

FCC Proposes Sweeping Broadband Privacy Rules

Broadband Internet access service providers would face a new, top-to-bottom consumer privacy regime.

Twelve months after the US Federal Communications Commission (FCC) imposed common-carrier telecommunications rules on broadband providers in the agency's landmark Open Internet proceeding,¹ the FCC has now proposed customer privacy and data breach rules for broadband.² The new comprehensive privacy regime the FCC has proposed (which will be finalized after the FCC receives public comment) is intended to implement the core privacy principles of transparency, choice and security. The regime would impose, for the first time, broadband-specific privacy requirements pursuant to Section 222 of the Communications Act (the Act) on all broadband Internet access service providers (broadband providers), which the FCC calls "the most important and extensive conduits of consumer information."³

Who and what would be regulated?

The FCC's proposed rules are focused almost entirely on broadband providers, and would not apply to providers of "edge services" (everything from websites, web-based email and streaming services, to mobile applications and search engines). In the FCC's view, broadband providers, because of their unique role as gateways to the Internet, have a singular ability to track their subscribers' activities across the full breadth of the Internet. The broadband provider's role as gatekeeper, the FCC states, is unavoidable from the consumer perspective, and thus differentiates broadband providers from edge providers.⁴ Notwithstanding the focus on broadband, other network operators likely will face new or different regulation of their privacy practices. In particular, where the FCC proposes broadband privacy rules that would differ from existing requirements applicable to legacy telecommunications carriers, VoIP providers, cable operators and/or satellite providers, the FCC in many cases seeks comment on whether the agency should harmonize the privacy rules across all service types (often by proposing to apply the proposed broadband rule to other services).

The proposed rules would govern two categories of information: "customer proprietary network information" (CPNI) and "personally identifiable information" (PII). CPNI generally equates to a customer's technical usage or billing data, which in the broadband context would encompass information such as Internet service plan and pricing, geo-location data, MAC address(es) and Device ID(s), IP addresses and traffic statistics.⁵ PII (which is not defined in the Act) would be defined broadly to include all "linked and linkable" information about an individual, ranging from name, Social Security number and date of birth, to browsing history, shopping records, education and employment information, and medical records, among other data.⁶ CPNI and PII together comprise a broader category of information: "customer proprietary information" (customer PI). Customer PI also would be defined broadly to include "private information that customers have an interest in protecting from public exposure."⁷ Under the proposed

rules, broadband providers would be required to implement measures to protect information that qualifies as customer PI for current and former customers, whether paying or non-paying, as well as any applicant for service.⁸

The FCC's proposed privacy framework for broadband

Proposed rules governing use and sharing of customer PI

The proposed rules would place strict controls on how broadband providers may collect, use, share and protect customer PI. At the point of collection, broadband providers would have to meet new standards for transparency and customer choice. Once customer PI is collected, the rules would govern how broadband providers may use and must secure the information.

Transparency is at the forefront of the FCC's proposed rules. Broadband providers would be required to provide customers with "clear and conspicuous notice" of the providers' privacy practices, both at the point of sale and through a persistent link on the providers' homepage and/or mobile application.⁹ While most broadband providers are already subject to state laws that require similar practices, the proposed rules would include particular requirements on the format, location and language of broadband providers' privacy policies. Although the FCC does not anticipate treating fixed and mobile broadband providers differently, the agency seeks comment on whether mobile-specific considerations warrant such treatment.¹⁰

Once a broadband provider collects customer PI, the new rules would require that customers be given a choice for whether and how certain information may be used. As in the context of telephone service, the proposed rules would not require customer choice if a customer's consent is implied or unnecessary (such as information sharing necessary to: provide or bill for service; market similar broadband service offerings; facilitate emergency response; or protect the broadband provider's property rights).¹¹ The proposed rules would also allow using customer PI for related services that would directly benefit customers, such as to prevent certain robocalls or protect against cyber threats.¹²

Beyond these limited situations, a broadband provider's ability to use or share customer PI would be curtailed, with the provider required either to allow a customer to opt out of certain information use/sharing, or to secure affirmative opt-in approval from a customer before information use/sharing may occur. In the former instance, broadband providers would be required to allow customers to opt out of receiving marketing for other communications-related services offered by the broadband provider or its affiliates.¹³ Under the proposed rules, all other forms of information sharing/use would be prohibited absent express customer opt-in approval.¹⁴ In addition, the timing and format of opt-out and opt-in requests would be subject to agency regulation.¹⁵ The FCC proposes more relaxed rules for using and sharing aggregate customer information, allowing broadband providers to use and share de-identified information so long as such information cannot be re-identified. Parties sharing aggregate data would be subject to requirements prohibiting the re-identification of individual-level data (including by third parties).¹⁶

The FCC explores, but stops short of specifically proposing, several other even more robust customer privacy protections. For example, the FCC asks whether certain highly sensitive information, such as Social Security numbers, children's information, location data and health information, should always be subject to opt-in approval before the information use/sharing may occur.¹⁷ The proposed rules would also prohibit offering broadband services contingent on the customer's waiver of their privacy rights,¹⁸ and the FCC seeks comment on whether broadband providers should be able to offer discounted rates or other financial incentives to customers who consent to broader use or sharing of their customer PI.¹⁹ The FCC also seeks comment on whether to prohibit other practices that may impact customer PI, such as the use

of deep packet inspection (for purposes other than managing the network), and using persistent identifiers to track broadband users or their devices.²⁰

