Chicago Daily Law Bulletin®

Volume 162, No. 239 Serving Chicago's legal community for 161 years

# FCC's new broadband privacy rules stirs up opponents and advocates

Under controversial new rules adopted by the Federal Communications Commission, consumers may choose how internet service providers use and share their personal data.

The FCC adopted the rules, which apply regardless of whether consumers use mobile broadband or fixed broadband, on Oct. 27, despite strong opposition from business, advertising and consumer organizations.

In February 2015, the FCC voted to reclassify broadband internet access service as a telecommunications service in its Open Internet Order. The reclassification removed broadband providers from the Federal Trade Commission's jurisdiction and into the FCC's. Then, the FCC decided that its existing privacy rules were not well suited to regulating broadband internet access.

In March, the FCC adopted the Broadband Consumer Privacy Proposal and solicited public comment as well as input from the FTC. Then, on Oct. 6, FCC Chairman Tom Wheeler formally proposed his Broadband Consumer Privacy Proposal.

**The privacy proposal**

The Broadband Consumer Privacy Proposal does not prevent internet service providers from using or sharing customers' information but mandates specific measures, including notification about data collection and use; opt-in consent to use sensitive personal information; guidelines for sharing customers' "de-identified" information; and "common-sense" data breach notification requirements.

Service providers must advise customers clearly how they collect, use and share their information by specifying the type of information collected, how and for what purpose it will be used and with whom it will be shared.

This information must be provided as soon as a customer signs up for service, updated whenever privacy policies change significantly and made available on the provider's website or mobile app. Under the new rules, the FCC's Consumer Advisory Committee is tasked with creating a standardized privacy notice format for providers to use. Adoption of the format is voluntary, but a safe harbor is provided for providers that do adopt it.

The new rules align the type of customer consent required with the level of sensitivity of customers' personal information to better reflect existing approaches taken by the FTC and the Consumer Privacy Bill of Rights. Providers are now required to obtain opt-in consent — affirmative permission — to use and share customers' sensitive information.

Sensitive information includes not only customer location via mobile phone or other device, children's information, health details, financial information, Social Security numbers, but also web browsing history, app usage history and the content of communications.

The new rules put stringent protections in place for "de-identified" information, defined as "data that have been altered so they are no longer associated with individual consumers or devices." While de-identified information presents fewer privacy concerns, the FCC points out that providers have the ability and may have the incentive to reidentify consumer data.

The new rules require providers to meet the FTC's three-pronged test to ensure consumer information is not reidentified by altering customer information so that it can't be reasonably linked to a specific individual or device; publicly committing to maintaining and using information in an unidentifiable format and to not attempt to re-identify the data; and contractually prohibiting the reidentification of shared information.

PRIVACY, TECHNOLOGY AND LAW

**NERISSA COYLE MCGINN**

*Nerissa Coyle McGinn is a Chicago-based partner at Loeb & Loeb LLP. Her practice focuses on matters involving the convergence of advertising and promotions, emerging media, technology, and privacy law, as well as intellectual property law, focusing on trademark clearance and counseling. She can be reached at nmcginn@loeb.com.*

Common sense rules for data breach notification that protect consumers' right to know when such security lapses occur also are now in place. The notification requirements are triggered when a provider determines that an unauthorized disclosure of a customer's personal information has taken place, unless the provider establishes that no harm is reasonably likely to result from the breach.

In the event of a reportable data breach, providers must notify affected customers as soon as possible, but no later than 30 days after the discovery and the FCC no later than seven business days after the discovery. In addition, the FBI and the U.S. Secret Service must be notified of breaches affecting more than 5,000 customers no later than seven business days after the discovery.

The new rules also prohibit "take it or leave it" offers, in which a provider refuses to serve customers who don't consent to the use and sharing of their information for commercial purposes, and increase scrutiny of "pay for privacy" offerings by requiring heightened disclosure for plans that give discounts or other incentives in exchange for a consumer's express affirmative consent to the use and sharing of their personal information.

