

FTC Issues Report on Mobile Privacy

February 07, 2013

On February 1, the FTC released a comprehensive report titled “[Mobile Privacy Disclosures: Building Trust Through Transparency](#).” As its title suggests, many of the recommendations in the report target mobile privacy issues. For example, the FTC report highlights the challenges of delivering privacy and data usage notices on small screens as well as the need for smartphones and providers to include Do Not Track (DNT) options for consumers. The report recommends that platforms use their leverage to encourage or require app developers to provide “just-in-time” disclosures to end users and require that apps obtain affirmative consent before geolocation options can be turned on or activated by an app. The report also calls for platforms to develop a “privacy dashboard” approach that allows consumers to review their privacy and data selections and change them after they have installed an app. The FTC does note that some platform owners such as Google (Android) and Apple (iOS) already have some form of a privacy dashboard in place. The report emphasizes that transparency is key. When announcing the report, FTC Chairman Jon Leibowitz said: “Say what you'll do, don't mislead, and safeguard the data.” This sentiment echoes the general message of the FTC report, which should be interpreted as a soft warning by the FTC that it is focusing on the mobile space with stepped-up enforcement measures. If your organization has a mobile app available on any platform, you should be aware of the FTC report and that your privacy disclosures, data collection, and safeguarding policies will be under increased scrutiny, both by the platform you rely on to distribute your app, and by federal and state regulators. Apps for banks, retailers, and insurance companies are among the most commonly downloaded apps on both the iOS and Android platforms. Companies that provide apps on any platform in the mobile space should be aware of this report and how it will impact their business and ability to offer mobile services to their customers. Carlton Fields has the experience and expertise to help our clients develop quality data collection and privacy policies and practices to meet industry standards and stay ahead of regulation.

Related Practices

[Cybersecurity and Privacy](#)

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.