Cooley

FCC's Internet Privacy Proposal Raises Key Issues for Online Advertising

April 12, 2016

The Federal Communications Commission plans to protect consumer privacy on the internet by regulating internet service providers. But the proposals, if adopted, could disrupt the internet advertising industry. In a 147-page Notice of Proposed Rulemaking released on April 1, the FCC appropriately seeks comment "on what effect, if any, our proposed opt-in approval framework will have on marketing in the broadband ecosystem, over-the-top providers of competing services, the larger internet ecosystem, and the digital advertising industry."

The notice proposes several new rules that could affect third party online advertisers that contract with internet service providers ("ISPs"), or their affiliated companies, including ISP-affiliated adtech companies. As described below, the FCC's far-reaching proposals, if adopted, likely will reverberate throughout the online advertising universe.

Requiring affirmative consent to share virtually any customer information

A centerpiece of the FCC's proposal is a new requirement for affirmative customer consent. As proposed, ISPs could no longer share customer proprietary information ("customer PI") with any third party absent documented, affirmative (opt-in) customer consent. ISPs would also be barred from sharing this information with their own affiliates, including advertising-related affiliates, if the information is to be used for marketing non-communications related services or products. For example, Verizon Wireless could use customer PI to market a new data plan to its subscribers, but could not, without customer opt-in, make customer PI available to third party retailers, ad brokers or other adtech companies.

Customer PI is broadly defined, and would consist of two overlapping categories: (1) personally identifiable information ("PII"); and (2) customer proprietary network information ("CPNI"). The FCC would define PII as "any information that is linked or linkable to an individual" and proposes a long, but not exhaustive, list of data that would be classified as PII. This list includes not only financial and medical information, but also device identifiers like cookies, MAC addresses, IP addresses, as well as browsing history and shopping, demographic, and geolocation information. CPNI would include some of this same information, as well as information about the type of broadband service the customer uses. Given the breadth of these definitions, virtually any information used today to build customer profiles for advertising purposes would require affirmative customer consent before the ISP could share it with third parties or even their own advertising-related affiliates.

Today, affirmative opt-in consent is required by some internet companies only for particularly sensitive information, and much of the customer information available in the online advertising ecosystem is obtained and used largely on the basis of opt-out consent. The new opt-in requirement, if adopted, could fundamentally alter access to such information unless customers are willing to provide affirmative consent.

ISP obligations must be passed through to third parties by contract

1. Contractual ban on attempts to re-identify aggregate data

The FCC would require ISPs to pass through to third parties with whom they share customer data many of the same obligations that would apply to the ISPs directly. For example, a third party online advertising company that receives from an ISP anonymized or de-identified data at a group level (called aggregate data) would be barred by its contract with such ISP from attempting to re-identify specific individuals or even the unique device

identifiers that may be needed to target ads to specific smart phones, tablets or desktops. The FCC's proposal would require ISPs to "contractually prohibit any entity to which the [ISP] discloses or permits access to the aggregate customer data from attempting to re-identify the data" and would require the ISP "to exercise reasonable monitoring of the contractual obligations relating to aggregate information and to take reasonable steps to ensure that if compliance problems arise they are immediately resolved." If this framework were adopted, we expect the FCC would look to ISPs to affirmatively police the activities of its online advertising counterparties to ensure they comply with these FCC-mandated contractual requirements. Failure to do so could result in substantial enforcement penalties against ISPs.

2.Third-party data protection and breach notification

The FCC proposes to impose on ISPs new customer data security and breach notification requirements, including that they undertake periodic risk assessments, notify customers and authorities of any breach within specified time frames, and take responsibility for the use of customer PI by third parties. To ensure the continued protection of data shared by ISPs with third parties, the FCC also provides examples of contractual commitments that ISPs could require of third parties, including that they: (1) limit the use and disclosure of customer PI to the specific purpose for which the ISP shared the customer PI with the third party and to which the customer provided approval; (2) train their employees on the third parties' information security program and monitor compliance; (3) follow the same data security and breach notification requirements that the FCC proposes to adopt for ISPs; (4) notify the ISP of any breach of security involving customer PI as expeditiously as possible and without unreasonable delay; (5) institute data retention limits and minimization procedures; and/or (6) document compliance with these contractual commitments, including records of the use and/or disclosure of customer PI. In other words, a third party who contracts with an ISP to obtain and use customer PI effectively would be required, under the terms of its contract with the ISP, to manage on-line security and report data breaches in accordance with the same set of rules the FCC is proposing to impose on ISPs.

