Cooley

FCC Releases Sweeping Privacy Order

November 7, 2016

The Federal Communications Commission has released a 177-page order detailing new privacy and data security rules. It is important to note that these new rules not only apply to providers of broadband internet access service ("BIAS") but also replace the existing customer proprietary network information ("CPNI") rules applicable to voice providers. The order also excludes from these rules services provided to enterprise customers if privacy and data security issues are addressed in their service agreements. This alert supplements our recent alert based on the information provided in a Fact Sheet released when the FCC approved the rules.

Scope of the rules

The rules apply to all companies providing telecommunications services subject to Title II of the Federal Communications Act, including BIAS providers. For providers of voice and data services, including interconnected VoIP services, these new rules will replace the existing CPNI rules. Voice and other telecommunications services provided to enterprise customers are excluded from all of these rules as long as their contracts address the issues of transparency, choice, data security, and data breach, and provide a mechanism for customers to communicate with the carrier about privacy and data security concerns. Carriers serving enterprise customers will, however, still be subject to the more general CPNI provisions of section 222 of the Communications Act. Carriers providing enterprise services should revise their customer contracts accordingly if they wish to avoid application of these rules.

The rules also do not apply to edge providers or to the non-telecommunications services offered by BIAS providers, such as email, websites, cloud storage services, social media sites, music streaming services, and video streaming services. Consistent with the definition of BIAS adopted in the Open Internet Order, the rules also do not apply to premises operators such as coffee shops, bookstores, airlines, private end-user networks (*e.g.,* libraries and universities) and other businesses that acquire broadband service from a broadband provider to enable patrons to access the internet.

The order broadly defines customer to include former customers and applicants, as well as current subscribers. The FCC purposely did not include any end date by which former customer data ceases to be protected so as to encourage data minimization. Thus, all covered data remains subject to the rules as long as it is retained by the provider. Protected customers also include any other users of the subscriber's service, such as other people in the household or guests, and their data is subject to whatever privacy choice the subscriber made.

Types of information covered and key definitions

The FCC defines three types of customer proprietary information or customer PI: (1) individually identifiable Customer Proprietary Network Information (CPNI) as defined in Section 222(h); (2) personally identifiable information (PII); and (3) the content of communications. Some types of information may fall within different categories. A fourth type of information – de-identified information – is not subject to the privacy rules and may be shared or used without needing to obtain approval.

CPNI in the broadband context

In the context of BIAS, the FCC interprets the statutory definition of CPNI to include the following non-exhaustive list of information.

- Broadband service plans (*e.g.,* service type (wireless or cable), speed, pricing and capacity).
- Geo-location (*e.g.,* GSP, service address, nearby cell towers or beacons)
- MAC addresses and other device identifiers that uniquely identify a device

- Dynamic or static IP addresses and domain name information
- Traffic studies (*e.g.,* packet size, data consumption, average speed, frequency of visits to particular domains and IP addresses) specific to identifiable customers
- Port information (port numbers can identify specific destinations used for specific purposes)
- Application header (Application headers instruct the recipient application how to process the communication and may include unique identifiers injected by the BIAS provider, such as a unique identifier header (UIDH))
- Application usage (constitutes CPNI when the BIAS provider directs the collection and storage of usage information)
- Application payload (the substance of a communication, such as the text of an email or instant message or the body of a webpage)
- Customer premises equipment (CPE) and device information (*e.g.,* model number, operating system, software and/or settings of smart phones, tablets, computers routers, computers, VoIP phone connected to a broadband service).

Some of this information is deemed sensitive and subject to opt in approval (e.g., geo-location) while other information is non-sensitive and subject to opt out approval (e.g., Broadband service plans).

