THE
NATIONAL LAW REVIEW

They Can Be Heroes: The FCC Proposes Expansive and Detailed Privacy & Cybersecurity Regulations for Broadband ISP

SheppardMullin

Article By
Dave Thomas
J. Aaron George
Ashley L. Yeager
Sheppard, Mullin, Richter & Hampton LLP
FCC Law Blog

- Communications, Media & Internet
- All Federal

Friday, April 8, 2016

On April 1, 2016, the FCC released a Notice of Proposed Rulemaking ("NPRM") that would impose new regulatory burdens on broadband Internet service providers' use of customer data. The wide-ranging NPRM also proposes rules covering providers' protection of customer information and their actions in the event of a data security breach.

Comments are due on **May 27, 2016**, with **Reply Comments** due on **June 27, 2016**.

While we have done our best to balance brevity with detail, we hope that this longer-than-usual summary proves useful in understanding both the specifics of the FCC's proposal and the contours of this important debate.

Espousing the overarching concepts of ***transparency, choice and security***, the FCC proposed a 45-page slate of new regulations addressing both privacy and related practices, and information and cybersecurity practices.

The new rule proposals follow the FCC's reclassification of broadband Internet access service providers ("BIAS providers") as communications common carriers in

its April 2015 *Open Internet Order*. The FCC stated in the *Open Internet Order* that, like other providers of telecommunications services, BIAS providers are governed by the privacy requirements in Section 222 of the Communications Act. *See 2015 Open Internet Order*, 30 FCC Rcd 5601, 5820-23 ¶¶ 462-67. Continuing down that path, the FCC now proposes broadband-specific privacy regulations under that section. Potentially complicating both record development and eventual implementation of the proposed rules, the FCC released the NPRM prior to the release of the D.C. Circuit's decision addressing the legality of the 2015 *Open Internet Order*.

The proposals, if adopted, would require fundamental changes to many ISPs' (both fixed and mobile) handling, storage and use of customer information, as well as their marketing practices, privacy policies, data-protection standards, systems and protocols and breach-notification requirements.

ISPs Are Covered, But Not Edge Providers

The proposed rules would apply only to BIAS providers, not to websites or other consumer-facing "edge services," including social media sites like Facebook and Twitter that collect vast amounts of consumer data. The FCC reasoned that regulation in this area is necessary because BIAS providers have access to a broader range of consumer information than edge providers and are less easily avoided by consumers who are unhappy with the provider's privacy protections.

The FCC Proposes a Dramatic Expansion of Protected Customer Information

The proposed rules would expand and fundamentally redefine the customer information subject to FCC regulation. The rules would cover customer proprietary network information ("CPNI"), the only category of information covered today, consisting of data that service providers possess regarding individual customers' usage of broadband services, service-plan information, data about the devices they use, and source and destination IP addresses and domain names. But they would expand dramatically from CPNI to customers' personally identifiable information ("PII"), defined in the Notice as any information that is "linked or linkable" to individual customers, such as their Social Security numbers and financial account information, and the content of customer communications (*e.g.,* the text of their emails). Covered or protected information also would include information collected or stored on customer premises equipment, such as cable set-top boxes (information that has been protected since passage of the 1984 Cable Act). The FCC speculates that, with the advent of the Internet of Things, the definition of CPNI could extend to information collected by Internet-enabled devices in the home, like a smart thermostat.

Specific Rules Regarding Use of Customer Information

Under the proposed rules, potential uses of customer information would be divided into three categories:

- uses to which information may be put based on the customer's implied consent, inferred from its decision to do business with the BIAS provider;

- uses to which information may be put unless the customer opts out; and
- uses which require the provider to obtain express customer consent before sharing or using his or her data.

Under the implied consent category, BIAS providers could use customer data as necessary to provide broadband services to customers and to bill and collect for the services purchased. Providers also could use customer information without consent (or with implied consent) to market to existing customers any additional service offerings in the same category of service (fixed or mobile) that the customer already receives. The FCC Bureau Chief responsible for the item recently stated that, for example, an ILEC ISP (such as Verizon, AT&T, or CenturyLink) could market a fiber-to-the-home product to a DSL customer without obtaining consent to use his or her personal information. The rules would allow BIAS providers to use customer information in a few additional, but very limited, circumstances – for instance, to protect other users from fraudulent or abusive telemarketing by a BIAS subscriber or to protect the BIAS provider itself from cybersecurity threats.

The proposed rules would require that BIAS providers give customers the ability to opt out of any use of their information to market other "communications-related services." Specifically, the rules would require providers to notify customers about potential marketing-related uses of their information and give them an opportunity to opt out. The rules would eliminate the 30-day "window" granted to voice providers under their Section 222 rules, and instead make a customer's opt-out decision effective immediately. The FCC also seeks recommendations on how to limit the definition of "communications-related services" to make the "opt-out" category as narrow as possible.

The proposed rules would prohibit any other use of customer data unless the customer *affirmatively opted in and agreed* to share personal information for that purpose. The rules would require BIAS providers to notify customers and seek permission before their first intended use or sharing of customer information for a non-communications marketing purpose, and provide a "convenient and persistent" way for customers to continue to weigh in on their privacy preferences (*e.g.,* through an online dashboard or user interface on the provider's website).

