
FTC Staff Issues Long-Awaited Cross-Device Tracking Report

JANUARY 24, 2017

On January 23, 2017, the FTC Staff [released](#) its long-awaited [Report](#) (“Report”) on cross-device tracking following its [November 2015 workshop](#) on the topic. The Report explains what cross-device tracking is, discusses the benefits of and challenges posed by tracking consumers across their many devices, and outlines industry self-regulatory efforts regarding this technology. The Report concludes by offering recommendations to industry regarding transparency, choice, the use of sensitive data, and data security.

The Technology Behind Cross-Device Tracking

As the FTC explains, cross-device tracking allows companies to “associate multiple devices with the same person.” By linking multiple devices with the same person, companies can track that person’s activity across all of his devices and generate a detailed picture about his online behavior. This can be used to deliver more targeted and more effective advertisements. Cross-device tracking can also be used to deliver more tailored services. A video streaming service, for example, might engage in cross-device tracking to allow a user to begin watching a movie on her computer, pause it, and resume it on her tablet.

Methods of cross-device tracking are deterministic or probabilistic. Deterministic methods track consumers using “a consumer-identifying characteristic,” like a user account. For example, when a consumer logs in to the same account on multiple devices, companies can infer that each of those devices belongs to that same consumer. On the other hand, probabilistic methods use information like IP addresses or geolocation information to discern ownership. For example, if multiple devices have the same IP address, then companies can infer they belong to the same person. Similarly, if a user’s Wi-Fi connected phone shares the same IP address as his work computer during the day, and his home computer during the evenings and weekends, companies can infer that all three devices belong to the same consumer. Companies can also combine deterministic and probabilistic methods to engage in even more accurate tracking.

The “Benefits” and “Challenges” of Cross-Device Tracking

The Report discusses the numerous benefits of, and challenges posed by, cross-device tracking. On the benefit side of the ledger, cross-device tracking promotes “seamless” online experiences by ensuring that activities performed by a user on one device—for example, checking his email—are reflected in other devices.

Such tracking also promotes greater account security and reduces the threat of cybercrime. For example, companies can use cross-device tracking to determine when a new device is used to

access an account. To ensure that the account owner, and not an identity thief, is the one using the new device, companies can then require additional authentication or alert the account owner of the use of the new device.

Cross-device tracking also holds much promise in the advertising space. Advertisers can use cross-device tracking to promote ads that are more tailored, relevant, and effective. For example, a consumer who engages in online shopping on one device can receive relevant ads on his other devices. At the same time, cross-device tracking allows companies to avoid over-saturating a consumer with the same ads across all of her devices. Plus, information about consumers gleaned from cross-device tracking can be associated with purchases online or in stores, thus allowing companies to better measure the effectiveness of advertisements.

But, according to the Commission Staff, cross-device tracking carries with it risks to consumer privacy. At the most basic level, consumers might not even know that their behavior is being tracked across their devices or understand the scope of this tracking. While some consumers might understand that their behavior is being tracked across multiple devices when they sign on to the same account on each device, the Commission Staff believes that they are less likely to be aware of probabilistic cross-device tracking. They may also not realize, according to the Staff, that information from wearable devices and other Internet-of-Things devices may be combined with information from mobile devices and computers to develop in-depth understandings of consumer behavior. What's more, the Report states that consumers may not be aware that many advertising and analytics companies collect and use data generated by cross-device tracking.

The Report also states that cross-device tracking may also pose security concerns. The detailed and expansive data collected by cross-device tracking provides a valuable target to hackers. These data can be used for blackmail, targeted phishing campaigns, identity theft, and other nefarious activities. The FTC Staff even posits that these data could be used to render security questions—those questions users often have to answer to log in or change their passwords—less effective.

Industry Efforts at Self-Regulation

The Report briefly outlines efforts by two industry self-regulatory groups to help their members navigate this space. First, the Network Advertising Initiative (NAI) introduced a [code of conduct](#) governing the use of cookieless tracking technologies. This code, among other things, emphasizes the need to give consumers notice of the use of cookieless technologies in their privacy policies and provide the ability to opt out of such technologies.