Upon disclosure, the FCC must determine on a case-by-case basis the legitimacy of programs that link service price to privacy protections.

What the new rules do not do, however, is regulate the privacy practices of websites or apps, like Twitter and Facebook, or other services provided by internet providers, such as the operation of a social media website, which both remain under the FTC's authority. The rules also do not address issues such as government surveillance, encryption or law enforcement.

**Responses to the proposal**

While the FTC threw its support behind Wheeler's proposal, the rules also drew considerable criticism.

Opponents argue that the FCC, which regulates interstate and international communications by radio, television, wire, satellite and cable, does not have a mandate to establish new privacy restrictions for online data collection. Critics also maintain that the proposed rules are out of step with the FTC's existing privacy regulation efforts.

In a Sept. 14 letter to Sen. John Thune, R-S.D., chairman of the Senate Committee on Commerce, Science and Transportation, Sen. Bill Nelson, D-Fla.,

ranking member of the committee, and nine organizations led by the U.S. Chamber of Commerce said the FCC's proposal "would create restrictions that are unnecessary, overly burdensome and outside the FCC's statutory authority."

The eight advertising and privacy organizations that signed the letter are the American Advertising Federation, American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing Association, Electronic Retailing Association, Interactive Advertising Bureau, National Business Coalition on E-Commerce & Privacy and Network Advertising Initiative.

Specifically, they argue that the FCC lacks congressional authority to issue the proposed rules. Congress directed the FCC to foster competition among telephone providers and to enforce rules to safeguard proprietary data that such providers maintained through their services. This mission does not include establishing privacy rules for online data collection.

Several organizations led by the U.S. Chamber of Commerce also pointed out that the rules are not in line with the FTC's established history of addressing and enforcing privacy-related issues across industries. These organizations argue that the existing self-regulatory standards used by the FTC are sufficient to govern online content and advertising.

They also called the proposed consent standard "too restrictive," arguing that opt-out consent has proven to be more effective than opt-in consent to recognize consumer privacy preferences in the broadband context.

Other advertising and marketing trade groups added to the list of concerns in an Oct. 10 letter to the FCC. The Direct Marketing Association joined the Interactive Advertising Bureau and Network Advertising Initiative by protesting the "unprecedented step" of requiring opt-in consent to use and share "sensitive data" which include web browsing and application use history when linked to a device alone. They argue that requiring opt-in consent for such data would "stifle e-commerce and bombard consumers with unnecessary notices."

The consumer watchdog Electronic Privacy Information Center contends the proposed rules should not apply to merely providers. "While ISPs are clearly engaged in invasive consumer tracking and profiling practices, they are not the only so-called gatekeepers to the internet who have extensive and detailed views of consumers' online activities."

The Electronic Privacy Information Center urged the FCC to target all companies that gather consumer data generated by online communications services, including e-mail providers, social networking sites and search engines. It added that the FCC's proposal fell short of the Consumer Privacy Bill of Rights' guidelines.

In June, the House of Representatives Committee on Energy and Commerce's Subcommittee on Communications and Technology convened a hearing on the proposal to address fears that the proposed rules would fail to protect consumers online any better than the FTC's approach and could actually harm broadband providers.

Others raised objections on the grounds that the rules are unconstitutional. Harvard Law School professor Lawrence Tribe maintains that under a three-pronged legal test, the new rules violate the constitutional guarantee of freedom of speech.

According to Tribe, the rules fail to properly articulate why the need for consumer privacy constitutes a "substantial state interest." The rules also are too selective and under-inclusive to advance consumers' interests and impose more burdensome restrictions on "the internet ecosystem" than the FTC's pre-reclassification regulations for broadband providers, Tribe said.

As the FCC moves ahead to implement the new rules, supporters and critics alike will be watching. Legal challenges to the FCC's authority seem likely. Changes in leadership at the FCC with the incoming administration also will affect how the new rules will be implemented and whether the FCC will engage in further rulemaking on privacy concerns.