The FCC further asks whether ISPs should "use their contractual relationship with mobile device or mobile operating system (OS) manufacturers that manufacture the devices and hardware that operate on the mobile BIAS provider's network to obtain the contractual commitments described above."

Barring persistent tracking technologies

ISPs may currently insert unique identifiers into the headers of packets containing instructions on where to route internet traffic. Sometimes called Supercookies, this kind of tracking technology can help websites and ad companies identify devices for targeted advertising. The FCC earlier this year fined Verizon $1.35 million as part of a settlement for using this technology without customer knowledge or consent. The FCC's notice asks whether it should now ban this type of tracking technology altogether, or require specific consent before its use. Persistent tracking technologies have been of particular concern to privacy advocates and consumer groups. To the extent that websites or online advertisers rely on these technologies, the FCC's proposed ban could limit their ability to serve targeted ads.

Broader implications for online advertising or other internet companies

The FCC has stated that it does not intend to regulate edge providers or other actors in the online advertising industry. While this may be true in the sense of immediate and direct regulatory impact, the above-described proposals to regulate indirectly the behavior of third parties who contract with ISPs suggest the FCC's official posture may be understated. Edge providers and other on-line participants therefore should be monitoring the FCC's proceeding. Another reason for such monitoring is that it is not unusual for FCC regulations to be used as templates for broader initiatives, including by individual regulatory authorities in the states. Moreover, even if the FCC adopts its internet privacy rules as proposed, a substantial amount of targeted advertising will continue to occur, including as a result of on-line customer data that originates outside the ISP framework. Consumers may be confused and disappointed when they continue to receive targeted ads notwithstanding their refusal to let their ISP share online information. Consumers understandably could question the efficacy of rules if they do not in fact substantially reduce the use of consumer data, leading to calls for even broader protections by federal and state authorities.

A fast track

Despite the potentially far-reaching impacts of the FCC's proposals, Chairman Wheeler appears to be fast-tracking the proposed rules. In an unusual move that underscores the agency's sense of urgency, the FCC has taken the step of setting specific comment dates in the notice, rather than tying those dates to future publication in the Federal Register. Initial comments are due **May 27, 2016** and responses to those comments are due by **June 27, 2016.** While sweeping regulatory changes of the type proposed in this proceeding typically take more than year to develop, it appears that Chairman Wheeler intends to complete this proceeding by the end of this year. That is because his term as Chairman is expected to end following the election of a new President, and he may view these new rules as an important part of his regulatory legacy.

Filing comments is important

The FCC has launched a significant and controversial proceeding with potential far-reaching implications and, as indicated at the beginning, is seeking comments from all interested stakeholders. As one FCC commissioner noted when adopting this notice, the FCC has asked some 500 questions on how best to proceed. Companies with concerns should strongly consider responding to the FCC's call to submit comments. Comments not only educate the FCC about the implications of its proposals, but also can form the basis for a later legal challenge of the agency's ultimate conclusions. To withstand legal challenges, the FCC must address serious arguments presented to it and justify both the course of action taken, and why alternatives presented in comments were rejected. Failure to do so risks judicial reversal. But the FCC cannot be challenged based on arguments not first presented to the agency.

Legal and political context

The FCC's notice stems from its Open Internet ruling last year that classified both wireline and wireless internet access service as a telecommunications service subject to privacy rules applicable to telecommunications service providers. This notice implements that decision. That decision, however, is currently under review by the District of Columbia Court of Appeals. If the court finds the FCC lacked the statutory authority to support its open internet framework, the privacy initiative may also lack the necessary legal foundation. The Court's decision is expected in the next month or two and whichever way it comes out, a request for Supreme Court review is likely.

The FCC adopted the notice in a 3-2 vote, with the two Republican Commissioners issuing sharp dissents and all five commissioners issuing separate statements. The notice comes in the context of continuing opposition by Republican members of Congress to the FCC's decision to increase its oversight of the internet. One open question is the extent to which the Republican Commissioners, backed by influential members of Congress and industry comments opposing the notice, are able to moderate at least some of the proposals contained in the notice. Moreover, while three Democrats on the Commission voted in support of the proposals, at least one noted the importance of advertising-supported free internet content as a countervailing benefit, potentially suggesting some moderation in final outcome.

For further information, please contact one of the attorneys listed.

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. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our legal notices.

Key Contacts

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.