wiley

NEWSLETTER

Developments Concerning Privacy in Mobile Apps

January 2013

As 2012 drew to a close, the privacy practices of mobile applications continued to attract significant interest from both law enforcement officials and policymakers. Here are some of the most important developments, with a forecast for what app developers and businesses that use their products should do and expect.

California Attorney General Sues Delta Air Lines over Lack of App Privacy Policy

In October, California Attorney General Kamala Harris notified approximately 100 mobile application developers and companies that they were in violation of the California Online Privacy Protection Act (CalOPPA) because they did not post a privacy policy informing users of what personally identifiable information the apps collect. The California law requires operators of online services that connect to the Internet to post a privacy policy that is readily accessible within the app and is posted conspicuously on an operator's website. The Attorney General construes the law as applying to mobile apps, although that interpretation is not entirely free from dispute. Ms. Harris gave the apps a month to post, conspicuously, a privacy policy that complies with CalOPPA.

Following through on her warning, in early December Ms. Harris sued Delta Air Lines for an alleged failure to comply with CalOPPA. The Delta lawsuit is the first enforcement action since the October warning letters.

The Attorney General's complaint alleges that the "Fly Delta" app collects a number of categories of personal information—including name, address, email address, Delta frequent flyer account number, passport number and credit card data—all without a privacy policy. The Complaint notes that the website privacy policy does not disclose that Delta collects certain types of personal information by the app that the website does not collect. Implicit in the Complaint is the Attorney General's position that an app constitutes an online service, a question that may be a subject of dispute under the law.

The Complaint charges that the absence of a privacy notice for the "Fly Delta" app, and the failure of Delta's website privacy policy to even mention the app, is a violation of CalOPPA and California's Unfair Competition Law. The Complaint asks that Delta be ordered to pay $2,500 per violation (which the Attorney General interprets to mean "per download," an interpretation that rapidly could lead to very large fines for popular apps) and also seeks injunctive relief.

This is the second time that Attorney General Harris has taken measures affecting mobile apps. Earlier in 2012, she forged an agreement with the operators of the leading app platforms–Apple, Google, Amazon, Microsoft, RIM, Hewlett-Packard and later joined by Facebook—pursuant to which the platforms will require app developers to allow consumers an opportunity to review an app's privacy policy before they download the app rather than after, and will offer consumers a consistent location at which to find an app's privacy policy. Under the agreement, the platforms also will educate developers about their obligations to respect consumer privacy, will disclose to consumers their information collection and usage practices and will facilitate the ability of consumers to report noncompliant apps.

The Attorney General's action against Delta serves as an example for other businesses. If your business has customers in California, you should consider whether it is subject to this law.

FTC Issues Report Highly Critical of App Privacy Disclosures

On December 10, the Federal Trade Commission (FTC) released a report on "Mobile Apps for Kids: Disclosures Still Not Making the Grade." The report summarized research conducted by FTC staff over the summer into the data practices (and associated disclosures, or not, to parents) of many of the top apps in the Apple and Android app stores. The FTC summarized its conclusion that "many of the apps surveyed included interactive features, such as connection to social media, and sent information from the mobile device to ad networks, analytics companies, or other third parties, without disclosing these practices to parents."

The conclusions in the report are problematic for app developers for several reasons. First, it will feed the frustration of the agency and its staff that developers have not made great progress in improving app privacy disclosures. This will only attract further regulatory (and congressional) attention.

Second, the report suggests that some are collecting data from apps targeted at children in a manner that may violate the Children's Online Privacy Protection Act (COPPA). In general, COPPA forbids operators of websites or online services from collecting personally identifiable information from children under the age of 13 without first securing prior verifiable parental consent to the collection and use of that personal information. Indeed, the FTC report mentions that the agency is currently conducting a number of enforcement investigations into app practices, and it is reasonable to expect the agency to announce some enforcement actions in the first half of 2013.

What should apps do while waiting for that next shoe to drop? One important step is to review the app to see what information it collects, and then review what is done with that data after it is collected. This review should ask questions such as: How are the data used? How long are the data retained?

In addition, in late December the FTC announced revisions to its long-standing COPPA regulation. The changes, effective July 1, 2013, will greatly limit the ability of websites and apps to use third-party plug-ins and advertising networks in their services. For example, the FTC rules would require a mobile app that is supported by targeted in-app advertising delivered by an ad network to obtain parental consent to the collection and use of personal information from a child under 13, even if the app itself collects no personal data.

NTIA Multistakeholder Process on Transparency in Mobile App Privacy Practices

Since July, the National Telecommunications and Information Administration (NTIA)—a branch of the Department of Commerce—has hosted a series of multistakeholder meetings that are intended to devise an enforceable code of conduct to promote transparency in the privacy and data practices of mobile apps. This process was initiated by NTIA in response to the White House's "Blueprint for Consumer Privacy," which called for industry and consumer groups to cooperate in devising binding self-regulatory privacy codes of conduct tailored for different types of technologies.

The process, one unfamiliar to Washington policymakers, got off to a slow start, but by the end of 2012 appeared to be making some progress in identifying potentially useful forms of short notices that developers could readily use. But many issues remained unaddressed by year's end, and it is not yet clear whether the process will successfully produce a consensus.