FTC Urges Mobile Apps to Disclose to Consumers What Data Apps Collect

Mobile apps should disclose in easy-to-understand language what data they collect and how the data is used, and they should consider a do-not-track mechanism, the Federal Trade Commission (FTC) recommended in a staff report adopted by the FTC.

The report, "Mobile Privacy Disclosures: Building Trust Through Transparency," noted that "mobile technology presents unique privacy challenges. First, more than other types of technology, mobile devices are typically personal to an individual, almost always on, and with the user. This can facilitate unprecedented amounts of data collection. The data collected can reveal sensitive information, such as communications with contacts, search queries about health conditions, political interests, and other affiliations, as well as other highly personal information. This data also may be shared with third parties, for example, to send consumers behaviorally targeted advertisements."

In addition, mobile devices "can reveal information about a user's location that could be used to build detailed profiles of consumer movements over time and in ways not anticipated by consumers," the report said. "Even if a company does not intend to use data in this way, if the data falls into the wrong hands, the data can be misused and subject consumers to harms such as stalking or identity theft."

The FTC made recommendations for mobile app platforms (Apple, Google, Amazon, Microsoft), developers, and advertising networks. The recommendations are intended to inform consumers at the time the data is being gathered about what is being collected and to whom the data is being sent.

For mobile app platforms, the report recommended that before platforms allow apps access sensitive content, such as geolocation information, the platforms should disclose that fact and obtain "affirmative express consent from consumers." This disclosure "will allow users to make informed choices about whether to allow the collection of such information." Platforms should also provide just-in-time disclosures and obtain affirmative express consent before collecting other sensitive information "such as photos, contacts, calendar entries, or the recording of audio or video content." These disclosures should be "clear and understandable. For example, if an app can access geolocation information over time, the platform should avoid conveying the impression that access is one-time only."

The report further suggested that platforms should consider imposing privacy requirements on apps because "many consumers believe that the app stores provide significant oversight of apps; if an app uses their personal information in unexpected ways, this is likely to affect the platform's reputation."

The FTC report urged app platforms to include a do-not-track (DNT) mechanism to prevent an entity from developing profiles about mobile users. The DNT mechanism should allow

consumers to make a one-time selection rather than having to make decisions on an app-by-app basis. The FTC found that an effective DNT system would be "(1) universal, (2) easy to find and use, (3) persistent, (4) effective and enforceable, and (5) limit collection of data, not just its use to serve advertisements."

For app developers, the FTC recommended that developers have a privacy policy that they make available through the platform's app store. The apps should "provide just-in-time disclosures and obtain affirmative express consent when collecting sensitive information outside the platform's API, such as financial, health, or children's data, or sharing sensitive data with third parties."

The FTC observed that it is "common for app developers to integrate third-party code to facilitate advertising or analytics within an app with little understanding of what information the third party is collecting and how it is being used." App developers should understand the function of the code they use.

Advertising networks are encouraged in the report to improve "coordination and communication with app developers so that the app developers can in turn make truthful and complete disclosures to consumers." The staff found that frequently "app developers do not fully appreciate the function" of the code that advertising networks provide to include in the app and might not be aware of the information an advertising network collects.

While the staff report is not binding on mobile app developers, the FTC strongly encouraged companies to adopt the policies. The FTC has authority to prevent fraudulent, deceptive, and unfair business practices.