DORSEY
DORSEY+WHITNEY LLP

BIAS Rules: New FCC Regulations on Broadband Customer Privacy

November 16, 2016 – The TMCA
by Erica Larson and Robert E. Cattanach

On October 27, 2016, the Federal Communications Commission ("FCC" or "Commission") adopted sweeping new privacy rules applicable to all telecommunications providers including broadband internet access service ("BIAS") and interconnected voice-over-internet-protocol ("VoIP") providers. *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*. These rules place limits on how providers can use and share customer data, regulate providers' privacy policies, require telecommunications providers to take "reasonable" steps to prevent data breaches, and establish new data breach notification requirements. Some of the rule's new requirements become effective as soon as 30 days after publication in the Federal Register, others may not become effective for a year or more. It is unclear how the change in administrations might affect the timing and/or the implementation of these rules.

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

Use and Sharing of Customer Data

The customer information covered by the new rules includes (1) customer proprietary network information ("CPNI"), (2) personally identifiable information ("PII"), and (3) the content of communications, all of which the Commission calls, collectively, customer proprietary information ("PI"). The Commission also clarified that PI is "information that BIAS providers and other telecommunications carriers acquire in connection with their provision of service."

CPNI is a statutory term, defined in 47 U.S.C. § 222(h)(1), and has a more-or-less well understood application in the traditional telephone context. However, its application to BIAS providers was and still is somewhat unclear. The Commission declined to set out a comprehensive list of data elements that do or do not satisfy the statutory definition of CPNI in the broadband context, but did provide a short list of examples of broadband CPNI: Broadband Service Plans; Geo-location; MAC addresses and other device identifiers; IP addresses and domain name information; traffic statistics; port information; application headers; application usage data; application payload and customer premises

equipment; and device information.

PII is defined as “information that is linked or reasonably linkable to an individual or device.”

The Commission’s new rules require providers to obtain affirmative customer consent prior to using so-called sensitive customer PI, which includes, “at a minimum,” financial information; health information; Social Security numbers; precise geo-location information; information pertaining to children; content of communications; call detail information; and a customer’s web browsing history, application usage history and their functional equivalents. In addition, providers must provide mechanisms to allow customers to opt-out of the use or sharing of non-sensitive PI. The Commission recognizes certain exceptions to this opt-in, opt-out regime, such as the use of customer information in order to provide the telecommunications service from which the information is derived. Customer consents obtained by BIAS providers prior to issuance of these rules are “grandfather[ed]” only if they are consistent with the requirements of the new rules.

Privacy Policies

The new FCC rules require that telecommunications carriers must maintain privacy policies describing the types of customer PI that the provider collects and how the provider uses that information; under what circumstances the provider shares PI that it collects; and how a customer can make opt-in and opt-out decisions related to his or her privacy. The privacy policy must be presented to a customer at the point when they initially sign up for service, and must be made available on a continuing basis on the provider’s website.

Steps to Prevent Data Breaches

The FCC rules require that telecommunications providers take “reasonable measures to protect customer PI from unauthorized use, disclosure or access.” The Commission chose not to prescribe specific practices that a provider must undertake to comply with the new data security rules, but did list a series of practices that it considers to exemplify reasonable data security measures, such as robust customer authentication. The FCC cautioned, however, that the practices it listed were neither mandatory to comply with the rule nor a safe-harbor for compliance.

Data Breach Notification Requirements

The rule establishes new notification requirements for telecommunications providers in the event of a data breach. Specifically, unless a provider can reasonably determine that no harm to customers is reasonably likely to occur, it must notify the Commission of any data breach. If the breach affects 5,000 or more customers, the provider must also notify the Secret Service and FBI. For data breaches effecting more than 5,000 customers, notification to the Commission, FBI and Secret Service must occur within seven days of the breach and at least three days prior to any customer notification. The term “breach” is

defined by the new rules as “any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information [PI].” The FCC promises to develop a centralized portal for reporting breaches to the FCC and other federal law enforcement agencies.

Notification to customers must be made “without unreasonable delay and no later than 30 calendar days following the carriers’ reasonable determination that a breach has occurred, unless the FBI or Secret Service requests a further delay.” In addition, the Commission’s rule requires customer notifications to include certain information such as the date of the breach, a description of the customer PI that was disclosed, customer service contact information, information about how to contact the FCC and any relevant state regulatory agencies, and, if there is any risk of financial harm, information about the national-credit reporting agencies and steps customers can take to protect themselves from financial harm. These data breach regulations, and all the regulations announced in the new rule, pre-empt state laws only to the extent they are inconsistent with the rules adopted by the Commission.