Cooley

FCC Chairman Proposes Final Privacy Rules

October 6, 2016

The Federal Communications Commission ("FCC") is scheduled to vote on proposed new privacy rules governing broadband internet access service providers ("ISPs") at its October 27, 2016 Open Meeting. FCC Chairman Tom Wheeler has released a fact sheet outlining the proposed new rules and the agency is likely to adopt this proposal with few, if any, changes. The Chairman's proposed rules are less expansive in several respects than had originally been proposed by the FCC in April, particularly with respect to the scope of personal information that would be subject to opt-in consent requirements. The proceeding has been hotly contested and internet companies and others concerned that the FCC's rules could provide a template for their future regulation have become very active and appear to have convinced the Chairman to pull back in some areas. Key aspects of the proposal are summarized below.

Who is covered

The proposed rules would apply to ISPs when they provide internet access services to residential consumers, including over wireless networks. Chairman Wheeler reiterated that the rules would *not* apply to websites or apps, even if run by ISPs. Excluding ISP-owned websites could raise interesting questions in light of the Ninth Circuit Court of Appeals decision that the Federal Trade Commission ("FTC") does not have jurisdiction over the non-common carrier activities of entities, like ISPs, that also provide common carrier service. (See Cooley's recent alert on this case). Under that court's reasoning, ISPs' social media and other websites (which are not common carrier services) might escape both FTC and FCC oversight.

We also expect that these new rules for ISPs will be harmonized with existing privacy rules covering voice services. In other words, existing customer proprietary network information ("CPNI") rules that have governed privacy requirements for voice services offered by traditional telephone companies and voice over internet protocol (VoIP) providers will be revised to match these new, proposed ISP privacy rules.

Consent requirements

A central issue in this proceeding has been the extent to which affirmative, opt-in consent would be required before ISPs could use or share their customers' personal information for marketing or advertising purposes. The FCC initially proposed applying opt-in consent to a broad set of information, both sensitive and non-sensitive. Consistent with the FTC's privacy approach, the Chairman's proposal instead would require opt in consent only for sensitive personal information, an approach championed by internet companies and others. The following information would be considered sensitive:

- Geolocation information – the physical location of a smart phone or a mobile device
- Children's information
- Health information
- Financial information and social security numbers
- Web browsing and app usage history
- The content of communications.

ISPs could use of other types of individually identifiable customer or network usage information for marketing or other purposes with only opt-out consent or no consent at all, depending on the specific purposes for which the information would be used.

De-identified information

The rules would allow use of information that has been altered so that it is no longer associated with individual

consumers or devices (de-identified information) without obtaining any type of consent. However, before using de-identified information without consent, ISPs would have to comply with a three-part test designed to ensure the information is not re-identified. ISPs must:

- Alter the customer information so that it cannot be reasonably linked to a specific person or device
- Publicly commit to maintain and use information in an unidentifiable format and not attempt to re-identify the data
- Contractually bar recipients of de-identified information from attempting to re-identify it.

Data security and breach notification

Following the cybersecurity risk management approach set forth by the National Institute of Standards and Technology ("NIST"), the proposed rules would require IPSs to take steps to protect customer data, calibrated to the nature of the data and size resource of the provider, including:

- Implementing up-to-date and relevant industry best security practices
- Providing appropriate accountability and oversight of security practices
- Implementing robust customer authentication tools
- Properly disposing of data consistent with FTC best practices

ISPs would also be required to notify consumers and government agencies of unauthorized disclosures. Notification timelines would be triggered by an ISP's determination of a breach, unless the ISP establishes that no harm is reasonably likely to occur. Providers would be required to notify consumers of a reportable breach within 30 days of discovery; to notify the FCC with seven business days; and to notify the FBI and the US Secret Service within 7 days for breaches affecting more than 5000 customers. These breach notification requirements are less strenuous than originally proposed. The FCC initially proposed notification of customers within 10 days for all breaches, regardless of possible harm.

Next steps

The FCC will vote whether to approve the Chairman's proposed rules on October 27. It appears likely that something very similar to what has been outlined above will ultimately be approved, with actual implementation likely subject to some form of transition period. We would expect the FCC's two other Democratic Commissioners to vote with the Chairman, providing the three votes needed for adoption. The two Republican Commissioners sharply dissented to the proposed rules in April. It is unclear whether the modifications from that original proposal will be sufficient to garner their support. Parties still have approximately two weeks to lobby the Commission on particular issues.

Key Contacts

J.G. Harrington Washington, DC	jgharrington@cooley.com +1 202 776 2818
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090