Personally identifiable information

Customer PII is "any information that is linked or reasonably linkable to an individual or device." Information is "linked or reasonably linkable" if "it can reasonably be used on its own, in context, or in combination to identify any individual or device, or to logically associate with other information about a specific individual or device." The FCC provides an "illustrative, non-exhaustive" list of examples of PII (where each element could be PII):

- Name, physical address, and telephone number
- Social Security number, date of birth and mother's maiden name.
- Government issued identifiers (*e.g.,* driver's license number)
- Email address or other online contact information
- MAC addresses or other unique device identifiers and IP addresses
- Persistent online or unique advertising identifiers

Content of communications

Content is defined as "any part of the substance, purport, or meaning of a communication or any other part of a communication that is highly suggestive of the substance, purpose or meaning of a communication." The definition is intended to consistent with the definitions contained in the wiretap laws, the Electronic Communications Privacy Act (ECPA) and section 705 of the Communications Act. The FCC also cautions that some types of metadata or the information in application headers such as source and destination information in an email or website URL may fall within the definition of content. Among the types of data considered content are: contents of emails; communications on social media; search terms; web site comments; items in shopping carts; inputs on web-based forms; and consumers' documents, photos, videos, books read and movies watched.

De-identified data

The FCC has expressed concerns that de-identified data may too readily be re-identified and linked back to specific persons or devices. It adopted the FTC's three prong test for de-identified information and places the burden squarely on the provider to demonstrate that identifying information has been removed and cannot be reconstructed. The three-part test for de-identified information is as follow:

1. The information must not be linked or reasonably linkable to an individual or device, and reasonableness goes to the ease of re-identification.
2. The service provider must publicly commit to not attempting to re-identify the information, for example by including language in its privacy policy.
3. Providers must contractually bar any recipient from attempting to re-identify information. However, contractual commitments are not required when the de-identified information is "so highly abstracted that a reasonable data science expert would not consider it possible to re-identify it."

Notification of privacy rights

Voice and BIAS providers must inform their customers of what information is collected and for what purpose, the types of entities (including affiliates) with which the provider will share information, and how the consumer can exercise choice. The FCC is not prescribing any specific format or content for such notices and it has called on a stakeholder group to develop by June 1, 2017, a model privacy notice that can act as a safe harbor. Notice is required in at least two situations: (1) at the point of sale and (2) before the provider makes a "material change" (a defined term) in its privacy policies.

Choice: opt-in for sensitive customer PI/opt-out for non-sensitive customer PI

Providers must obtain affirmative opt-in consent before using "sensitive customer PI" a category comprised of: geolocation, health, financial, children's information; social security numbers; content; and web browsing and app usage history and their functional equivalents. In addition, for providers of voice services, the FCC treats call detail information as sensitive information requiring opt-in approval.

Providers may obtain permission to use non-sensitive customer PI via either opt-in or opt-out consent. Under current CPNI rules, providers must wait 30 days before assuming the customer does not intend to opt out. The FCC eliminates that waiting period. Although no waiting period is adopted the rules do not permit carriers to assume that a customer has granted opt-out consent "when a reasonable customer would not have had an opportunity to view the solicitation." While this creates a more flexible standard, it would appear to place providers at some risk that they would start using or sharing data prematurely.

Marketing by the provider (first-party marketing)

The FCC rejected a broad first-party marketing exception to the consent requirements. Instead, carriers may use non-sensitive information without consent only to upsell existing services or to sell services typically bundled with internet access, such as voice or video services. Carriers may not use sensitive information for first-party marketing without opt-in consent.

Financial incentives to relinquish privacy rights

The order bars BIAS providers from conditioning the provision of broadband service on a customer surrendering his or her privacy rights. It also imposes heightened disclosure and consent requirements, including obtaining opt-in consent, for BIAS offerings of discounts or other financial incentives in exchange for use of any customer PI.

Data security and breach notification

The FCC does not prescribe any specific data security duties but "requires that every BIAS provider and other telecommunications carrier to take reasonable steps to protect customer PI from unauthorized use." A covered provider *must* adopt security practices "appropriately calibrated to the nature and scope of its activities, the sensitivity of the underlying data, the size of the provider, and technical feasibility."

