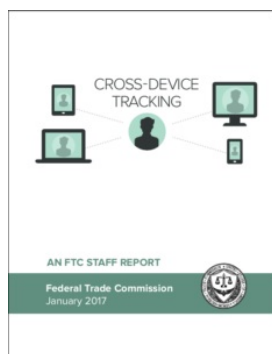


# FTC Staff Report Details Best Practices for Cross-Device Tracking

Dana B. Rosenfeld

January 24, 2017



The ubiquitous use of multiple devices by consumers has created new opportunities for mobile apps, platforms, providers, and publishers alike to capture more, and more accurate, consumer data. This practice – known as cross-device tracking – serves many purposes but is particularly valuable to advertisers.

On January 23, 2017, FTC staff released a report entitled [Cross-Device Tracking: A Federal Trade Commission Staff Report](#), which details how cross-device tracking works, the benefits and challenges of cross-device tracking, and industry efforts to address the privacy and security implications of this practice, and provides recommended best practices. The report follows the FTC’s [November 2015 Cross-Device Tracking Workshop](#) where academics, consumer advocates, and representatives from the digital advertising industry and self-regulatory organizations provided various perspectives for consideration by policymakers.

Cross-device tracking generally occurs when a consumer’s activity is linked across his or her smartphone, tablet, desktop computer, and other connected devices. This can be done in several ways, including when a consumer logs into the same platform account on multiple devices, or through social sharing widgets or analytics codes. Although its primary use is to track consumers’ activities for analytics or advertising purposes, cross device tracking provides other benefits, such as improved fraud detection and account security, and creating a seamless experience for consumers across their devices.

Despite the significant benefits, the FTC staff report notes that cross-device tracking creates many privacy and data security challenges. For example, this type of online tracking may be particularly surprising and concerning to consumers, especially where sensitive information is involved. Consumers may also be unaware of the potential scope of cross-device tracking. While a consumer may expect cross-device tracking to occur across desktops, laptops, tablets and smartphones, the

consumer may not expect it to include the collection of viewing information from smart televisions, health information from a wearable device, or shopping habits at brick-and-mortar stores. Importantly, the report notes that many companies engaged in cross-device tracking do not appear to be explicitly discussing these practices in their privacy policies.

In addition, when cross-device tracking companies collect and aggregate vast amounts of data about sites visited and apps used, this is often in conjunction with raw or hashed email addresses. Although cross-device tracking information may not contain credit card or financial account numbers, or Social Security numbers, the report explains that consumers could be harmed if this information is released without authorization following a data breach.

As such, the FTC staff report lays out some recommended best practices for companies engaging in cross-device tracking, as well as publishers, app developers, and website operators:

- **Transparency:** Companies engaging in cross-device tracking at all phases should truthfully disclose their tracking activities, accurately identify the categories of data collected involved, and provide meaningful information about whether and how cross-device tracking occurs.
- **Choice:** Companies should offer choices about how consumers' cross-device activity is tracked and ensure that consumer choice is respected across the board. In addition, to the extent opt-out tools are provided, any material limitations on how they apply or are implemented with respect to cross-device tracking must be clearly and conspicuously disclosed.
- **Sensitive Data:** Companies should refrain from engaging in cross-device tracking relating to sensitive information (such as health, financial, and children's information) and precise geolocation information, without consumers' affirmative express consent.
- **Security:** Companies should keep only the data necessary for their business purposes and properly secure the data they do collect and maintain, especially when the information collected includes personally identifiable information or information that could reasonably be linked to a person.

Companies can expect to see an increase in enforcement in this area, including by both the FTC and through self-regulatory programs. As we detailed [last month](#), enforcement of the DAA's guidance on cross-device tracking is set to begin on February 1, 2017.

\* \* \*

**Please join us for a timely webinar on cross-device tracking January 25 at 12 PM ET**, where Megan Cox, Attorney at the Federal Trade Commission, J. Jurgen Van Staden, Vice President, Policy & Technology at the Network Advertising Initiative, and Dana Rosenfeld, Partner at Kelley Drye & Warren LLP will discuss how to maintain transparency and respect consumer choice while achieving marketing objectives. CLE available. For more information and to register, please click [here](#).