Skadden

PRIVACY & CYBERSECURITY UPDATE

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP & AFFILIATES

02.13.13

FTC Mobile Privacy Disclosures: Building Trust Through Transparency

Overview

On February 1, 2013, the Federal Trade Commission (FTC) issued a staff report providing guidance and promoting best practices to improve transparency throughout the mobile app ecosystem (the Report). The Report arose out of a panel discussion on transparency held at the FTC's privacy workshop in May 2012. The Report is limited in scope, focusing on the topic of transparency as a means to providing consumer choice and promoting privacy.

Background. The Report comes amidst a variety of privacy-related activities by government and private entities in the mobile space. At the federal level, in February 2012, the White House released a **nonbinding framework**[1] for the use and handling of personal data by private-sector entities in commercial settings, which included a **"Consumer Privacy Bill of Rights"**[2] and addressed privacy and disclosure issues concerning mobile apps. In July 2012, the National Telecommunications and Information Administration (NTIA) responded to the White House's call to action by convening a multistakeholder group to draft an enforceable code of conduct on the topic of mobile app transparency.

At the state level, the California attorney general has been active in promoting consumer privacy in the mobile space. In January 2012, the California attorney general's office released its own set of **recommendations directed at the mobile app ecosystem,**[3] including app developers, app platform providers, mobile carriers, advertising networks and operating systems developers. These recommendations addressed a variety of issues, including adherence to the Fair Information Practice Principles (which includes transparency) and education of app developers and consumers.

Private organizations also have been active in the area of transparency issues in the mobile space, offering conferences, workshops and best practices on the subject.

Insights into FTC's Approach. Although the Report is narrow in scope, it offers several important insights into the FTC's evolving approach to mobile privacy.

First, the FTC unequivocally includes geolocation information within the category of "sensitive" information that warrants added protection. The Report also includes in this category: (i) communications with contacts; (ii) search queries about health conditions, political interests and other affiliations; and (iii) "financial, health, and children's data." The Report recognizes that consumers may consider other types of data to be "sensitive" in certain contexts as well, specifically mentioning photos, contacts, calendar entries, and the recording of audio or video content.

---

1 Available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

2 Available at http://www.skadden.com/insights/privacy-update-overview-legislative-regulatory-and-technology-developments-privacy-sector-1.

3 Available at http://www.skadden.com/newsletters/Privacy_Update_January_2013.pdf.

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact **Stuart D. Levi,** 212.735.2750, stuart.levi@skadden.com or your regular Skadden contact.

* * *

Four Times Square
New York, NY 10036
Telephone: 212.735.3000
WWW.SKADDEN.COM

Second, the Report notes that platform providers perform a key role in the mobile ecosystem. The FTC identifies these companies as "gatekeepers to the app marketplace," exerting "the greatest ability to effectuate change with respect to improving mobile privacy disclosures." Accordingly, the bulk of the recommendations in the Report are directed at platforms such as Apple, Google, Amazon, Microsoft and Blackberry.

Finally, as noted in greater detail below, while some of the FTC's "recommendations" are phrased as recommendations (*e.g.*, "consider implementing …"), others are worded as imperatives (*e.g.*, "implement …") even though they have no binding effect. Although the Report does not itself expand any legal obligations, entities in the mobile environment should be attentive to the FTC's signals and consider implementing the FTC's more strongly worded recommendations. These recommendations may end up incorporated into the code of conduct currently being drafted by the multistakeholder process facilitated by the NTIA.

Goals of Report

Although nonbinding, the FTC intends for the Report to serve several purposes outlined below.

Improve Transparency. The Report and its recommendations are intended "to promote more effective privacy disclosures." This approach is in line with the federal government's general approach of allowing the market to self-regulate in order to avoid the stifling effects of over-regulation, while attempting to address aspects of mobile technology that may be uniquely challenging from a privacy perspective. These unique challenges include:

- **The Amount of Data Collected**: Mobile devices can facilitate an unprecedented amount of data collection about the personal life of individuals, as they are "always on and always on us";
- **The Number of Persons Receiving the Information**: The technology permits the collection and sharing of personal data amongst many entities, including wireless providers, mobile operating system providers, handset manufacturers, app developers, analytics companies and advertisers;
- **The Type of Data Collection**: Mobile devices can capture precise location data regarding individuals that can be used or abused in ways that consumers will not anticipate; and
- **The Practical Challenges of Disclosure**: Mobile device screens are small, resulting in practical limitations in conveying information to consumers.

The Report draws on the FTC's expertise in disclosures to promote best practices regarding transparency in the mobile app ecosystem. The FTC's studies of the mobile app industry indicate that current industry standards fall well short of what the FTC considers necessary to protect consumers. Meanwhile, consumers of mobile apps remain concerned about protecting their privacy and confused about their privacy-related decisions. The FTC hopes that participants in the mobile app space will adopt its recommendations to address these shortcomings.

Influencing NTIA's Code of Conduct. Second, the FTC hopes that the Report will influence the aforementioned multistakeholder process of NTIA aimed at creating an enforceable code of conduct — a process in which the FTC is a participant. While implementing such a code of conduct will not be a safe harbor against FTC enforcement actions, the FTC has stated that "to the extent that strong privacy codes are developed, the FTC will view adherence to such codes favorably in connection with its law enforcement work."

