Cooley

FCC Adopts Much-Anticipated Broadband Privacy Rules

October 27, 2016

As expected, today the FCC adopted new privacy rules for broadband providers. Based on the information provided at the FCC's open meeting and in its press release and fact sheet, the new rules follow the general outline of the proposal that was released on October 6. The new rules will require significant changes in how many broadband providers collect and use customer data, and will impose constraints on broadband providers that will not apply to edge providers.

The FCC will harmonize the new rules with existing privacy requirements applied to traditional telecommunications services. This means that the previous consent requirements for voice service are being replaced by the new regime. The precise details, including whether any of the existing telephone privacy rules will be applied to broadband services, will not be known until the FCC releases the actual order, which is expected in next week or two.

The FCC rejected requests from a wide range of Internet companies to exclude web browsing and app usage from the definition of "sensitive" information that will require affirmative "opt-in" consent from customers. The FCC's requirement differs from the Federal Trade Commission's framework which only requires opt-out approval. These are the key elements of the rules:

- The rules will apply only to broadband services, not to edge providers or to the non-broadband offerings of companies that offer both broadband services and edge services or apps.
- Broadband providers will be required to notify customers about the types of information they collect about customers and how those customers use broadband service; how that information is used and for what purposes; and what entities receive that information.
- Customer notice must be provided when the customer signs up for service and when the provider's privacy policy changes in significant ways, as well as being available at all times on the provider's website or mobile app.
- Providers that want to use customer information that the FCC deems sensitive generally will be required to obtain affirmative consent from the customer. Information subject to this "opt-in" requirement will include:
    - Geo-location information
    - Web browsing history
    - App usage history
    - Actual content of customer communications
    - Children's information
    - Health information
    - Financial information
    - Social security numbers
- Except for certain limited first person marketing, all other customer information would be subject to negative option consent, so that information could be shared or used unless consumers opt out.
- Broadband providers do not need to obtain customer consent to use their information in the following circumstances:
    - To market services and equipment "typically marketed with" broadband service.
    - To provide the underlying service and for billing and collection.
    - When information has been "de-identified" (*i.e.,* all identifying data has been altered or removed so that the consumer who generated it cannot be identified), provided that the broadband provider: must alter the information so it cannot be reasonably linked to a specific individual or device; commit to maintaining and using the information in an unidentifiable format; and contractually prohibit other parties from re-identifying any information that is shared.
- Subject to heightened disclosure requirements, broadband providers can offer financial incentives (*e.g.,* reduced rates) to customers to permit use and sharing of sensitive information. Providers will not be permitted to make "take it or leave it"

offers. The FCC will review whether financial incentives meet these requirements in response to complaints or inquiries on a case-by-case basis.

- The rules adopt new data protection requirements. The FCC provides guidelines on what practices would be reasonable, based on the nature of the data and the size of the company The rules will require providers to adopt industry best practices (with specific reference to the NIST Cybersecurity Framework); to provide accountability and oversight of their security practices; to implement "robust customer authentication tools"; and to properly dispose of data.
- Broadband providers will be required to notify their customers and authorities when there has been a "reasonable determination of a breach." Customers and the FCC must be notified within 30 days of a breach. Breaches affecting 5,000 customers or more must be reported to the FCC, the FBI, and the Secret Service within 7 business days.

The FCC adopted a graduated calendar for implementation of the rules. The data security requirements will go into effect 90 days after the rules are published in the *Federal Register.* The data breach notification requirements will go into effect six months after publication. Large broadband providers will have 12 months from publication to comply with the notice and opt-in/opt-out rules, and smaller providers will have 24 months from publication to comply with those portions of the rules.

The FCC also announced that it will be opening a new proceeding to consider whether broadband providers should be permitted to apply mandatory arbitration requirements to customer privacy issues. It expects to open that proceeding in February, but has no deadline for action.

The rules were adopted by a party-line 3-2 vote, as has become common for significant FCC initiatives, and are almost certain to be appealed.

The new rules likely will significantly affect the ability of broadband providers to use customer information for targeted advertising purposes and will impose significant compliance obligations that do not apply to edge providers today. Whether the rules will have broader impact on the Internet ecosystem will depend on the extent to which they create a new baseline for privacy regulation that the FTC or state regulators adopt.

Key Contacts

J.G. Harrington Washington, DC	jgharrington@cooley.com +1 202 776 2818