1. Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, Report and Order, FCC 16-148 (27 Oct 2016).
2. Protecting and Promoting the Open Internet, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, FCC 15-24 (12 Mar 2015), petitions for review denied, U.S. Telecom Ass'n v. FCC, 825 F.3d 674 (D.C. Cir. 2016).
3. Ibid. at ¶ 462.
4. Ibid. at ¶ 488.
5. Ibid. at ¶ 497.
6. Ibid. at ¶ 509, 511.
7. Ibid. at ¶ 513.
8. https://morningconsult.com/2016/09/15/rosenworcel-nomination-caught-up-in-end-game-chess-match/
9. https://www.scientificamerican.com/article/trump-s-plans-to-shake-up-the-tech-world1/
10. The Administrative Procedure Act defines 'rule making' as an agency process 'for formulating, amending, or *repealing* a rule.' 5 U.S.C. § 551(5) (emphasis added).
11. President Obama created precedent for this approach when he directed the Justice Department to stop defending the Defense Against Marriage Act.

George Foote Partner and Head of Telecom Practice
foote.george@dorsey.com

Erica Larson Associate

Dorsey & Whitney LLP, Washington, DC and Minneapolis

The US FCC adopts new, expanded consumer privacy protection rules

The US Federal Communications Commission ('FCC' or 'Commission') adopted on 27 October 2016 new rules around privacy, applicable to telecommunications providers including broadband internet access service ('BIAS') and interconnected voice-over-internet-protocol ('VoIP') providers. The rules include *inter alia* notification requirements for data breaches and limits in regard to the sharing of customer data. George Foote and Erica Larson of Dorsey & Whitney LLP discuss these privacy rules as well as the potential impact of the change in US Government administration on such rules.

On 27 October 2016, the FCC adopted sweeping new privacy rules applicable to all telecommunications providers[1]. 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 rules' 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. The rules impose new duties on BIAS and VoIP service providers, but the scope of the rules and the sanctions for failing to comply remain vague. The fate of the new rules under the Trump administration is not clear.

Use and sharing of customer data

The FCC identified a broad new class of information it calls proprietary information or 'PI.' According to the Commission, PI is 'information that BIAS providers and other telecommunications carriers acquire in connection with their provision of service.' PI includes (1) customer proprietary network information ('CPNI'), (2) personally identifiable information ('PII'), and (3) the content of communications. CPNI is defined in 47 U.S.C. § 222(h)(1), and is well-understood in the traditional telephone context. However, its application to BIAS providers is unclear. The FCC declined to specify data elements that satisfy the statutory definition of CPNI in the broadband context, but did provide examples: broadband service plans; geolocation; media access control ('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 FCC's new rules require providers to obtain affirmative customer consent, referred to as opt-in, before using 'sensitive customer PI,' which includes, 'at a minimum,' financial information; health information; Social Security numbers; precise geolocation 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.

Providers must allow customers to opt-out of the use or sharing of non-sensitive PI. The FCC recognises certain exceptions to this opt-in, opt-out regime, such as using customer information to provide the telecommunications service from which the information is derived. Customer consents obtained by BIAS providers before issuance of these rules are invalid under the new rules unless the consents meet the standards of the new rules.

Privacy policies

The new rules require telecommunications carriers to 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. The privacy policy must be presented to a customer at the point when they initially sign up for the service, and must be available on the provider's website.

Steps to prevent data breaches

The FCC rules require telecommunications providers to take 'reasonable measures to protect customer PI from unauthorized use, disclosure or access.' The FCC chose

not to prescribe specific practices that a provider must undertake to comply with the new data security rules, but listed practices 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 if a data breach occurs. 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, customer notifications must include 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.

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 affecting 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 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 committed to develop a centralised portal for reporting breaches to the FCC and other federal law enforcement agencies. These data breach regulations, and all the regulations announced in the new rule, pre-empt state laws to the extent state law is inconsistent with the FCC rules.

The statutory basis for the rules implies more to come

Two themes run through the FCC's description of its legal basis for the new rule. Both are embedded in the Commission's statement that it is "implement[ing] Congress's mandate to ensure that telecommunications carriers protect the confidentiality of proprietary information of and relating to customers." The first theme is old: since 1934, Section 222 of the Communications Act has imposed a duty on carriers to protect the confidentiality of certain customer information. The second theme is new: as a consequence of the 2015 Open Internet Order, BIAS providers are now considered telecommunications service providers subject to Title II of the Communications Act[2]. Thus, the FCC concludes that the new privacy rules are a natural consequence of the 2015 Open Internet Order's reclassification of BIAS providers.

In the Open Internet Order, the FCC forbore from applying many Title II provisions to broadband providers, including the previously existing rules promulgated by the Commission under its Section 222 authority[3]. The Commission's view of its legal authority for the new privacy rules implies that these rules may be the first of several possible rulemakings interpreting long-standing statutory authority in light of the reclassification of broadband services. Other key provisions which the FCC chose not to apply to BIAS providers at the time of the 2015 Open Internet Order include Section 254(d)'s universal service contribution requirement[4]; the tariffing provisions of Sections 203 and 204[5]; the discontinuance, transfer of control, and network reliability approval obligations of Section 214[6]; and the interconnection and market-opening provisions of Sections 251, 252 and 256[7].

Administration change

It is unclear how the change in administration will affect the new rules. The term of Democratic Commissioner Jessica Rosenworcel expires in 2017, and unless she is re-confirmed by Congress during the lame duck session, President Trump may appoint a Republican commissioner to replace her[8]. Some have predicted that the Trump administration will prioritise a repeal of the privacy rules[9]. But, because the new rules have already been adopted by the FCC, an administrative repeal of the rule by a new Commission would be delayed for at least several months by the notice-and-comment procedures required by the Administrative Procedure Act[10]. A messier, but potentially faster route for undermining the new rules would be to turn to the court system. President Trump could effectively repeal the rules by refusing to defend legal challenges to them[11]. A third option would be for a newly-Republican Commission to leave the new rules on the books, but not enforce them. Such an approach might be easiest to implement, but would leave in place the groundwork for potential enforcement by future Commissions.