PAUL HASTINGS

STAY CURRENT

November 2016

Follow @Paul_Hastings

FCC Releases Order Imposing New Privacy Rules on ISPs and Telcos

By Sherrese M. Smith & Andrew J. Erber

On November 2, 2016, the Federal Communications Commission ("FCC" or "Commission") released the text of a Report and Order (the "Order") which adopts sweeping new privacy and data security rules for ISPs and other telecommunications service providers.[1] The Order comes just seven months after the Commission released a Notice of Proposed Rulemaking (the "NPRM") on the topic[2]—breakneck speed for an agency whose proceedings are more often measured in years (and sometimes decades).

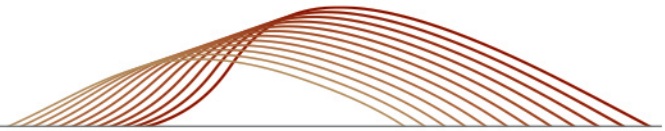
Approved last Thursday in a 3-2 party-line vote, the Order spans 203 pages and establishes a comprehensive set of rules which regulate how telecommunications carriers collect, use, and protect their customers' personal information. The FCC's new privacy framework adopts a sensitivity-based approach for obtaining consumer consent that requires opt-in consent for the use and sharing of sensitive information (such as Social Security Numbers and health information), while allowing an opt-out approach for most other non-sensitive information. Adequate notice, reasonable data security practices, and prompt data breach notification are also required under the new rules, together with prohibitions on "take-it-or-leave-it" offers and heightened disclosure standards for "pay-for-privacy" plans.

The NPRM's original aim was to apply the requirements of Section 222 of the Communications Act (the "Act") to broadband Internet access service in the wake of its classification as a Title II telecommunications service last year. While the new privacy rules will indeed apply to broadband, they will also apply to legacy voice services which are currently governed by the Commission's existing rules on customer proprietary network information ("CPNI"). Once effective, the new rules will replace these legacy CPNI rules so that one privacy framework applies to all telecommunications carriers. Some legacy requirements—such as the annual compliance certification and biennial delivery of privacy policies to customers—will be eliminated in favor of the FCC's new approach to privacy.

We address all of these elements in summary below, but the Order contains much more detail on each topic. Without a doubt, this is the most comprehensive privacy framework adopted by the Commission to date. All telecommunications carriers should carefully consider how the new rules impact their collection, use, and security practices in the coming months.

Scope of the FCC's New Privacy Framework

The FCC cites transparency, choice, data security, and heightened protection for sensitive customer information as the guiding principles behind its new privacy framework. The rules implementing these



concepts can be broken out into four broad categories: meaningful and transparent notice, customer choice with respect to the use and sharing of their information, data security and breach notification, and rules pertaining to carrier practices the FCC finds particularly harmful.

Each of these new requirements apply to customer proprietary information ("customer PI"), a newly defined term which includes individually identifiable CPNI, personally identifiable information ("PII"), and the content of communications. A customer is broadly defined as any current or former subscriber to a telecommunications service, or an applicant for a telecommunications service.[3] As such, carriers should be aware that their duty to protect customer PI begins before service starts and continues after service is terminated.

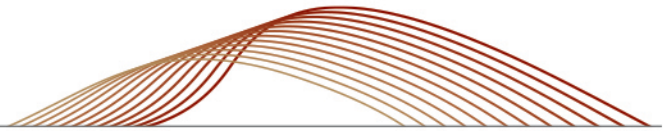
As defined in Section 222(h)(1) of the Communications Act, CPNI means customer information that relates to "the quantity, technical configuration, type, destination, location, and amount of use" of telecommunications services that is provided by a customer in the context of a carrier-customer relationship.[4] As in the past, the FCC has not provided a comprehensive list of CPNI, but in the broadband context suggests that CPNI includes:

- Broadband Service Plans
- Geo-location
- MAC Addresses and Other Device Identifiers
- IP Addresses and Domain Name Information
- Traffic Statistics
- Port Information
- Application Header
- Application Usage
- Application Payload, and
- Customer Premises Equipment and Device Information.[5]

Following the FTC's recommendation, the Order defines PII as "any information that is linked or reasonably linkable to an individual or device."[6] Communications content is also broadly defined as "any substance, purport, or meaning of a communication or any other part of a communication that is highly suggestive of the substance, purpose, or meaning of a communication."[7]