To aid customers in making these opt-in and opt-out decisions, the proposed rules would require BIAS providers to notify their customers, both at the point of sale and on an ongoing basis, about their collection and use of customer information, their privacy practices, and customers' rights to opt in or out of various uses of their information. No single form is suggested for those notifications, but the FCC suggests that a standardized disclosure format might provide a safe harbor for BIAS providers in the event that they are accused of inadequate privacy-policy disclosures.

Finally, the proposed rules would require BIAS providers to protect the information of applicants and former customers as well as current customers. The FCC seeks comment on whether more stringent restrictions are necessary for certain types of especially sensitive customer information, such as Social Security numbers, and whether the rules should also protect aggregated or de-identified information that may be re-identifiable and traceable to an individual.

Rules on Data Security and Breach Notification

The proposed rules would impose data security requirements on ISPs, loosely based on the NIST (National Institute of Standards and Technology) standards and the practices of other federal agencies (many of these have appeared in FCC consent degrees, as well as decisions from the FTC and other agencies). The rules would require ISPs to adopt system-compliance and risk-management practices, train their personnel in data privacy protection, appoint a manager responsible for data security, and adopt customer authentication requirements to restrict access to customers' personal information (if those measures are not already in place).

While the FCC does not propose technical standards for BIAS providers to fulfill on each of these fronts, it seeks suggestions for best practices and ways to measure provider compliance. For example, the FCC highlights multi-factor authentication – including both a password and some other form of credential, like an access key – as a means of protecting access to customer information. The FCC notes the difficulties inherent in such stringent requirements, yet still seeks comment on whether and in what scenarios multi-factor authentication is necessary and practicable. The FCC also seeks comment on other methods of protecting customer data, such as encryption requirements or rules that would minimize the collection of sensitive customer data in the first place or allow responsible disposal of information after a set period of time.

With respect to breach notification, the proposed rules would place stringent requirements on ISPs for contacting customers, the FCC, and law enforcement when a security breach occurs. The rules would require the BIAS provider to notify customers within 10 days of discovering the breach, the FCC within 7 days of discovery, and the FBI and Secret Service within 7 days if more than 5,000 customers are affected. The FCC expresses its willingness to consider other notification standards, including a flexible standard such as notifying customers "as expeditiously as possible" or "without unreasonable delay." If the BIAS provider shared customer information with third-party affiliates for advertising purposes, the proposed rules would make the collecting provider responsible for the customer information even after it is in the third party's hands, and would make the provider vicariously liable in the event of a breach. The FCC also contemplates requiring BIAS providers who have shared protected information with a third party to notify customers in the event that the third party is breached.

The definition of a "breach" under the proposed rules would not include an element of intent. This broad definition would increase the number of FCC and customer-notification events. The FCC also seeks comment on whether providers should have to provide notice if they discover conduct that could reasonably be tied to a breach, even if they are not certain that a breach has occurred.

Other Miscellaneous Rules

Finally, the proposed rules would outlaw certain BIAS-provider practices that might be regarded as disadvantaging customers – as opposed to compensating them for the use of their personal information. Prohibited practices might include making broadband services contingent on the waiver of privacy rights, or offering

differently-priced tiers of service with different levels of privacy protection. The FCC even contemplates prohibiting provisions in service contracts to compel arbitration.

The Debate

Commenters in this proceeding likely will agree that the growing threats to personal privacy, and to information and cybersecurity, pose serious challenges to individuals, business, democratic institutions and civil society. The debate will focus, instead, on whether the FCC's proposal is that agency's hasty, misbegotten contribution to a regulatory "arms race," or whether it can provide the appropriate structure, incentives, and flexibility to address real concerns and real threats in an effective, sustaining way.

Privacy and consumer advocates likely will argue that the FCC's proposal is no different from other sector-specific privacy and data-security regulations developing in the financial services, education, healthcare and consumer products and services sectors, and that more structure and ISP accountability is needed.

ISPs will have a different view. They will tend to see the FCC's very detailed regulations – requiring in many cases the reversal of long-established marketing and other business practices, coupled with increasingly rigorous enforcement practices – as highly intrusive, paternalistic, unnecessary, and unlawful. ISPs will argue that the rules would create a steep competitive imbalance between ISPs and edge providers – and that while edge providers are freely amassing, harvesting, packaging and brokering in this data, ISPs will be severely constrained in their ability to use *the* essential element in the exploding information economy – customer data.

ISPs likely will argue that their window into customers' activities is small – and, with increased encryption, shrinking. They will argue that the FCC greatly overstates the scope of ISPs' data collection in order to achieve a pre-determined policy objective. They may also argue that resources will be diverted away from anticipating and addressing real customer and marketplace needs (such as privacy and data security and development of better products) in order to fulfill ever-shifting, yet potentially rigid notions of privacy compliance.

ISPs may also argue that, far from achieving the sort of peace of mind that the FCC hopes will sharpen consumers' hunger for broadband capacity and functionality and spawn broadband deployment and adoption, the heavy hand of Government regulation instead will stifle innovation, leading to inferior products, services and online experiences.