Although the FCC does not propose specific security steps, the order makes clear an expectation that covered providers will adopt and maintain best security practices (called exemplary practices) as reflected in documents such as the NIST cybersecurity framework. The order identifies various types of practices the FCC considers reasonable, strongly indicating that failure to adopt these principles could result in enforcement action if there is a breach. This approach is similar to that taken by the California Attorney General.

Definition of breach

The FCC defines a breach as "any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information." Providers must report breaches within specified timeframes unless they "can reasonably determine that no harm to customers is reasonably likely to occur." The order states that providers will not be held strictly liable for all data breaches, rather the touchstone is reasonableness. To be reportable and potentially actionable, however, a breach or unauthorized

disclosure or access does not require intent or a bad purpose. An inadvertent or accidental breach becomes reportable under the harm-based trigger. However, breaches involving sensitive data effectively always must be reported because the order establishes a "rebuttable presumption that any breach involving sensitive customer PI presumptively poses a reasonable likelihood of customer harm."

Notice of a breach

Customers must be notified of a breach "without unreasonable delay" but no later than 30 days after the carrier "reasonably determines that a breach has occurred." For breaches affecting 5000 or more customers, providers must also notify the FCC, the FBI and the Secret Service within 7 business days of reasonably determining an unauthorized disclosure has occurred that meets the harm-based trigger. For breaches affecting fewer than 5000 customers, the FCC must be notified "without unreasonable delay" but no later than 30 days. The phrase "reasonably determining" means more likely than not that there has been a breach. In practical terms this regime requires providers to determine within 7 days (or 30 days for smaller breaches) of discovering the beach whether the harm-based trigger has been met and notification must occur.

The order also lists a number of specific types of information that must be included in the customer notification, specifies notification methods, and imposes certain record retention obligations.

Elimination of CPNI record keeping and certification requirements

The FCC eliminates the record keeping and annual certification requirements currently imposed on telecommunications carriers and VoIP providers. These provisions had required carriers to train personnel (although training is still strongly encouraged), maintain records of marketing campaigns using CPNI and all instances of sharing CPNI with third parties, and provide five days' notice to the FCC when opt-out mechanisms did not work properly. The FCC had required carriers to annually certify to compliance with these requirements. The FCC concludes that carriers are likely to keep records needed to defend against enforcement actions and that the new breach notification rules (described above) are sufficient.

Implementation

The order establishes various effective dates that are applicable to both BIAS providers and other telecommunications carriers:

- The privacy and choice provisions will become effective the later of (1) 12 months after publication of the order in the Federal Register (FR) or (2) eight weeks after notice of approval by Office of Management and Budget ("OMB") where required. Some of the rules will require OMB approval because they impose new record keeping obligations. Small providers – those with 100,000 or fewer broadband connections (for BIAS) or 100,000 or fewer subscriber lines (for voice providers) – will have an additional 12 months.
- The data breach notification requirements will become effective the later of (1) six months after FR publication or (2) OMB approval.
- The data security rules will become effective 90 days after FR publication. The short time frame for data security rules reflects the FCC's belief that carriers have already begun to implement reasonable data security procedures.
- Provisions regarding conditioning or discounting BIAS in exchange for relinquishing privacy rights goes into effect 30 days after FR publication.
- The order does not specify a time when the elimination of current recordkeeping or certification requirements goes into effect but they presumably would expire upon the effective date of the order when published in the FR.

The order also grandfathers some previous consents but close examination of the prior consent in light of the new rules should be undertaken.

The communications practice group and the privacy & data protection practice group at Cooley have highly complementary skills that uniquely situate the firm to help companies address IoT, FCC, and other privacy and data security related issues. The communications group has a deep and sophisticated understanding of

communications networks while the privacy & data protection practice group have technical expertise and substantial experience in assessing risks and responding to cybersecurity threats. We can help you understand the implications of the FCC order as well as the various related activities and how they apply to your organization.

Key Contacts

J.G. Harrington Washington, DC	jgharrington@cooley.com +1 202 776 2818
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090