Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Avoiding FTC's Cross-Device Tracking Crosshairs

Law360, New York (March 1, 2017, 1:21 PM EST) --


Julie O'Neill


Adam J. Fleisher

The recent Federal Trade Commission staff report addressing privacy issues associated with cross-device tracking builds upon the staff's traditional themes of transparency and choice to affirm the importance of appropriately disclosing cross-device tracking practices and the nature and scope of any associated opt-out. While the FTC's recommendations do not introduce any materially new suggestions for compliance beyond existing industry self-regulatory efforts, the report draws attention to the importance of compliance with those efforts and the potential risks of enforcement for failing to clearly and accurately describe cross-device tracking practices and the choices that consumers have with respect to them.

Before turning to approaches for appropriate disclosure and choice for cross-device tracking, however, it may be helpful to start — as the FTC's report does — with background on what cross-device tracking means.

What is Cross-Device Tracking?

As more consumers utilize multiple devices in their daily lives, more and more companies are using new technologies to attempt to ascertain that multiple devices are connected to the same person. This is generally done through the use of either deterministic information (e.g., by recognizing a user through the log-in credentials he or she uses across different devices) or probabilistic information (i.e., by inferring that multiple devices are used by the same person based on information about the devices, such as IP address, location, browser configuration and activities on the devices).

As the FTC staff notes in the report, cross-device tracking provides many benefits. For instance, it enables a seamless experience for users across their devices and can also help improve fraud detection by identifying devices not previously associated with a known user. The report also notes, however, that the practice raises privacy concerns because it may not be adequately disclosed to consumers, and they may not be able to readily control it.

Moreover, cross-device tracking may cross physical borders that consumers intentionally establish between their devices. Consumers may not want anyone to know, for example, that their work and personal devices all reflect activities by the same person. The FTC staff focuses in particular — as it has in many of its previous reports and commentary on privacy issues — on the potential implications of disclosing sensitive information. For example, the report notes that sensitive information that might be involved in cross-device tracking (such as by revealing an individual's personal interests or activity as

manifested on a personal smartphone on the user's family computer or on a work laptop) can be particularly problematic, especially if it is associated with probabilistic tracking and thus unexpected by consumers.

How to Stay Out of the Crosshairs

Statements and recommendations in FTC staff reports matter even through the recommendations do not have the force of law. They indicate the steps that the staff believes a company should take in order to avoid a charge of unfairness or deception under Section 5 of the Federal Trade Commission Act. Here, the FTC report largely reaffirms the current compliance regime and best practices associated with cross-device tracking. The current compliance regime largely flows out of the Digital Advertising Alliance (DAA) interest-based advertising (IBA) self-regulatory notice and choice principles, which the DAA expanded to specifically address cross-device tracking in response to earlier FTC statements on the privacy issues raised by cross-device tracking.[1]

In the cross-device tracking context, the DAA principles apply if browsing activity on one device is used to deliver ads on another device. In such scenarios, the principles require that consumers be provided with a device-specific opt-out from both (1) the collection of data on the specific device in order to deliver IBA on other devices; and (2) the delivery of IBA on that device based on information collected from another device.

The FTC staff report does not suggest changes to the DAA's notice and choice principles at this time. There had been some speculation that the staff might recommend that consumers be given a single way to opt out across all of their linked devices. It did not. Instead, the staff acknowledged that current technological limitations would make it difficult to offer such a universal opt-out. The staff did suggest that companies "continue to reassess technical limitations and simplify consumer choices whenever possible."

There had also been speculation that the staff might recommend that consumers be given a way to opt out of all tracking — and not merely out of the delivery of ads targeted based on such tracking. It did not recommend that, either.

The FTC's report does not require that companies go beyond the notice and choice required under the DAA's principles, but it puts a gloss on this regime as follows:

- **Transparency:** The report recommends increased transparency and truthfulness, including about the type of data collected and how it is used and shared. And, in what could be read as a clue of how the FTC might start enforcing in this space, the report explicitly notes that "[c]ompanies do not appear to be explicitly discussing cross-device tracking practices in their privacy policies." Furthermore, the report states that personally identifiable information includes any information that can be reasonably linked to a consumer or a consumer's device. The staff accordingly suggests that "companies that provide raw or hashed email addresses or usernames to cross-device tracking companies should refrain from referring to this data as anonymous or aggregate, and should be careful about making blanket statements to consumers stating that they do not share 'personal information' with third parties." Thus, companies should consider whether they are clearly and accurately disclosing their use of cross-device tracking, including whether and to what extent personal information (as construed by the FTC) is involved.

- **Choice:** Any opt-out that a company offers must be clear and effective. Moreover, its stated scope must be accurate and not misleading. For example, if an opt-out is effective only with respect to the device from which it is exercised, that fact should be clear from the opt-out instructions, and consumers should not be led to believe that the opt-out extends to all of their devices. In addition, it should be clear, if true, that the opt-out is an opt-out from the delivery of targeted ads, and not an opt-out from the tracking itself. The FTC has brought numerous cases based on allegedly misleading descriptions and choices regarding opt-outs with respect to other types of tracking practices (as discussed further below), and it would not be surprising for it to bring enforcement with respect to cross-device activity based on the same type of allegedly misleading choices (perhaps combined with inadequate, incomplete or erroneous disclosure of a company's practices).