Policing Through Disclosure. Third, although not explicitly mentioned in the Report, the FTC has a vested interest in increasing companies' disclosures. As a general matter, the FTC does not have authority to bring enforcement actions against companies that violate individuals' privacy unless the practice in question violates that company's consumer-facing disclosures, thus rendering it an "unfair or deceptive act or practice."[4] As a result, companies that do not disclose

---

4 15 U.S.C. § 45(a).

their practices cannot be prosecuted by the FTC for those practices.[5] To ensure that all companies in the mobile ecosystem are under the FTC's purview, the FTC needs for those companies to disclose their business practices relating to the collection and use of personal information.

Recommendations

App Platforms. As mentioned above, the bulk of the recommendations are directed at the platform providers, as gatekeepers of the mobile space that "reap significant benefits by serving as an intermediary between the apps and consumers." These recommendations include the following:

- **Just-in-Time Notice for Sensitive Information**: Provide a "just-in-time disclosure" to consumers when apps access "sensitive" information through the platform's application programming interface (API)[6] and obtaining consumers' "affirmative express consent";
- **Just-in-Time Notice for Other Information**: Consider providing just-in-time disclosures and "obtaining affirmative express consent" before permitting apps to access information through the platform's API that is not "sensitive" but that consumers would nonetheless "find sensitive" in a given context — such as photos, contacts, calendar entries, or recorded audio/video content;
- **Privacy Dashboard**: Consider developing a privacy "dashboard" where consumers can review and modify the types of content accessed by the apps that they have installed; the Report notes that both Apple and Google have implemented "dashboards," with the two companies taking different approaches;
- **Privacy Icons**: Consider developing icons to communicate "key terms and concepts" to consumers in an easy-to-understand manner;
- **Platform Oversight of Apps**: Promote app developer best practices, for example by (i) contractually requiring developers to make privacy disclosures, (ii) reasonably enforcing these requirements, and (iii) educating app developers regarding privacy;
- **Transparency About App Review Process**: Consider providing clear disclosures regarding the extent to which the platforms (i) review apps before making them available to consumers and (ii) conduct further reviews after the apps have been released; and
- **DNT for Mobile:** Consider implementing Do Not Track (DNT) for mobile platforms, so as to allow consumers to prevent tracking by advertising networks and other third parties.

App Developers. App developers also play a "critical role" in ensuring that consumers are informed about the app developers' privacy practices. The FTC's best practices regarding transparency for app developers include the following:

- Draft a privacy policy and make sure it is easy to access through the developer's app and the app stores;
- Provide just-in-time disclosures and obtain "affirmative express consent" of consumers before collecting and sharing "sensitive" information outside of a platform's API, but without repeating the abovementioned just-in-time disclosures from platforms;

---

5 Note that under the California Online Privacy Protection Act of 2003, all mobile apps that collect personally identifiable information from California residents are required to "conspicuously post" a privacy policy. California Business and Professions Code §§ 22575-22579. This requirement is implemented by the app stores of Amazon, Apple, Facebook, Google, Hewlett-Packard, Microsoft and Blackberry — the companies that endorsed the California attorney general's Joint Statement of Principles. S*ee Skadden Privacy Update, California Attorney General Issues Guidelines for Mobile App Privacy*, January 2013, available at http://www.skadden.com/newsletters/Privacy_Update_January_2013.pdf. However, the California law does not require the degree of disclosure set forth in these recommendations and does not apply to third parties that do not collect such information from residents, such as advertising networks and analytics providers.

6 The FTC recognizes that "although a platform would know what information the app is collecting through APIs, a platform would not necessarily know what information the app is collecting directly from consumers or what information the app is sharing with third parties."

- Coordinate and communicate with advertising networks and other third parties that provide services for apps so the app developers can accurately disclose to consumers how their data will be used by those third parties; for example, app developers routinely integrate third-party code into their apps to facilitate advertising or analytics within their apps, often with little understanding of what data the third party collects or how it is being used; and
- Consider participating in self-regulatory programs or other organizations that can provide guidance on drafting privacy disclosures.

Advertising Networks and Other Third Parties. Third parties that provide services to or through apps, such as advertising networks and analytics providers, should assist the app developers in making accurate disclosures concerning such third parties' collection and use of personal information. To that end, the FTC's recommendations include the following:

- Coordinate and communicate with app developers so that the developers can provide truthful disclosures to consumers regarding the collection and use of their data; and
- Work with platforms to ensure effective implementation of DNT for mobile.

Trade Associations. Lastly, the FTC sees app trade associations as also playing a "vital role" in improving transparency in the mobile app space "by developing and improving standardized privacy disclosures, terminology, formats, and model privacy notices." The FTC's recommendations to trade associations include the following:

- Develop icons, "badges"[7] and short-form disclosures for app developers;
- Promote standardized app developer privacy policies that will enable consumers to compare data practices across apps; and
- Educate app developers on privacy issues.

Conclusion

The Report, which describes best practices regarding transparency for all participants in the mobile ecosystem, is intended to build trust between consumers and the many companies that operate in the mobile space. Its immediate impact on the mobile industry is likely to be small, as none of the FTC's recommendations are binding, and the biggest platforms appear to have already implemented many of the recommendations directed at them. That being said, the Report may ultimately have a significant impact to the extent that its recommendations are included in the code of conduct that is currently being drafted in the multistakeholder process facilitated by the NTIA.

---

7 The term "badge" as used here refers to a short, standardized disclosure that could appear within apps or within advertisements for apps. One such badge, discussed in the Report, informs users about: (i) whether an app collects or shares data; (ii) whether an app contains advertising; (iii) whether any purchases can be made within the app; (iv) whether an app shares information with social networks; (v) whether an app includes external links to other websites; and (vi) the recommended minimum age for an app.