

FTC'S NEW STAFF REPORT APPLIES PRIVACY PRINCIPLES TO CROSS-DEVICE TRACKING

Only days before the Digital Advertising Alliance (DAA) was set to begin enforcing its cross-device guidance (*see*, "[Enforcement of DAA Cross-Device Guidance to Begin on February 1, 2017](#)"), the Federal Trade Commission (FTC) issued a new staff report on cross-device tracking. The FTC report further explores the benefits and challenges of cross-device tracking, including some of the FTC staff's concerns about cross-device tracking. While it remains generally consistent with past pronouncements and guidance from the FTC, the report does push forward with more specific transparency, choice, sensitive data and security recommendations tailored to cross-device practices.

BACKGROUND

As the FTC staff report explains, cross-device tracking occurs when platforms, publishers and ad tech companies try to connect a consumer's activity across the consumer's multiple smartphones, tablets, desktop computers and other connected devices. Such connections can create a seamless experience for consumers, while simultaneously allowing such companies to build detailed profiles and device graphs, helping them better understand consumers' behavior across all of their linked devices.

HIGHLIGHTS OF THE REPORT

[Incorporating lessons learned from a November 2015 FTC workshop on cross device tracking](#), the new report emphasizes "transparency." It explains that because the practice of cross-device tracking may not always be obvious to the consumer, they "may be surprised to find that their browsing

THE BOTTOM LINE

Between the new FTC guidance and pending DAA enforcement, cross-device tracking is an issue that promises to be of increasing importance for the online advertising industry as the year progresses. Publishers, ad tech companies, advertisers, agencies and other members of the ecosystem should make every effort to understand the changing regulatory landscape and how to remain in compliance should they choose to take advantage of these technologies.

behavior on one device will inform the ads they see on another device."

The report also points out that consumers may be "unaware" that tracking is not limited to desktops, laptops, tablets and smartphones but that it also may include information from smart televisions, health information from a wearable device, or shopping at brick-and-mortar stores.

The report then suggests that companies "do not appear to be explicitly discussing cross-device tracking practices in their privacy

policies." Next, the report observes that consumers uncomfortable with cross-device tracking have "only limited choices to control it."

In addition, the report continues, there "may be security-related concerns" when cross-device tracking companies collect and aggregate vast amounts of data about sites visited and apps used, often in conjunction with raw or hashed email addresses.

Finally, the FTC report commends efforts by the Network Advertising Initiative (NAI) and the DAA to improve transparency and choice in connection

>> *continues on next page*

with cross-device tracking, but it adds that both the NAI and the DAA “could strengthen their efforts to address cross-device tracking,” including by taking specific enforcement actions and by further clarifying the scope of their codes.

THE REPORT'S RECOMMENDATIONS

The report offers four key recommendations for the industry to address the concerns cited in the report about transparency, choice, sensitive data and security:

- 1) *Truthfully disclose tracking to consumers and business partners.* As to cross-device tracking companies, the report specifically recommends that such companies provide truthful disclosures to consumers and to the first-party companies on whose websites and apps they appear so that these companies can, in turn, make truthful disclosures to consumers.

The report also says that consumer-facing 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” because it “can be vulnerable to re-identification in some cases.” Accordingly, it adds, these consumer-facing companies should be careful about making

blanket statements to consumers stating that they do not share “personal information” with third parties. This is consistent with past FTC guidance which broadens the definition of what is considered to be personal information.

- 2) *Offer consumers choices about how their cross-device activity is tracked – and respect consumers’ choices.* In this regard, the report suggests that consumer-facing companies that use third-party companies for cross-device tracking, and the cross-device tracking companies themselves, should coordinate efforts to help ensure that consumers receive truthful claims about their choices.
- 3) *Obtain consumers’ affirmative express consent* before engaging in cross-device tracking on sensitive topics, including health, financial and children’s information, and before collecting and sharing precise geolocation information.
- 4) *Maintain reasonable security to avoid future unexpected and unauthorized uses of data.* Among other things, the report suggests that companies should only keep the data necessary for their business purposes and that they should properly secure the data they do collect and maintain.

FOR MORE INFORMATION

Richard S. Eisert
Partner
212.468.4863
reisert@dglaw.com

Gary A. Kibel
Partner
212.468.4918
gkibel@dglaw.com

or the D&G attorney with whom you have regular contact.

Davis & Gilbert LLP
212.468.4800
1740 Broadway, New York, NY 10019
www.dglaw.com

© 2017 Davis & Gilbert LLP