WILMERHALE

Commission Examines Privacy and Cybersecurity Issues Associated With Emerging Cross-Device Tracking Technology

NOVEMBER 17, 2015

On Monday, November 16, the Federal Trade Commission (FTC) held a workshop that examined the key privacy and security issues raised by emerging technologies that track users across their various devices, such as smartphones, tablets, desktops, TVs and other Internet-connected devices. The outcome of the workshop has potentially broad implications for any company that provides websites, apps and online services to consumers, since cross-device technologies are increasingly being used to personalize content, improve targeting, provide security and fraud prevention, and perform analytics and attribution functions.

As companies integrate cross-device capabilities into their online products and services, the FTC's workshop will serve as an important guide. In addition, we expect that the FTC will issue a staff report that outlines key issues and best practices for cross-device tracking in the future. The FTC has invited companies to submit public comments on the topic by December 16, 2015.

What is Cross-Device Tracking?

A key goal of the workshop was to establish a baseline understanding of what constitutes cross-device tracking. Cross-device technologies often use a combination of "probabilistic" and "deterministic" methods to infer connections among consumers' various devices, such as smartphones, tablets, desktops, TVs and other Internet-connected devices. For example:

- ***Probabilistic Linking.*** Probabilistic methods collect and use device attributes (such as device IDs, IP address, time/date, etc.) to determine the statistical likelihood that browsers or devices are shared by the same user or household.
- ***Deterministic Linking.*** Deterministic methods use authenticated connections—such as through account logins or hashed email addresses—to link devices and provide a high level of confidence that devices are shared by the same user.

After a company establishes connections between devices, they often store that information in a "device graph" that may, in some instances, be shared with third parties. Panelists at the workshop noted that other technologies may be used to provide cross-device capabilities (such as "audio beacons" that use audio signals to establish connections), although alternative technologies do not

appear to be widely used at this time. Cross-device technologies differ substantially across the industry, and workshop participants noted that it can be difficult for consumers to detect whether and what cross-device technologies are being used on any particular website or mobile app.

Key Privacy Issues Raised by FTC Chairwoman Edith Ramirez

FTC Chairwoman Edith Ramirez opened the workshop by highlighting some of the key issues raised by cross-device tracking technologies. Although many of her concerns are similar to those related to online and mobile tracking in general, Chairwoman Ramirez emphasized that cross-device technology adds a layer of complexity that magnifies existing privacy concerns. In particular, the Chairwoman focused on the following challenges:

- ***Transparency.*** Chairwoman Ramirez noted that cross-device technology raises new transparency concerns because companies may collect and use information in new ways that are often difficult for consumers to detect. She also expressed concern that consumers may not understand how their cross-device data may be used, especially if it is used for potentially sensitive or discriminatory purposes.
- ***Meaningful Choice.*** She also explained that concerns about transparency may be exacerbated by a lack of meaningful choice for users. For example, she noted that consumers are not always adequately informed or educated regarding their opt-out choices.
- ***Data Minimization and Security.*** Chairwoman Ramirez also suggested that other privacy principles may apply to cross-device technology, such as data minimization, accountability and data security. In particular, she expressed the view that companies should not retain data longer than necessary to achieve its purposes.

Chairwoman Ramirez called on companies to "rise to the challenge of fostering technological solutions to inform consumers, offer choices, and honor those choices." She highlighted the role of self-regulatory organizations such as the Digital Advertising Alliance (DAA) and Network Advertising Initiative (NAI) in developing standards to provide transparency and choice to users, while also noting that the FTC "will continue to monitor the marketplace and take action as needed."

Technological and Policy Perspectives on Cross-Device Tracking

The remainder of the workshop consisted of two panels moderated by FTC staff, which examined the technological and policy perspectives on cross-device tracking. The panels included representatives from self-regulatory organizations, consumer advocacy groups and academic researchers. The panelists largely viewed cross-device tracking as a natural evolution from existing practices, and therefore that existing FTC guidance and self-regulatory codes may offer valuable notice-and-choice frameworks. Nonetheless, several themes did emerge that focused on how cross-device technology may differ from existing technologies and present unique privacy and security issues for consumers.

