CONNECTED NATION POLICY BRIEF

Newly Adopted FCC Privacy Rules Give Broadband Consumers Say Over Personal Data

October 28, 2016

The Federal Communications Commission (FCC) recently adopted rules that will ensure that broadband consumers have greater control over their Internet Service Providers' (ISPs) use and sharing of personal information. Consumers will be required to provide consent to any sharing of information, and will be able to adjust their personal privacy preferences over time.

The FCC Fact Sheet on the action said that these rules would ensure that "broadband customers have meaningful choice, greater transparency and strong security protections for their personal information collected" by Internet Service Providers. Consistent with other standard privacy practices—such as the Federal Trade Commission and the Administration's Consumer Privacy Bill of Rights—the newly adopted rules establish a framework of customer consent by which ISPs can use and share customers' personal information based on the sensitivity of the information collected.

The rules reflect the extensive public comments submitted and received in response to the Proposed Rules adopted by the FCC in March 2016. Chairman Wheeler, along with Democratic Commissioners Rosenworcel and Clyburn, voted to adopt this week's new rules, while Commissioners Pai and O'Reilly opposed the rules citing unjustified and tougher regulations for ISPs.

The rules will begin to go into effect three months after official publication, although the consumer opt-in will not be effective for a full year. While the full text of the FCC's rules has not yet been released, this Policy Brief summarizes the key points of the FCC News Release and Factsheet provided to date.

Summary of the Rules

In the course of providing Internet access services to consumers, ISPs (often by necessity) collect, use, and store information about their consumers and the Internet services and applications they access and use. The FCC has authority under Section 222 of the Communications Act to regulate the security and privacy of information collected by providers of telecommunications services to consumers and has historically applied that authority to traditional telephone calling and billing records. By successfully defining broadband Internet access service to be a "telecommunications service" in the Open Internet Order, the FCC's authority to protect consumer data now extends to data collected by ISPs in providing broadband Internet access.

The Internet access privacy rules adopted by the FCC are divided into three main categories with specific instructions for consumers and ISPs alike on using and sharing information:

1. **Opt-in:** ISPs are required to obtain affirmative "opt-in" consent from consumers to use and share sensitive information. The rules specify categories of information that are considered sensitive, which include precise geo-location, financial information, health information, children's information, social security numbers, web browsing history, app use history, and the content of communications.
2. **Opt-out:** ISPs would be allowed to use and share non-sensitive information unless a customer "opts-out." All other individually identifiable customer information—such as e-mail address or service tier information—would be considered non-sensitive, and the use and sharing of that information would be subject to opt-out consent, consistent with consumer expectations.
3. **Exceptions to consent requirements:** Customer consent is inferred for certain purposes specified in the statute, including the provision of broadband service or billing and collection. For the use of this information, no additional customer consent is required beyond the creation of the customer-ISP relationship.

The Order also requires that ISPs adopt the following practices that are designed to enhance consumer privacy:

Transparency Requirements

ISPs must provide customers with "clear, conspicuous, and persistent notice about the information they collect, how it may be used, and with whom it may be shared, as well as how customers can change their privacy preferences," as well as transparent information when a customer signs up for service or when the ISP's privacy policy changes in significant ways. This information must remain available on the ISP's website or mobile app.

Limits on ISPs' Ability to Refuse Services

ISPs cannot refuse service to customers who do not consent to share their personal information. The rules also require a heightened disclosure process for plans that provide discounts or incentives in exchange for allowing the ISP to collect and share personal data.

Data Security

The Order states that ISPs must engage in what the FCC considers "reasonable" data security practices, and provides guidelines on steps ISPs should consider taking. These include implementing relevant industry best practices, providing appropriate oversight of security practices, implementing robust customer authentication tools, and properly disposing data consistent with FTC best practices and the Consumer Privacy Bill of Rights.

While the FCC recognizes that data security is a "dynamic and innovative arena," the rules do not provide a specific list of required data security activities. The rules will, however, provide guidelines about steps ISPs should consider taking to develop reasonable practices, such as:

- Implement up-to-date and relevant industry best practices, including available guidance on how to manage security risks responsibly.
- Provide appropriate accountability and oversight of its security practices.
- Implement robust customer authentication tools.
- Properly dispose of data consistent with FTC best practices and the Consumer Privacy Bill of Rights.

In the event of a security breach, ISPs will be required to notify affected customers as soon as possible, but no later than 30 days after a reasonable determination of a breach. If the breach affects fewer than 5,000 customers, the FCC will need to be notified at the same time as the affected customers. If the breach affects more than 5,000 customers, ISPs will be required to notify the FCC, the Federal Bureau of Investigation, and the U.S. Secret Service no later than 7 business days after reasonable determination of the breach.

De-Identification Requirements

De-Identified information is data that has been altered to prevent a person's identify from being associated with certain information. Since this type of data presents fewer privacy concerns than other types of consumer data, the new rules allow ISPs to use and share properly de-identified information outside the strict requirements for other customer data. Since the incentive and, increasingly, the technical ability to easily re-identify customer information may exist, the ISP must meet the strong, three-part test first articulated by the FTC in 2012 to ensure consumer information is not re-identified including practices to:

- Alter the customer information so that it can't reasonably be linked to a specific individual or device.

- Publicly commit to maintain and use information in an unidentifiable format and to not attempt to re-identify the data.
- Contractually prohibit the re-identification of shared information.

What the Rules Do Not Do

While the rules do many things, the FCC is clear about several key points that are not included. First, the rules do not apply to websites or apps like Twitter or Facebook since these are regulated by the Federal Trade Commission. Secondly, they do not regulate other services of broadband providers such as social media websites in operation. Lastly, the new rules do not address issues like government surveillance, encryption, or law enforcement.

Next Steps

In terms of implementation, the FCC states that the Order allows time for providers to implement necessary changes in accordance with the rules, while still ensuring customers receive the benefits intended as quickly as possible. Three points outlined as next steps in the implementation process are:

- The data security requirements will go into effect 90 days after publication of the summary of the Order in the Federal Register.
- The data breach notification requirements will become effective approximately 6 months after publication of the summary of the Order in the Federal Register.
- The Notice and Choice requirements will become effective approximately 12 months after publication of the summary of the Order in the Federal Register. Small providers will have an additional 12 months to come into compliance.

Also, in February 2017, the FCC plans to proceed with a rulemaking to address mandatory arbitration requirements in contracts for communications services.

For more information about these issues, as well as other broadband policy issues, please contact Connected Nation at policy@connectednation.org.

Subscribe via RSS to Connected Nation's Policy Briefs.