WINSTON & STRAWN LLP

BLOG

FTC Recommends Increased Consumer Disclosures in the Mobile Marketplace

FEBRUARY 7, 2013

In response to growing concerns over consumer privacy in the mobile marketplace, the Federal Trade Commission released a staff report on February 1, 2013 recommending various steps mobile marketplace participants can take to better inform consumers about their data collection practices. The report makes recommendations for mobile platforms (OS providers such as Apple and Android), application developers, advertising networks and analytics companies, and trade associations. The overarching goal of the recommendations is to provide easy-to-understand disclosures to consumers about how their information is being collected and used, and to make sure that information is provided in a timely manner. In the report, the FTC offered specific recommendations for each critical player in the mobile marketplace. For example, mobile platforms should provide just-in-time disclosures to consumers and obtain affirmative express consent before allowing apps to access sensitive content, such as geo-location information, contacts, photos, calendar entries, and audio/video recordings. Platforms should also consider offering a Do Not Track mechanism for smart phone users to prevent tracking across mobile apps. Those that create and offer apps to consumers should have easily accessible privacy policies, coordinate with ad networks to accurately disclose what their software collects, and participate in self-regulatory programs. Ad networks and third parties should support the effective implementation of a mobile Do Not Track mechanism, while trade associations can help create standardized disclosures and privacy policies. The report is based on the FTC's enforcement and policy experience with mobile issues, as well as an FTC workshop involving the industry, trade associations, academia, and consumer privacy groups. In addition to the full recommendations in the report, the FTC also introduced a new business guide for mobile app developers outlining ways to adopt and maintain reasonable security practices. Tips included making someone responsible for security, generating credentials securely, using transit encryption, protecting servers, and remaining diligent even after the app is released. The FTC has strongly encouraged companies operating in the mobile marketplace to quickly implement these changes.

TIP: While non-binding, this report emphasizes the FTC's focus on the mobile environment, and likely signals enforcement actions that will come during 2013. Companies operating in the mobile context, including advertisers, should look at their mobile privacy policies, and ensure that they coordinate the activities of vendors like ad networks. We will continue to monitor the development of the "Do Not Track" concept.

This tip has been created for information and planning purposes. They are not intended to be, nor should they be substituted for, legal advice, which turns on specific facts.

2 Min Read

Related Topics

Consumer 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.