PUBLICATION

Time to Review Your Online Marketing Practices and Privacy Policies

January 27, 2017

Earlier this week, the Federal Trade Commission (FTC) released a staff report on cross-device tracking, which is part of a larger series of efforts by the FTC to explore emerging issues in the ever-evolving area of online behavioral advertising. This type of advertising involves the collection of data from a particular computer or device regarding a user's Internet-viewing behavior over time and across non-affiliate websites for the purpose of inferring user preferences or interests. Cross-device tracking is the logical next step in this practice and enables online behavioral advertising to be implemented across your various devices such as your smartphones, tablets, computers, game consoles and Internet-connected TV.

The FTC acknowledges the benefits of cross-device tracking, but remains concerned with the privacy and consumer protection challenges raised by the practice. On the one hand, the FTC cites the benefits of a seamless experience for consumers across their devices, such as when they check email, read a book or watch a movie. Cross-device tracking also enables improved fraud detection and account security. It provides companies more options to protect a consumer by identifying a new device and requiring authentication through a known device. On the other hand, however, the FTC cites as concerning the lack of consumer transparency with the use of the technology, particularly given that the scope of cross-device technology in this space is not understood by a majority of the public.

Within the FTC report, FTC staff cites a study published earlier this month in which 100 popular websites were tested to determine which sites transmit data or otherwise perform actions known to facilitate cross-device tracking. When visiting these 100 websites with two different devices, the authors of the study were connected to a staggering 861 different third party domains on both devices, including domains operated by dedicated cross-device tracking companies. To be fair, the test results only show that data practices observed can be utilized to implement cross-device tracking, but cannot confirm the practice. That said, only 3 of the 100 sites tested linked to a privacy policy that explicitly discussed enabling third parties to engage in cross-device tracking. This finding is surprising, given how often visitors were connected to third party domains and it suggests that privacy policies for a majority of the tested sites may need to be updated.

The FTC has begun to bring actions against entities that utilize cross-device tracking and do not properly disclose their practices to the user, as in the FTC complaints against ScanScout and Turn Inc. In these actions, the FTC utilizes its power under Section 5 of the FTC Act, which prohibits unfair and deceptive acts or practices, commonly referred to as UDAP. The FTC argues that the privacy policy and opt-out directions disclosed to visitors of these sites were insufficient and incomplete, thereby constituting an unfair and/or deceptive act or practice.

A large issue with cross-device tracking is that the approach to the practice is in no way uniform. There are many paths as well as a myriad of technologies that can accomplish the goal. For example, you can track a user through the use of traditional cookies, flash cookies, web beacons and countless other technologies, all of which may require you to use different opt-out methods. You can also positively identify the same user across multiple devices using login information or other personally-identifiable information, commonly referred to as the deterministic method or, alternatively, you can track and identify a probable user through non-personal data, such as an IP address. This practice is known as a probabilistic method. As a proprietor of a website you

must understand the technology and methods being utilized by your marketing partners in order to properly disclose your practices to your consumers. This requires a level of due diligence that many proprietors fail to perform. Without proper controls and policies governing these practices, your regulatory, reputation and litigation risks all increase dramatically.

To avoid these risks, the FTC report sets forth four best practices for addressing privacy concerns and improving consumer transparency with regard to cross-device tracking; they include:

1. Be transparent about your data collection and use practices by truthfully disclosing your tracking activities. The FTC believes that by providing meaningful information to consumers about cross-device tracking policies, consumers can make an informed choice and decide whether to use existing opt-out tools, whether to attempt to silo their activities or whether to stop using a website, app or service altogether. The FTC also reiterates its position that data are personally-identifiable if such data are reasonably linkable to a consumer or a consumer's device.

2. Provide choice mechanisms that give consumers control over their data and, when you offer such choices, ensure that they are respected. 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.

3. Provide heightened protections for sensitive information, including health and financial – meaning express consent – should be granted by a consumer prior to engaging in cross-device tracking on these and other sensitive topics.

4. Maintain reasonable security over the collected data. Companies should keep only the data necessary for their business purposes and properly secure the data they do collect and maintain.

If you have any questions regarding the best practices associated with online behavioral advertising, cross-device tracking or any other privacy related issues, please contact any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.