Cooley

FCC Proposes New Internet Privacy and Data Security Rules

April 1, 2016

At its March 31, 2016 open meeting, the FCC adopted a notice seeking comment on privacy rules for Internet service providers (ISPs). The rules would govern how ISPs can collect and use information about their customers' online activities, as well as prescribing cybersecurity requirements for protecting customer information. Much more detailed information will be available in the coming days when the agency releases the text of the notice. The proposal was adopted over the dissent of the two Republican commissioners who expressed concern that ISPs would be subject to restrictions not applicable to other entities that collect and use this information for targeted advertising.

The rules would directly govern how ISPs collect data. They do not purport to regulate other companies that collect the same kind of information, such as websites and operating systems. They will, however, likely affect the advertising ecosystem in which companies increasingly rely on information from ISPs to build customer profiles and use ISPs to help deliver ads across numerous screens, such as TVs, tablets, smartphones and laptops.

Privacy proposals

The general outline of the privacy rules as described during the FCC meeting and **press release** create a three tiered system of customer consent:

- No consent would be required to obtain customer data necessary to provide the broadband services and for marketing the same kind of broadband services;
- Customer data could be shared with affiliates to market "communications-related services" – a category that generally includes voice telephone service and Internet access – with notice and the opportunity for customers to opt-out.
- Customers would need to provide affirmative consent to any other uses of customer data. In particular, the proposal would require affirmative consent to collect, use, share or sell customer data for targeted advertising purposes.

Under the proposed rules, ISPs must provide "clear, conspicuous and persistent notice" about what information they collect and share with third parties and how customers can limit the use of that data.

The FCC also asks whether to ban three types of practices altogether:

- ISPs could not use so-called deep packet inspection technology to review the content of on-line transmissions, presumably except for network purposes.
- Some types of persistent tracking technology would be banned. It appears that this prohibition is aimed at technologies like "supercookies" that cannot be easily disabled.
- ISPs could not offer "financial inducements" to collect and use customer data. This prohibition would cover practices like offering lower broadband prices in exchange for the ability to share or sell customer data.

Data security proposals

The FCC would require ISPs to adopt cybersecurity risk management practices, institute training programs, implement strong authentication requirements, and undertake some form of periodic security risk management audits. The notice will ask questions and seek comment on steps to secure, retain and transmit sensitive customer information. Finally, the FCC proposes to require ISPs to notify their customers of security breaches within specified time frames.

Potential impacts

The FCC's proposals are broad-reaching and will affect the online advertising ecosystem in ways that are significant but as yet unclear. Companies that partner with ISPs or use ISP-collected information in developing profiles for targeted advertising are likely to see that information flow effectively ended if the FCC adopts the rules as proposed. ISPs also have their own ad networks that work with ad exchanges, data brokers, and ad servers. Those relationships also are likely to affected as well. The ability of ISPs to assist in serving or tracking ads across devices connected to that ISP may also be affected.

The FCC's proposed cybersecurity rules could also set a precedent for other federal or state agencies. At a minimum, it is likely that any requirements adopted by the FCC will create a baseline for best practices that will be applied in other contexts.

It also is important to note that the FCC's proposals are subject to change at any point in the rulemaking process, and that the FCC could change the scope of the information covered by the rules, the requirements for consent, the limits on use of customer data, or the cybersecurity standards it has proposed. As one commissioner said during the meeting "everything is on the table."

We will provide further information and analysis as further details are made available.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as “Cooley”). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. This content may be considered **Attorney Advertising** and is subject to our **legal notices**.

Key Contacts

Michael Basile Washington, DC	mdbasile@cooley.com +1 202 776 2556
J.G. Harrington Washington, DC	jgharrington@cooley.com +1 202 776 2818

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.