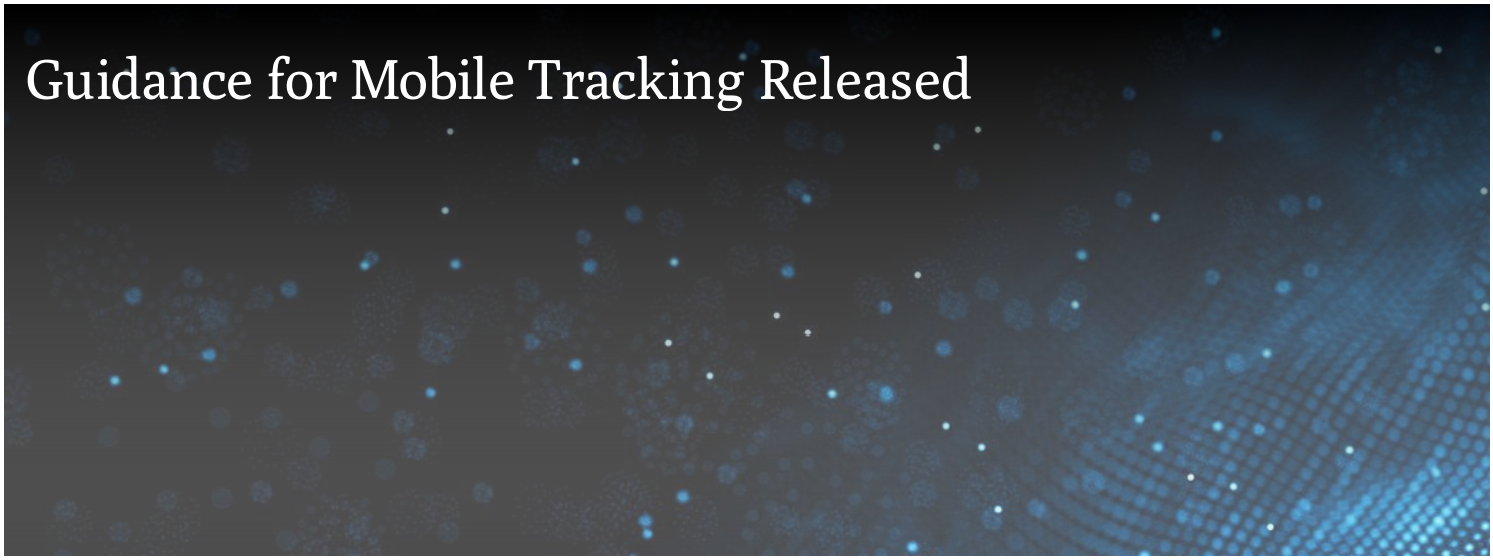
WINSTON & STRAWN LLP

BLOG

Guidance for Mobile Tracking Released



JULY 29, 2013

Last week the Digital Advertising Alliance released a much-anticipated guidance regarding how its self-regulatory principles apply in the mobile environment. The guidance clarifies what companies should do if they (1) are engaging in behavioral targeting (cross-app tracking to serve ads) in the app environment, (2) have app-based tracking of geo-location data, (3) have mobile apps that passively gather address book information, or (4) engage in behavioral advertising on mobile websites. The DAA stressed that it isn't changing its fundamental stand on notice and choice as outlined in its behavioral advertising principles or its multi-site data tracking principles. Instead, the guidance merely gives instructions on how to give notice and choice on mobile devices. For entities that have apps that (1) have behavioral advertising in the app environment, (2) have app-based tracking of geo-location data, or (3) have mobile apps that passively gather address book information, these entities must provide notice to consumers. This notice obligation is very similar to companies' obligations for computer-based behavioral advertising. However, what is new is the need to provide notice for some non-OBA tracking, specifically geo-location and address book information. In the online environment, non-OBA tracking obligations fall more heavily on vendors and other third parties, not the companies that run the websites where those third parties' tracking might occur.

Notice can be provided at the location where the app is downloaded, when the app is first opened, or when such data is collected. This can either be through linking to specific language or a separate disclosure (the notice cannot be buried deep in another document, like an app terms or EULA). The notice must also be placed in the app's privacy policy and can be put in the "settings" of the app. If the company is engaging in behavioral advertising, the guidance indicates that a company can have the privacy policy link from the app to a website, presumably because if behavioral tracking occurs, the app is connected back to the Internet to operate. If notice is in the settings, it must be accessible from everywhere that the settings are accessed. In terms of content, the notice must explain what is collected, how the data is used (*i.e.*, that behavioral advertising occurs, geo-location is tracked, and/or address book information is being gathered), provide an opportunity to opt out of these activities, and state that the entity adheres to the self-regulatory principles. If you are hiring a vendor who will help with behavioral tracking or gathering of geo-location data on your app and the vendor will be doing activities for its own purposes, be aware that these vendors have their own obligations. They must have notice of their practices in the privacy policies located on their websites. And, for behavioral tracking, they must also ensure that there is notice in or near the targeted ad, unless you have met your notice disclosures using the procedures listed above.

Choice for behavioral advertising in the app environment will be an opt-out scheme, as it is in the computer-based environment. Similar to the computer-based environment, a cross-entity process will be put in place. This process is currently being created. The DAA has indicated that while the process is being developed, it will not enforce the choice principle (although it has made no such representations about delaying enforcement of the notice obligations). For geo-location tracking, choice is opt-in. However choice should be relatively simple to obtain, as it can be part of the platform permission process. Indeed, most app stores currently require that prior notice and consent occur for geo-location tracking. There also needs to be an opt-out if someone gave consent and wishes to later revoke it. This can be done by directing users to the device settings, as long as the user can opt-out of tracking just from your app. It is also acceptable to give users instructions on how to delete the app to stop tracking as long as the deletion is easy for the user to do and it results in the tracking being stopped. For passive collection of address book information, the user must give "authorization." The guidance does not indicate how a user would provide such authorization, but it seems that "authorization" is an opt-in approach, however it might work. Even if permission is provided, the guidance stresses that this information should not be used to determine: 1) employment eligibility; 2) credit eligibility; 3) health care treatment eligibility; or (4) insurance eligibility. With respect to mobile websites, the guidance simply says that the collection and use of data from a device over time regarding web viewing across non-affiliated sites for the purpose of serving targeted ads (*i.e.*, behavioral advertising) is covered by the existing self-regulatory principles. As such, there needs to be notice about this activity on the mobile website, and consumers must be provided a choice to opt-out of these practices. This should not come as a surprise for companies that engage in these practices on traditional websites. Although the guidance does indicate that if a company cannot fit a separate link to a disclosure on their mobile website (something that should be done on computer-based sites), it is acceptable to put the notice in the company's privacy policy.

TIP: The FTC has indicated for some time that it expects entities to provide notice and choice of many tracking activities in the mobile environment. These guidelines from the DAA give clarity on how to provide notice. Companies should make sure they read and heed these instructions if they are engaging in mobile OBA, geo-location tracking, or passively collecting address book information. While there is still some time to implement choice for OBA in mobile, the guidance does have instructions for choice with respecting to geo-location and address book tracking.

This tip has been created for information and planning purposes. It is not intended to be, nor should it be, substituted for legal advice, which turns on specific facts.
4 Min Read

Related Topics

Online Privacy | Mobile Privacy

Related Capabilities

Privacy & Data Security

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.