Proposed rules governing security of customer PI

The FCC's proposed rules include rules governing how broadband providers must secure and protect the customer PI they collect, including a broad general obligation for broadband providers to "protect the security, confidentiality, and integrity of customer PI" from all unauthorized use or disclosure by "adopting security practices appropriately calibrated to the nature and scope of the [its] activities."²¹ Under that standard, most (if not all) data breaches could be found to violate this regulatory duty, as breaches invariably involve a system, process or person that was improperly "calibrated." The proposed rules also would require all broadband providers to: conduct regular risk management assessments; provide data security training to employees, contractors and affiliates; designate a member of senior management to be responsible for data security; establish customer authentication procedures; and accept vicarious liability for improper use of customer PI by third parties with whom the broadband provider shares information.²² The FCC also seeks comment on a number of other specific data security practices, including record retention and disposal practices.²³

Proposed requirements triggered in the event of a data breach

The FCC's proposed rules would set new requirements for notifying the FCC, customers and law enforcement in the event of a data breach. The rules would require broadband providers to notify the FCC within seven days of discovering a breach, regardless of the number of individuals impacted, and to notify customers within 10 days of discovering the breach.²⁴ While the proposed rules define a breach as when a person "without authorization or exceeding authorization, has gained access to, used, or disclosed customer PI,"²⁵ the rules do not specifically provide a safe harbor for data that is properly encrypted, leaving the definition of "access" unclear. When a breach impacts more than 5,000 customers, the broadband provider would be required to notify the Federal Bureau of Investigation and the US Secret Service, at least three days before notifying customers.²⁶ The FCC seeks comment on whether additional data security incidents should also be reported to federal or state law enforcement, and how notification should occur in the event of a third party breach involving customer PI a broadband provider has provided.²⁷

Public comments on the FCC's proposals are due on May 27, with reply comments due on June 27. If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

[Matthew A. Brill](#)
matthew.brill@lw.com
+1.202.637.1095
Washington, D.C.

[Amanda E. Potter](#)
amanda.potter@lw.com
+1.202.637.2192
Washington, D.C.

[Alexander L. Stout](#)
alexander.stout@lw.com
+1.202.637.2158
Washington, D.C.

[Jennifer C. Archie](#)
jennifer.archie@lw.com
+1.202.637.2205
Washington, D.C.

You Might Also Be Interested In

[Privacy Blog: FCC Proposes Broad Privacy Regulations for Broadband Providers](#)

[Technology, Media and Telecommunications Review – US](#)

[EU Court of Justice Invalidates US Safe Harbor Decision](#)

[Privacy Blog: FCC Imposes Record Penalty for Data Breach](#)

[FCC Issues Controversial TCPA Declaratory Ruling](#)

Client Alert is published by Latham & Watkins as a news reporting service to clients and other friends. The information contained in this publication should not be construed as legal advice. Should further analysis or explanation of the subject matter be required, please contact the lawyer with whom you normally consult. The invitation to contact is not a solicitation for legal work under the laws of any jurisdiction in which Latham lawyers are not authorized to practice. A complete list of Latham's *Client Alerts* can be found at www.lw.com. If you wish to update your contact details or customize the information you receive from Latham & Watkins, visit <http://events.lw.com/reaction/subscriptionpage.html> to subscribe to the firm's global client mailings program.

Endnotes

-
- ¹ See, generally, *Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (2015).
 - ² See, generally, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Notice of Proposed Rulemaking, FCC 16-39 (rel. Apr. 1, 2016) (NPRM).
 - ³ *Id.* at ¶ 2.
 - ⁴ *Id.* at ¶ 4.
 - ⁵ NPRM ¶¶ 38, 41.
 - ⁶ NPRM ¶ 62.
 - ⁷ *Id.* at ¶ 57.
 - ⁸ *Id.* at ¶¶ 31-37.
 - ⁹ *Id.* at ¶ 82.
 - ¹⁰ *Id.* at ¶¶ 102-03.
 - ¹¹ *Id.* at ¶¶ 113-15.
 - ¹² *Id.* at ¶¶ 118-21.
 - ¹³ *Id.* at ¶ 122.
 - ¹⁴ *Id.* at ¶ 127.
 - ¹⁵ *Id.* at ¶¶ 143-44.
 - ¹⁶ *Id.* at ¶¶ 74, 154.
 - ¹⁷ *Id.* at ¶¶ 134, 136-37.
 - ¹⁸ *Id.* at ¶ 256.
 - ¹⁹ *Id.* at ¶¶ 259-62.
 - ²⁰ *Id.* at ¶¶ 264-67, 268-70.
 - ²¹ *Id.* at ¶ 170.
 - ²² *Id.* at ¶ 174.
 - ²³ *Id.* at ¶¶ 215-16, 222-32.
 - ²⁴ *Id.* at ¶ 234.
 - ²⁵ *Id.* at ¶¶ 75-77.
 - ²⁶ *Id.*
 - ²⁷ *Id.* at ¶¶ 247, 250, 255.