes to require federal law enforcement notifications to occur at least three days before a provider notifies affected customers. (¶ 246) For both law enforcement and FCC notifications, the FCC proposes to extend existing Section 222 requirements for both the method and substance of data breach notifications. (¶ 251)

Record Retention. The FCC proposes to extend existing Section 222 record retention requirements regarding data breaches to BIAS providers. This would require providers to maintain a record of any discovered breached and notifications to the FBI, the Secret Service, and customers for a period of at least two years. (¶ 252-53)

Harmonization. The FCC proposes to apply is new data breach requirements to both voice and BIAS providers. The FCC asks whether the rules should apply equally to all providers of telecommunications services, or whether there are reasons why BIAS providers and other providers should have different notification requirement for breaches of customer PI. (¶ 254)

*Third-Party Data Breach Notification.*The FCC seeks comment on how it should treat data breaches by third parties with which a provider has shared customer PI.The FCC proposes that BIAS providers enter into contractual agreements with third parties to ensure that data breach notification procedures are followed by whichever party has access to customer PI.(¶ 255)

G. Specific Business Practices that May Be Prohibited

The FCC proposes to prohibit the offering of broadband services contingent on the waiver of privacy rights by consumers. Should commenters suggest heightened notice and choice requirements for certain practices, the FCC asks that those commenters explain why it is appropriate for the practice at issue and to identify the statutory authority that would support such requirements. (¶¶ 256-57)

The FCC seeks comment on a number of proposals to address specific practices:

- *Service Offers Conditioned on the Waiver of Privacy Rights*. The FCC proposes to prohibit BIAS providers from making service offers contingent on a customer surrendering her privacy rights. The FCC also asks for alternative proposals to prohibit these type of arrangements and for comment on alternative approaches to protect broadband consumers from potentially coercive service offerings. (¶ 258)
- *Financial Inducement Practices*. The FCC seeks comment on whether business practices that offer customers financial inducements for consent to use and share confidential information are permitted under the Act. The FCC asks whether it should adopt rules concerning such practices, such as subjecting the practices to opt-out or opt-in requirements. The FCC also asks whether offering these practices is violative of the Section 222(a) duty to protect the confidentiality of customers' proprietary information, or whether these practices actually benefit consumers. (¶¶ 259-63)
- *Deep Packet Inspection.* The FCC seeks comment on whether the use of DPI for purposes other than providing broadband services and reasonable network management should be prohibited or subject to a heightened approval framework. The FCC asks whether the use of DPI should be subject to opt-out or opt-in requirements. The FCC also asks for comment on how broadband providers use DPI and to what extent DPI is encrypted. (¶¶ 264-67)
- *Persistent Tracking Technologies*. The FCC seeks comment on whether the use of persistent tracking technologies should be prohibited or subject to opt-out or opt-in consent. The FCC also asks what other technologies can be used by BIAS providers to track broadband users and their devices, whether these technologies pose a risk to BIAS consumers, and, if so, how best to protect consumers' private information and enhance consumer control. (¶¶ 268-70)

Section 222(b). The FCC seeks comment on how best to apply the limitations imposed by Section 222(b) on carriers receiving proprietary information from other carriers for the purposes or providing telecommunications services. The FCC asks whether the provision applies specifically to carriers' proprietary information or whether it applies to all three types of proprietary information referred to in Section 222(a): information of or relating to carriers, equipment manufacturers, and customers. (¶ 271)

Other. The FCC seeks comment on whether there are other practices involving the use or disclosure of customer PI that should be prohibited or subject to heightened notice and choice requirements. (¶ 272)

H. Dispute Resolution

The FCC asks whether its current informal complaint resolution process for alleged violations of the Communications Act is sufficient to address customer complaints under the rules proposes in the NPRM. The FCC seeks comment on whether BIAS providers do or should provide other optional, impartial, and efficient dispute resolution mechanisms. (¶ 273) The FCC seeks comment on whether to prohibit BIAS providers from compelling arbitration in their contracts with customers. (¶ 274) The FCC also seeks comment on any other dispute resolution proposals, including whether and how to harmonize such proposals with the Commission's existing voice CPNI framework. (¶ 275)

I. Miscellaneous

Preemption of State Law. The FCC proposes to preempt state laws only to the extent that they are inconsistent with the rules that the Commission adopts. (¶ 276) But the FCC also seeks comment on whether a broader application of its preemption authority is warranted or whether it should decline to preempt state law altogether. (¶ 277)

Other Proposed Frameworks and Recommendations. The FCC seeks comment on a number of proposals and recommendations for BIAS privacy frameworks that have been submitted by industry associations and other organizations. (¶¶ 278-79) Specifically, the Commission seeks comment on proposals put forth 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).

Other. The FCC seeks comment on any alternative approaches it can take to protect customer privacy, preserve customer control, and promote innovation. (¶ 292)

Multi-stakeholder Processes. The FCC seeks comment on whether there are specific ways it should incorporate multi-stakeholder processes into its proposed approach to protecting customer PI. The FCC asks what lessons have been learned from the multi-stakeholder processes that NTIA has convened on behalf of the Department of Commerce and whether such processes would be useful in developing guidelines and best practices. (¶ 293)

J. Legal Authority

The FCC proposes to ground its new rules primarily in Section 222 of the Communications Act, but it also finds support for the rules in Sections 201 and 202 of the Communications Act and Sections 705 and 706 of the Telecommunications Act. (¶ 294) The FCC seeks comment on its chosen legal framework and asks whether there is additional statutory authority upon which it should rely, including for example Sections 631 and 338(i) of the Communications Act. (¶ 295)

Section 222. The FCC seeks comment on whether its proposals are fully supported by Section 222 of the Communications Act. The FCC explains that while its earlier decisions focused on Section 222(c)'s protection of CPNI, the set of customer information protected by Section 222(a) is broader than CPNI. (¶¶ 297-98) The FCC seeks comment on its proposal to rely on subsection (a) of Section 222 for authority to adopt rules to protect customer information that is not CPNI. (¶ 300) The FCC also seeks comment specifically on its reliance on Section 222 to adopt customer disclosure rules (¶ 301), customer approval rules (¶ 302), and data security and breach notification rules (¶ 303)

Additional Statutory Authority. The FCC seeks comment on how its reliance on Sections 201 and 202 of the Communications Act for the Open Internet "no-unreasonable interference/disadvantage" standard should inform the rules proposed in the NPRM. (¶ 305) The FCC also asks to what extent FTC Act and the FTC's precedents may inform its consideration of whether practices by common carriers are unjust or unreasonable. (¶ 306)

The FCC seeks comment on whether Section 705 of the Telecommunications Act provides a source of authority for protecting the privacy of customer information, including the content of customer communications. (¶ 307) The FCC also asks whether the rules adopted in the NPRM are independently supported by Section 706 of the Telecommunications Act. (¶ 308-09) Finally, the FCC asks whether Section 303(b), 303(r), and 316 of the Communications Act give it authority to adopt rules for licensed entities providing mobile BIAS. (¶ 310)

For further information on these issues, please contact one of the authors listed.