De-identified Information

Importantly, data that has been altered so as to be no longer associated with individual customers or devices do not constitute customer PI and so fall outside the scope of the rules.[8] To be considered de-identified for purposes of the FCC's rules, the Order requires that the data meet the FTC's three part de-identification test before use or sharing. Specifically, a carrier must: (a) alter the customer information so that it can't be reasonably linked to a specific individual or device; (b) publicly commit to maintain and use information in an unidentifiable format and not attempt to re-identify the data; and (c) contractually prohibit the re-identification of shared information.[9]



Transparency & Notice to Consumers

Beginning with the FCC's *2010 Open Internet Order*, the Commission has increasingly focused on transparency as a key consumer protection tool. The privacy framework continues this trend and adopts rules which require all telecommunications carriers to:

- Provide privacy notices that describe what customer information they collect, how that information is used, under what circumstances it is shared, and the types of entities it is shared with;
- Inform customers of their rights to opt in or opt out of use and sharing of their information;
- Present their privacy notice at the point of sale and later in a persistently available, easily accessible manner; and
- Give customers advance notice of material changes to the carrier's privacy policies.[10]

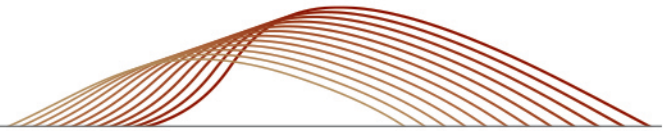
Additionally, the FCC will require carriers to provide "heightened disclosures" when they offer discounts or other incentives in exchange for a customer's express affirmative consent to the use and sharing of their personal information—offerings the Order calls "pay for privacy" plans.[11] To help companies comply with the notice rules, the FCC has tasked its Consumer Advisory Committee ("CAC") with developing a standardized privacy notice that will serve as a "safe harbor" for those providers who voluntarily choose to adopt it.[12]

Choice & Obtaining Customer Consent

Before an ISP can use or share customer PI under the rules, it must obtain that individual's consent. The Order establishes three consent mechanisms to accomplish this: opt-in, opt-out and "inferred" consent. Each consent mechanism applies to different types of customer PI, depending on the information's sensitivity and its treatment under the statute.

- **Opt-in:** Affirmative permission from the customer is required to use or share "sensitive" customer PI, which includes: precise geo-location, children's information, health information, financial information, social security numbers, web browsing history and app usage history (and their functional equivalents), and the content of communications. For voice providers, call history is also considered sensitive information. Opt-in consent is also required for retroactive changes to a carrier's privacy policies.[13]
- **Opt-out:** All other customer PI is considered non-sensitive and is subject to an opt-out.[14]
- **Inferred Consent:** Carriers may infer consent to use customer information to provide the underlying service, bill for that service, to prevent fraudulent use of the provider's network, and certain other purposes specified in the statute.[15]

At a minimum, a carrier must solicit customer opt-in or opt-out approval at the point of sale and when making one or more material changes to its privacy policy. The solicitation should reiterate the four notices required to be provided in the privacy policy, and must otherwise be comprehensible and not misleading. Once selected, a consumer's choice must be persistent until they choose to change their election, and such changes must be implemented "promptly."[16]



The most notable difference between the FCC's consent framework and the FTC's existing privacy and data security guidance is the Order's treatment of web browsing and app usage history. The FTC has never considered this information *per se* sensitive such that opt-in consent would be required for use or sharing. The FCC has adopted a different perspective. According to the Order, broadband ISPs are uniquely situated to comprehensively observe all of their customers' unencrypted browsing and app usage. Because of this unique ability to see all of a customer's unencrypted traffic, the FCC concluded that browsing and app usage history must be considered sensitive in the communications context and be subject to opt-in consent.[17]

Nevertheless, "edge providers" (such as search engines, social networks, and other apps) are not subject to the FCC's rules, and they will continue to operate under the FTC's existing guidance which does not require an opt-out for such information. Industry and dissenting Commissioners Pai and O'Rielly have been highly critical of this disparity, arguing that dissimilar consent mechanisms risk confusing consumers and creating a competitive imbalance.

