Communications | Cybersecurity, Data Protection & Privacy | November 8, 2016

New FCC Privacy Rules for Broadband and Voice Providers

By Glenn S. Richards and Deborah S. Thoren-Peden

In an order issued November 2, 2016, the Federal Communications Commission for the first time imposed privacy requirements on providers of broadband internet access services ("BIAS"). The much-anticipated order was an outgrowth of the FCC's 2015 decision to reclassify BIAS as a telecommunications service and wrested jurisdiction from the Federal Trade Commission. The rules will also apply to voice service providers (including VoIP, wireless and wireline); replacing longstanding rules.

The decision was based on the FCC's conclusion that BIAS providers have access to vast amounts of information about their customers including when they are online, where they are physically located when they are online, how long they stay online, what devices they use to access the internet, what websites they visit and what applications they use. According to the FCC, the rules will give broadband customers the tools they need to make informed choices about the use and sharing of their confidential information by their broadband providers, and provide clear, flexible, and enforceable data security and data breach notification requirements. The FCC has previously defined BIAS as a mass-market retail service (by wire or wireless) that provides the capability to transmit data to and receive data from all or substantially all internet endpoints.

The FCC rules are modeled in part on the privacy and data security work done by the FTC. The framework focuses on transparency, choice and data security, and provides heightened protection for sensitive customer information. The rules are designed to protect consumer choice while giving broadband providers the flexibility they need to continue to innovate. The order was approved along party lines, with the three Democrats voting in support and the two Republicans opposing.

In particular, the rules define the information protected under Section 222 of the Communications Act as customer proprietary information ("PI"), which includes three types of information collected by telecommunications carriers: (i) individually identifiable Customer Proprietary Network Information (CPNI) as defined in Section 222(h); (ii) personally identifiable information (PII) and (iii) content of communications.

The FCC also adopted a multi-part approach to determining whether data has been properly de-identified and is therefore not subject to the customer choice regime adopted for customer PI. Specifically, the FCC found that customer proprietary information is de-identified if the carrier (1) determines that the information is not reasonably linkable to an individual or device; (2) publicly commits to maintain and use the data in a non-individually identifiable fashion and to not attempt to re-identify the data; and (3) contractually prohibits any entity to which it discloses or permits access to the de-identified data from attempting to re-identify the data.

Transparency. The rules require carriers to provide privacy notices that clearly and accurately inform customers about what confidential information the carriers collect, how they use it, under what circumstances they share it and the categories of entities with which they will share it. Carriers must also inform their customers about the right to opt in to or opt out of the use or sharing of their confidential information. Carriers must present their privacy notice to customers at the point of sale, and make their privacy policies available and easily accessible on their websites and applications. Carriers must also give their customers advance notice of material changes to their privacy policies.

Choice. The new rules provide customers with the ability to choose how their service providers may use and share their data, providing heightened protection for sensitive information, including financial information, health information, Social Security numbers, precise geo-location information, information pertaining to children, content of communications, web browsing history, application usage history and the functional equivalents of web browsing history or application usage history. For voice services, call detail information is also considered sensitive information. The FCC adopted three categories of approval for the use of customer PI obtained by providing the telecommunications service:

- ***Opt-in Approval***. Carriers must obtain customers' opt-in approval for use and sharing of sensitive customer PI (and for material retroactive changes to carriers' privacy policies). Opt-in approval requires that the carrier obtain affirmative, express consent allowing the requested usage, disclosure, or access to the customer proprietary information after the customer is provided appropriate notification of the carrier's request.

- ***Opt-out Approval.*** Carriers must obtain customers' opt-out approval for the use and sharing of non-sensitive customer PI. Under opt-out approval, a customer is deemed to have consented to the use, disclosure, or access to the customer's proprietary information if the customer has failed to object after the customer is provided appropriate notification of the carrier's request for consent.

- ***Exceptions to Customer Approval Requirements***. The rules allow telecommunications carriers to use and share customer data in order to provide the customer's chosen services. These uses would include billing for the services; protecting the carrier and its other customers from unlawful use of the services (including unlawful robocalls), research to improve and protect networks and services and providing customer location and non-sensitive PI in certain emergency situations (such as 911 calls).

To the extent carriers collect and maintain customer PI, the FCC requires that they take reasonable measures to secure it, including the adoption of security practices appropriate to the nature and scope of its activities, the sensitivity of the underlying data, the size of the provider and technical feasibility. The FCC declined to mandate specific activities that carriers must undertake in order to meet the reasonable data security requirement.