Second, the Digital Advertising Alliance (DAA) has released [guidance](#) on cross-device tracking specifically. This guidance explains that companies should give notice to consumers when collecting data that may be used for cross-device tracking and allow consumers to opt out of such use. For example, if a consumer opts out of behavioral advertising on one device, data collected from that device should not be used to provide behavioral ads on other devices. The DAA will begin enforcing this guidance in February 2017.

While the FTC “commends” these efforts, it maintains that efforts to regulate cross-device tracking could be “strengthen[ed].”

Recommendations

The Report includes recommendations for how companies can take advantage of cross-device tracking while maintaining consumer privacy and security. The Report also touches on “lessons learned” from some of the FTC’s enforcement actions. The recommendations concern the long-standing FTC principles relating to: (1) transparency; (2) choice; (3) the use of sensitive data; and

(4) security.

Transparency

The FTC Report encourages companies that use cross-device tracking disclose to consumers “meaningful” information about their use of cross-device tracking so that consumers can decide whether to opt out. Further, the Report states that cross-device tracking companies should disclose information about the use of cross-device tracking not only to consumers, but also to first-party companies that make use of such tracking. The failure to provide truthful information about cross-device tracking, the FTC Staff warns, could constitute a deceptive trade practice, and the FTC may bring Section 5 charges. This holds true for all companies in the cross-device tracking ecosystem, from publishers to device manufacturers to app developers. For example, tracking companies can be liable if they misrepresent their tracking activities to app developers.

The FTC Staff also emphasizes in its Report that companies should make accurate statements about the types of data collected. It reiterates that “data that is reasonably linkable to a consumer or a consumer’s device is personally identifiable.” Notably, the Report states that this may include raw or hashed email addresses, so companies should not claim that such information is anonymous.

Choice

The FTC’s Staff Report states that cross-device tracking companies should offer consumers choice about how their behavior is tracked—and respect those choices. So, if companies offer opt-out options, “any material limitations on how they apply or are implemented with respect to cross-device tracking must be clearly and conspicuously disclosed.” Otherwise, companies open themselves up to potential Section 5 charges. Given the complexity of the cross-device tracking ecosystem, the FTC encourages public-facing companies and tracking companies to “coordinate efforts” to ensure that they make only truthful claims.

While the FTC Staff emphasizes the need to give consumers choices, it notes that a single opt-out for cross-device tracking across all devices may be difficult to implement at this moment in time. So, the Report states that device-by-device opt-outs are sufficient. Indeed, the FTC Staff commends the DAA for offering device-by-device opt-outs and suggests that the NAI do the same. But the FTC Staff warns that stakeholders should monitor the development of technology and that a single opt-out may become more feasible in the future.

Sensitive Data

As it has in other contexts, the FTC Staff encourages companies to be especially mindful of activities that implicate sensitive data. In particular, absent consumers’ affirmative express consent, the Report states that companies should not engage in cross-device tracking with respect to sensitive information, like children’s or health information. The FTC Staff commends the NAI and DAA for requiring opt-in consent before consumers’ sensitive data to be used. But it criticizes the DAA’s definition of sensitive information as being too narrow. It encouraged both organizations to “provide heightened levels of protection for sensitive information, consistent with the Commission’s longstanding principles.”

Security

Finally, the Report reminds companies to take measures to maintain reasonable security. Such measures include data minimization and protection from breaches.

Looking Forward

The Report suggests that the FTC Staff will continue to monitor companies’ use of cross-device

tracking. In some respects, the FTC Staff seems content to allow companies and self-regulatory bodies, like the NAI and DAA, to continue to develop best practices for using cross-device tracking in a privacy-protective way. For example, it believes that device-by-device opt-out is appropriate now, but suggests that a single opt-out across devices is preferable as technology develops and encourages companies and self-regulatory bodies to monitor such technology developments and to consider requiring a single, cross-device opt out when it becomes feasible to do so. At the same time, the Report makes clear that the FTC will not hesitate to bring Section 5 charges in appropriate cases. It is crucial that companies involved in the cross-device tracking ecosphere track the FTC's actions in this space to stay out of the Commission's enforcement crosshairs.