Reasonable Data Security

The Order requires that ISPs adopt "reasonable" data security practices calibrated to the nature and scope of the ISP's activities.[18] The FCC specifically declined to adopt the particular security standards proposed in the NPRM on the grounds that security standards are highly dynamic and evolve based on the situational interplay between risk and cost.[19] The Commission was keen to point out multiple times that this standard is one of "reasonableness rather than strict liability."[20]

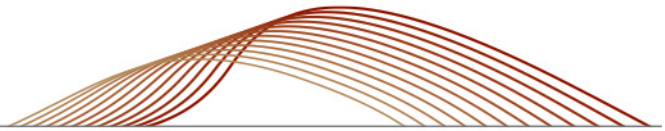
Though not a safe harbor, the Order does provide some guidance on what the Commission will consider when evaluating data security practices in the future. Specifically, the FCC recommends: implementing industry best practices and risk management tools, instituting internal accountability and oversight, implementing robust consumer authentication tools, and properly disposing of data consistent with FTC best practices and the Consumer Privacy Bill of Rights.[21] These measures include appointing a data security officer, conducting employee privacy and data security trainings, and entering into enforceable data security commitments from third parties as a condition of disclosure.[22]

Data Breach Notification

Should a security breach occur, the Order adopts rules requiring ISPs and other telecommunications carriers to notify customers, the FCC, the FBI, and the Secret Service of the breach. The rules define a breach broadly as "any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer PI."[23]

Following some state data breach notification laws, the Order adopts a "harm-based" notification trigger. Should a carrier determine that no harm to customers is reasonably likely to occur as a result of the breach, the rules require no notification.[24] Harm is not defined, but the Order suggests that the term covers not only identity theft and financial loss, but also "reputational damage, personal embarrassment, or loss of control over the exposure of intimate personal details."[25] When a breach involves sensitive customer PI, there is a rebuttable presumption that customer harm is reasonably likely.[26]

Carries must notify customers and the FCC within 30 days of the determination of a reportable breach, with certain prescribed information included in the notification.[27] For breaches affecting 5,000 or more customers, the carrier must notify the FCC, FBI, and Secret Service within seven business days. These timelines run from the moment when a carrier has obtained information indicating that a breach is



more likely than not to have occurred. Records of any breaches and notifications to customers need to be retained for two years.

Take-It-or-Leave-It Offers

The Order prohibits carriers from conditioning the provision of broadband on a customer granting consent to the use or sharing of customer PI over which the customer has either an opt-in or opt-out right.[28] The FCC finds that customer acceptance of such offers is not "approval" within the meaning of Section 222(c)(1) of the Act and would constitute an unjust and unreasonable practice under Section 201(b) and unjust and unreasonable discrimination under Section 202(a).[29]

Effective Dates for the Rules

The Order staggers the effective dates of these various requirements so that some less burdensome standards become effective ahead of the others. Under the new framework, the following rules will become effective at these times:

- Data security rule: 90 days after publication in the Federal Register
- Take-it-or-leave-it Prohibition: 30 days after publication in the Federal Register
- Data breach notification rule: the later of six months after publication in the Federal Register or Paperwork Reduction Act ("PRA") approval.
- Notice and choice rules: the later of 12 months after publication in the Federal Register or PRA approval.[30]

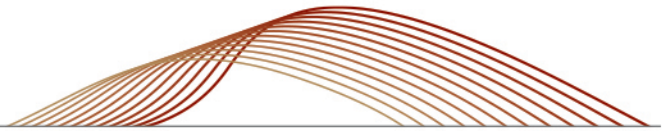
The same compliance timeline applies to both newly regulated broadband providers and legacy voice services. However, the Order specifically notes that until the new privacy rules become effective, the existing CPNI rules remain in place for legacy voice providers.[31] The FCC will treat as valid or "grandfather" any consumer consent obtained prior to the effective date of the rules, so long as it the consent is consistent with the new rules.[32]

Business Customer Exemption

Because the FCC's privacy framework is primarily designed to safeguard consumer privacy and data security interests, the Order exempts telecommunications services provided to enterprise customers from the new rules under certain conditions. To qualify for the "business customer exemption," the telecommunications service contract between the carrier and the enterprise customer must address "the issues of transparency, choice, data security, and data breach; and provide[] a mechanism for the customer to communicate with the carrier about privacy and data security concerns." Carriers providing enterprise telecommunications services may wish to explore utilizing this exemption to contractually tailor their privacy and data security practices to the diverse needs of their enterprise customers.