Challenges to Consumer Transparency

There was general agreement among panelists that transparency is a key issue. As with any new

technology, panelists expressed concern that consumers may be unaware of the cross-device technologies that companies use to collect information about users. One panelist noted that the traditional “silos” that consumers may rely on to separate their online and mobile experiences—for example between personal and business life—may no longer meaningfully distinguish a user’s online activities.

In response to questions about the steps that the industry is taking to improve consumer transparency, representatives from the NAI and DAA emphasized that they have released industry guidance and provided technical solutions to help companies provide notice and choice to consumers. For example, the DAA unveiled new guidance on Monday that is titled the Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices. Among other things, the new guidance requires first- and third-parties to comply with enhanced notice requirements under the existing DAA Principles and to inform users of cross-device practices and choices in their privacy policies.

Scope of Consumer Choice

Panelists also focused on the choices that are available to consumers with respect to cross-device technologies. There was agreement that consumers should be able to choose how their information is collected and used across devices. However, there was considerable disagreement regarding the scope of any opt-out provided and the means that would be used to effectuate that choice.

For example, the DAA’s recent guidance requires that companies extend user opt-outs only to the device from which a consumer has opted out (e.g., no data from that device may be used on other devices, and vice versa). However, some panelists suggested that opt-outs should extend to all devices that the company reasonably believes are associated with the device from which a consumer has opted out, to the extent possible. The FTC did not signal a preference for a single-device or multiple-device opt-out. Instead, the FTC staff suggested that key considerations likely would be whether a company has: (1) clearly disclosed the means through which a consumer may opt out and the effect that such a choice would have on the company’s collection, use and sharing of information about that user; and (2) that the company follow through with its disclosures, so that they are accurate.

Role and Sensitivity of Personally Identifiable Information

The panelists also considered the privacy and security risks that arise when companies collect and share hashed email addresses during the process of establishing authenticated connections among devices. Ashkan Soltani, Chief Technologist at the FTC, asked several questions that signaled that the FTC may consider the extent to which technical measures (e.g., hashing) protect users against the unlawful use or disclosure of information. For example, the FTC may consider the strength of any hashing algorithm, the retention period of hashed email addresses, and the contractual restrictions in place to prohibit re-identification and further disclosure of hashed personally identifiable information (PII).

Although panelists disagreed over the benefits of hashing PII, Jurgen Van Staden, the Director of

Policy at the NAI, explained that hashing nonetheless provides some key protections. In addition, he noted that the NAI Code of Conduct requires procedural and contractual protections designed to prevent re-identification of hashed email addresses. Justin Brookman, Policy Director for the Office of Technology Research and Investigation at the FTC, suggested that perhaps the traditional distinction between PII and non-PII is less relevant now, given the potential capabilities to re-identify individuals.

Data Retention and Data Minimization

The panelists also discussed the technical solutions that could be used to improve consumer privacy and security. While there was disagreement over the risks that are associated with the collection of information across devices, the panelists seemed to agree that one of the most basic solutions to reduce risk is to discard information after it is no longer needed for its intended purpose. Some panelists pointed out that recent data breaches have not been motivated by purely economic motives, and therefore data retention, data minimization and data security are important issues in the collection and use of cross-device technology.

Potential Misuse of Cross-Device Data

Finally, the panelists generally agreed that companies should not use cross-device technology to target sensitive categories of individuals without opt-in consent or engage in discriminatory practices. Nonetheless, there was disagreement as to how those sensitive categories or uses should be defined. For example, one panelist believed that nearly any type of price discrimination should be prohibited, but other panelists noted that individual pricing offers were not necessarily harmful to consumers. These issues likely will need to be developed over time with the participation of the FTC and self-regulatory organizations.