wiley

NEWSLETTER

Many Initiatives Address Privacy in Mobile Apps

August 2012

Developers or sponsors of mobile apps can be forgiven for thinking that they are the targets of the full attention of the nation's privacy policymakers. The combination of the remarkable growth of the app industry and some well-publicized perceived privacy violations has triggered a wide range of federal, state and industry privacy initiatives. A recent survey indicates that no less than four federal agencies, Congress, a half-dozen or so industry groups, state attorneys general and the courts are currently inquiring into privacy issues raised by mobile apps. One way or another, these inquiries will develop the regulatory framework that will govern privacy in mobile apps for years to come. The duties, obligations and responsibilities that may emerge remain far from clear.

Current Regulatory Initiatives

The Federal Trade Commission (FTC), which has taken a leading role in privacy matters generally, is taking a particularly active role in mobile privacy, relying on its enforcement authority under several different statutes. Under the Children's Online Privacy Protection Act (COPPA), the FTC staff in February of this year released a report in which it concluded that a large number of mobile apps targeted at children under the age of 13 had inadequate privacy practices. The report found that app stores and app developers seldom provided disclosures that informed parents as to what data the apps would collect from children. This report followed an FTC settlement in August 2011 with W3 Innovations—a developer of mobile apps for the iPhone and iPod Touch—of charges the developer had illegally collected personal information from children without obtaining prior parental consent.

Also this year, the FTC issued warning letters to a number of app developers reminding them that apps that function as background checks may be subject to the Fair Credit Reporting Act (FCRA). The FTC noted that apps that produce background screening reports, including information about criminal histories, may be producing "consumer reports" subject to the FCRA.

And, more generally, the FTC is relying on its consumer protection authority under Section 5 of the FTC Act to address deceptive or unfair trade practices involving mobile apps. As FTC Commissioner Julie Brill has said, "the screen is small, but Section 5 applies." In 2011, the FTC settled with the developer of a file-sharing application for the Android charges that the software's design was an "unfair" practice because preset

configurations in the installation process allowed sharing of files despite representations to the contrary by the developer.

In this vein, the FTC has conducted a series of workshops and roundtable events to raise awareness about e-tracking and mobile apps, has created a special group to address mobile privacy issues and is intent on remaining active on mobile privacy issues.

The FTC has criticized the "notice and comment" approach as inadequate and has placed more emphasis in recent months on other approaches, such as privacy by design and simplified forms of notice. The FTC's concerns are heightened by the unique features of mobile phones, including that they are almost always on and with the person, and that many parties can collect data about persons either directly or behind the scenes.

The National Labor Relations Board (NLRB), not an agency commonly known for addressing privacy issues, has taken a role on employment issues arising in social media, which of course can include mobile apps. In three published memos since August of last year, the acting general counsel of the NLRB has summarized recent agency decisions that, on the whole, take an expansive view of the rights of employees to discuss work-related issues in social media.

Not to be outdone, the Federal Communications Commission (FCC), on May 25, issued a report on location-based services and mobile network data privacy, and solicited comments on the privacy and data security practices of mobile services providers. The FCC's proceeding was spurred in part by public reports that software of Carrier IQ, a mobile analytics company, had the capability of logging users' keystrokes. Comments were filed in July, and the agency's next step is uncertain at this point.

Finally, the National Telecommunications and Information Administration (NTIA), part of the Department of Commerce, in July convened the first in what may be a series of "multistakeholder meetings" addressing disclosures of mobile app privacy practices. The NTIA process—one element of the Obama Administration's Blueprint for Consumer Privacy announced earlier this year—hopes to develop a "code of conduct" acceptable to a wide range of stakeholders, including industry and consumer advocates, that businesses would then pledge to adopt. The White House hopes that businesses would have an incentive to adopt a code of conduct in order to be more attractive to consumers, and code compliance would be subject to enforcement under the FTC's Section 5 authority. This process is in its early stages.

State law enforcement is involved, as well. In April, the attorney general of California announced an agreement with major industry participants that would require mobile apps to make privacy policies available at app stores within six months. Companies currently party to that agreement include Apple, Amazon.com, Facebook, Google, Hewlett-Packard, Microsoft and Research In Motion. In October, the attorney general's office will consider whether developers have done enough to comply with the California Online Privacy Protection Act or whether more enforcement action is needed.

Private and Legislative Initiatives

Against this background of activity by regulators, a number of industry initiatives have sought or are seeking to identify and establish best practices regarding mobile app privacy. CTIA—The Wireless Association—adopted recommended best practices for location-based services in 2010, and the Mobile Marketing Association also has adopted a recommended framework for mobile app privacy policies. The Future of Privacy Forum (FPF) and the Center for Democracy and Technology have recommended best practices for mobile app developers, and the FPF also maintains an online resource at ApplicationPrivacy.org. The FPF recently reported that more app developers are giving notice of their privacy practices (with free apps doing more than paid apps).

Mobile advertising practices are also receiving attention. Recently, a survey found that mobile advertising services were more invasive on users' devices. The Internet Advertising Bureau has announced that it is developing a set of mobile principles applicable to location services, mobile multisite data, and mobile cross-app data. The TRUSTe privacy seal company now offers a free mobile-optimized privacy policy service targeted at small app developers.

Congress, unsurprisingly, also has taken an interest. Senators Al Franken (D-MN) and Richard Blumenthal (D-CT) in 2011 introduced the Location Privacy Protection Act, which would have required businesses to obtain a user's consent before collecting or sharing location data. Just recently, Rep. Ed Markey (D-MA) elicited information indicating that law enforcement officers issued 1.3 million requests for consumers' mobile phone records in 2011 alone. And the number of individuals affected by those requests potentially was far larger.

And, of course, there is litigation. Just about every development in online or mobile privacy seems to result in a lawsuit at this time. Apple is defending a class action lawsuit in federal court arising from claims that the company secretly tracked iPhone, iPad and iPod users without their permission and disclosed data to application developers. A lawsuit filed in March in Texas sought damages from apps that uploaded the address books on users' mobile devices.

Implications for Companies

Such activity is taking place on nearly a daily basis. Companies participating in the app ecosystem should, at the least, pay attention to these developments. Legal counsel can advise on how to take these developments into account in the design and operation of apps. And businesses that wish to avoid adverse developments should consider taking a more proactive role, because the rules will be shaped by those who participate in these activities.