Proposed Rulemaking on Mandatory Arbitration

The NPRM also sought comment on the FCC's informal complaint process and whether to prohibit binding arbitration agreements between carriers and their customers for certain purposes. The Order reaffirms the right to use the FCC's information dispute resolution process and does not attempt to ban mandatory arbitration clauses in the privacy context. However, Chairman Wheeler has stated that



the FCC will put in place a process to initiate a rulemaking by February 2017 to address mandatory arbitration clauses in communications services contracts.

Takeaways

The FCC's new privacy rules have broad implications for the telecommunications industry. The Order adopts a complex set of interrelated rules which may require revisions to existing privacy policies, the implementation of new consent mechanisms, and the creation of new internal company policies for data security and breach notifications, just to name a few. Both broadband ISPs and legacy voice providers (including interconnected VoIP providers) should closely examine their privacy and data security practices in light of the FCC's new requirements.

Voice providers currently operating under the old CPNI rules should begin planning to transition to the requirements of the new framework, while still maintaining compliance with the previous standards until the new rules go into effect. Notable differences between the old and new rules include: the elimination of specific compliance recordkeeping and annual certification requirements under Section 64.2009, replacement of the existing data security procedures with a more flexible reasonableness test, and elimination of the biennial customer notice requirement.

As broadband ISPs transition to FCC governance, companies should become familiar with the differences between the FCC and the FTC. In addition to the substantive differences between the FCC and FTC's treatments of web browsing and app usage history, the agencies operate under very different statutes and possess different enforcement authorities. As one example, the FCC has authority under Section 503 of the Communications Act to issue forfeitures for violations of its rules, including on issues of first impression. In contrast, the FTC generally lacks the ability to impose fines for first time offenses under its "unfair and deceptive" trade practices authority, though it may seek civil penalties for subsequent violations of FTC or court orders. Other elements of the agencies' enforcement also differ and should be noted by companies in assessing their needs.

If you have any questions on the Order or its potential effects on your business, please do not hesitate to contact Sherrese Smith for more information.

✧ ✧ ✧

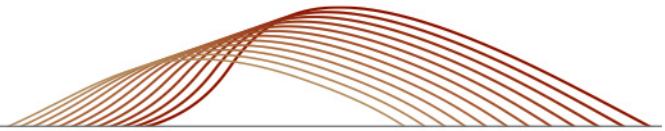
If you have any questions concerning these developing issues, please do not hesitate to contact the following Paul Hastings lawyer:

Washington, D.C.

Sherrese M. Smith
1.202.551.1965
sherresesmith@paulhastings.com

[1] *Protecting the Privacy of Customers of Broadband and other Telecommunications Services*, Notice of Proposed Rulemaking, WC Docket No. 16-106, 30 FCC Rcd ___ (2016) ("Order"), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1103/FCC-16-148A1.pdf.

[2] *Protecting the Privacy of Customers of Broadband and other Telecommunications Services*, Notice of Proposed Rulemaking, WC Docket No. 16-106, 30 FCC Rcd 2500 (2016) ("NPRM"), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1_Rcd.pdf.



[3] Order at para. 85.

[4] 47 U.S.C. § 222(h)(1).

[5] Order at para. 53.

[6] *Id.* at para. 89.

[7] *Id.* at para. 102.

[8] *Id.* at para. 106.

[9] *Id.*

[10] *Id.* at para. 125.

[11] *Id.* at paras. 298-303.

[12] *Id.* at paras. 153-155.

[13] *Id.* at paras. 192-195.

[14] *Id.* at paras. 196-200.

[15] *Id.* at paras. 201-220.

[16] *Id.* at paras. 221-233.

[17] *Id.* at para. 181-185.

[18] *Id.* at para. 238.

[19] *Id.* at para. 236.

[20] *Id.* at para. 241.

[21] *Id.* at paras. 248-255.

[22] *Id.* at para. 252.

[23] *Id.* at para. 261.

[24] *Id.* at para. 265.

[25] *Id.* at para. 266.

[26] *Id.* at paras. 267.

[27] *Id.* at paras. 275-282.

[28] *Id.* at para. 295.

[29] *Id.* at para. 297.

[30] *Id.* at paras. 312-315.

[31] *Id.* at para. 316.

[32] *Id.* at para. 317-319.