The FCC also adopted data breach notification requirements to ensure that affected customers and the appropriate federal agencies receive notice of data breaches, unless the carrier is able to reasonably determine that a data breach poses no reasonable risk of harm to the affected customers. For breaches affecting 5,000 or more customers, notice must be provided to the FCC, the FBI, and Secret Service within seven business days of when a carrier reasonably determines that a breach has occurred; and must be provided to the applicable federal agencies at least three days before notice to customers. For breaches affecting less than 5,000 customers, carriers must notify the FCC without unreasonable delay and no later than 30 days following the carrier's reasonable determination that a breach has occurred. In order to allow carriers more time to determine the specifics of a data breach, carriers must provide notice to affected customers without unreasonable delay, but within no more than 30 days. There are also new recordkeeping requirements for carriers that experience a breach; these records shall be retained for a minimum of two years from the date the carrier determines a reportable breach has occurred.

In the order, the FCC prohibits service offerings that require customer to surrender privacy rights and adopts rules requiring disclosure and consent for BIAS providers' offering of financial incentives, such as lower rates, in exchange for the right to use customers' confidential information. BIAS providers also must make available a simple mechanism for customers to withdraw such consent. The FCC noted that aggrieved consumers can use the FCC's existing dispute resolution procedures.

The FCC did recognize that business customers of telecommunications services (other than broadband services) have the ability to protect their information through contracts with service providers. Thus, carriers serving enterprise customers do not need to comply with the privacy and data security rules if the carrier's contract with that customer specifically addresses the issues of transparency, choice, data security, and data breach and provides a mechanism for the customer to communicate with the carrier about privacy and data security concerns. These telecommunications carrier do remain subject to the privacy requirements of Section 222 of the Communications Act.

The order recognizes that states have also adopted privacy, data security and data breach laws. The FCC stated its intention to pre-empt those state laws only to the extent that they are inconsistent with FCC rules.

The order provides a timeline for orderly transition to the new rules with additional time given for small carriers in case they need to change their practices. Until the rules become effective, Section 222 will apply to all telecommunications services, including BIAS, and the rules implementing Section 222 will continue to apply to telecommunications and VoIP providers (other than BIAS providers). Some of the rules will require separate approval from the Office of Management and Budget subject to the Paperwork Reduction Act ("PRA").

***Notice and Choice*.** The notice and choice rules will become effective the later of (1) PRA approval, or (2) 12 months after the FCC publishes a summary of the order in the Federal Register.

***Breach Notification Procedures*.** The data breach notification rule will become effective the later of (1) PRA approval, or (2) six months after publication of a summary of the order in the Federal Register.

Data Security. The specific data security requirements will become effective 90 days after publication of a summary of the order in the Federal Register.

Prohibition on Conditioning Broadband Service on Giving up Privacy. The prohibition on conditioning offers to provide BIAS on a customer's agreement to waive privacy rights will become effective 30 days

after publication of a summary of this order in the Federal Register. All other privacy rules adopted in the order will be effective 30 days after publication.

Treatment of Customer Consent Obtained Prior to the Effective and Implementation Date of New Rule. In order to minimize disruption to carriers' business practices, the FCC does not require carriers to obtain new consent from all their customers. It will "grandfather" any consumer consent that was obtained prior to the effective date of the rules that is consistent with the new requirements. However, if the customer consent was not obtained in the manner outlined in the new rules, a new opportunity for choice is required. Customer consent obtained by providers of other telecommunications services subject to the legacy rules remains valid for the time during which it would have remained valid under the legacy rules.

The FCC provided small carriers.an additional 12 months to implement the notice and customer approval rules. The FCC defined small BIAS providers as providers with 100,000 or fewer broadband connections and small voice providers with 100,000 or fewer subscriber lines as reported on their most recent Form 477, aggregated over all the providers' affiliates.

The FCC declined to extend the privacy rules to edge providers (such as Twitter or Netflix), stating that those providers only see a slice of any given consumers internet traffic. The FCC reasoned that users also have more control over tracking by web third parties; suggesting that there are a range of browser extensions that are largely effective at blocking third parties' access to information. There is also some question whether the FCC would have jurisdiction to impose privacy obligations on edge providers.

If you have any questions about the content of this alert, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

If you have any questions about the content of this alert, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Glenn S. Richards (bio)
Washington, DC
+1.202.663.8215
glenn.richards@pillsburylaw.com

Deborah S. Thoren-Peden (bio)
Los Angeles
+1.213.488.7320
deborah.thorenpeden@pillsburylaw.com