- **Opt-in for Sensitive Data and Security:** Consistent with the FTC's overall approach to privacy matters, the report recommends that companies obtain express consent to collect four types of sensitive information: health, financial, precise geolocation and children's information. The report also recommends that companies have reasonable security measures in place to avoid unauthorized access to and use of the personal information within their control.

In sum, to help minimize the risk of enforcement, companies should consider whether they are accurately describing that they engage in cross-device tracking, how they do it, the choices consumers have and the effect of the exercise of such choice.

Enforcement Risks and Related Considerations

Both the DAA accountability program[2] and the FTC have been active in enforcing notice and choice principles in connection with IBA. After the DAA applied its notice and choice principles for IBA to the mobile environment and began enforcement (in late 2015),[3] the accountability program brought a number of cases enforcing the principles as applied to apps and mobile devices.[4] This time around, enforcement of the DAA cross-device tracking principles began on Feb. 1, 2017, and based on previous patterns it would be surprising if the program did not find companies engaged in what it considered to be violations of the principles at some point this year.

The FTC has not yet used its authority under Section 5 of the FTC Act to bring an enforcement action based purely on a company's privacy practices relating to cross-device tracking, but it has not been shy in using this authority in connection with tracking and targeting practices deemed unfair or deceptive in violation of Section 5. Indeed, for every new type of tracking and targeting, it seems there is an example of an FTC enforcement action to affirm the applicability of notice and choice principles.

For example, in 2011, the FTC brought a case affirming that failing to properly describe notice and choice in connection with IBA can be deemed deceptive and in violation of Section 5. In that case, a company called Chitika allegedly set a cookie to opt users out of online tracking and advertising. The cookie expired after only 10 days, causing, in the FTC's view, the company's implied representation that the opt-out would last for a reasonable period of time to be deceptive.[5] Moving forward a few years, along with technological leaps, in 2015 the FTC brought a case against Nomi Technologies Inc., which provided mobile device tracking technology that enabled its clients — brick-and-mortar retailers — to receive analytics reports about aggregate customer foot traffic patterns. Nomi represented in the privacy policies posted on its website that it would "[a]lways allow consumers to opt out of Nomi's service on its website as well as at any retailer using Nomi's technology," but it allegedly did not provide

an opt-out mechanism at its clients' retail locations, thus rendering its privacy policy promise deceptive, in violation of Section 5 of the FTC Act.[6]

To take another example, the FTC recently brought a case against Vizio, the television maker, alleging in part that the company did not appropriately disclose to users that information collected from their internet-connected television viewing activity might be used by third parties to track their activity on other devices and deliver targeted advertising to them on those devices, or give users meaningful choice regarding this activity.[7] Finally, the FTC recently brought a case against online advertising services provider Turn Inc., alleging in part that the company misrepresented the scope of its opt-out: it allegedly applied only to mobile browsing and did not stop tracking and targeting users based on their activity on mobile applications.[8]

Each of these cases demonstrates the FTC's inclination to bring enforcement actions where companies do not fully and accurately describe: (1) their tracking practices; (2) the choices that consumers have relating to those tracking practices; and (3) the effect of an exercise of any such choice. Taking these cues, companies involved in tracking and targeting users across devices should consider the FTC report's recommendations and these FTC precedents when designing or revisiting their compliance strategies. The practice is becoming more prevalent and, as often happens as new technologies come on the market and the compliance regime settles into place, the FTC is paying attention and likely looking for its next case.

—By Julie O'Neill and Adam J. Fleisher, Morrison & Foerster LLP

Julie O'Neill is a partner in Morrison & Foerster's global privacy and data security group in Washington, D.C. She provides clients with practical solutions to compliance challenges around a variety of both online and offline privacy issues, including online and offline tracking, interest-based advertising, geo-targeting and other mobile tracking, personalization, and cross-device tracking.

Adam Fleisher is an associate in Morrison & Foerster's global privacy and data security group in Washington, D.C. He focuses on helping clients with all manner of challenges relating to privacy and data security, from compliance strategies to defending FTC and state attorney general regulatory investigations.

[1] The DAA is a consortium of media and marketing associations that created a self-regulatory program in the wake of a 2009 FTC report entitled "Self-Regulatory Principles for Online Behavioral Advertising." As technologies for collecting information from consumers' use of online services for IBA purposes have evolved, and as the types and number of devices on which consumers access online services has proliferated, the DAA has issued new and updated guidance, including, in November 2015, guidance on the "Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices." We previously wrote about this guidance here.

[2] Formally, the Advertising Self-Regulatory Council/Council of Better Business Bureau's Online Interest-Based Advertising Accountability Program.

[3] For background on the nature of this previous broadening of the application of the DAA principles,

see here.

[4] While the accountability program does not involve monetary penalties, it can bring companies bad press, and bring companies' practices to the attention of the FTC.

[5] In the Matter of Chitika Inc., FTC File No. 1023087 (June 17, 2011).

[6] In the Matter of Nomi Technologies Inc., FTC File No. 132 3251 (Sept. 3, 2015). For more on this initial foray by the FTC into the combination of online and physical tracking of consumers, see here.

[7] FTC v. Vizio Inc., CV No. 2:17-cv-00758 (Feb. 6, 2017).

[8] In the Matter of Turn Inc., FTC File No. 152 3099 (Dec. 20, 2016).
