Published on *The National Law Review* https://natlawreview.com

Tracking the Push for Privacy - the Senate's Push for Mobile App Privacy Policies

Article By:

Kevin M. Ceglowski

Recent controversy about the **tracking capabilities of mobile software, including apps** provided by Apple and Google, highlights the increased push for privacy policies covering mobile applications. Senator Al Franken of Minnesota, chairman of the **Senate Judiciary Committee's privacy subcommittee, r**ecently sent a letter to the CEOs of Apple and Google asking them to require "**clear and understandable" privacy policies for all applications i**n the Apple App Store and Android App Market. Currently, neither company proactively enforces a requirement for apps to include these policies.

Senator Franken's letter cites a study by TRUSTe and Harris Interactive that found less than 20 percent of the top free mobile applications link to a privacy policy. The effort to expand the use of mobile privacy policies follows increased scrutiny of online privacy policies by the Federal Trade Commission (FTC). In December 2010, the FTC released a privacy report criticizing privacy policies as overly lengthy and difficult for consumers to understand.

This push for mobile app privacy policies comes on the heels of Senator Franken's Congressional hearing in early May after high-profile coverage about a location database discovered in Apple iOS software for iPhones. That tracking file, which contained information about users' locations using data from Wi-Fi hot spots and cell towers, was extensively covered by major news organizations. Google's Android software has similar tracking capabilities and creates a similar log file.

In addition to the bad publicity related to these tracking issues, lawsuits have resulted. On June 9, 2011, two plaintiffs in Florida filed a class action complaint against Google alleging the Android software engaged in illegal tracking and recording of users and that Google violated the Computer Fraud and Abuse Act and Florida law by failing to inform Android users that they were being tracked. Apple has faced similar lawsuits recently.

In light of the recent press about mobile tracking and the increased attention to mobile devices and apps from Congress, mobile application developers should include comprehensive privacy policies with their software. In so doing, developers should bear several key points in mind and learn from the mistakes made by past targets of government enforcement.

Privacy policies must be carefully crafted to comply with the various laws dictating required content.

The laws that apply will vary based on industry, the type of data collected, and the age and residency of users. Age and residency can be particularly challenging to discern in a mobile environment.

Mobile application providers face special challenges in drafting comprehensive privacy policies that can be read and understood by users reading them on small screens. Short form notices, sometimes called “highlights notices,” can be helpful, but developers must ensure material information is conveyed without excessive linking that can bury crucial content.

The FTC frequently targets companies that make overly broad privacy promises and then fail to follow them. These companies typically make promises regarding information sharing or security that they inadvertently violate. For example, in 2010, the FTC took an enforcement action against Twitter, which stated in its privacy policy, “Twitter is very concerned about safeguarding the confidentiality of your personally identifiable information. We employ administrative, physical, and electronic measures designed to protect your information from unauthorized access,” but subsequently failed to secure users’ accounts and fell prey to hackers. The resultant settlement required Twitter to implement a comprehensive security program and submit to a third party audit of that program every other year for 10 years, among other equitable remedies. This action is representative of dozens of similar actions by the FTC in recent years.

Google provides another example of privacy policy enforcement. When launching Google Buzz in 2010, Google told consumers “When you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then we will ask you for your consent prior to such use.” The FTC enforced, claiming that Google: (1) violated its privacy policies by using information provided for its Gmail email program for social networking purposes without obtaining users’ permission in advance, misrepresented that users who clicked on certain options in the Gmail system would not be enrolled in Buzz, (2) misrepresented that users could exercise control over what personal information would be made public, and (3) failed to disclose adequately that users’ frequent email contacts would become public by default. Consumers sued on similar grounds. Google’s settlement with the FTC requires it to implement a comprehensive privacy program and calls for privacy audits by a third party biennially for the next 20 years. This action represents the first time an FTC settlement ordered a company to implement a comprehensive privacy program to protect the privacy of consumers’ information. Google’s settlement of the consumer class action lawsuit requires it to create an $8.5 million fund to award money to groups that provide education on Internet privacy.

As a last point of practice, mobile app providers should ensure that they understand precisely what information they will receive from operating platforms, device providers, and social networks, as applicable. Failing to disclose to consumers with particularity the types of information received when the app is used often serves as grounds for government enforcement, Congressional inquiry, and lawsuits. Keep in mind that an ever-broader array of data, such as user location, IP address, and device identifiers may be considered “personal information” that should be subject to a privacy policy.

Despite the risk inherent in making enforceable privacy promises to consumers, the abundance of lawsuits related to online and mobile tracking, the applicable legal requirements and the scrutiny from the press, regulators, legislators and consumers collectively mean that implementation of privacy policies is strictly necessary for mobile apps. The key to managing these risks is to understand the legal landscape, to understand the operation of the software, and to develop a prudent approach that serves the application developers and the companies providing mobile apps to their consumers and employees.

National Law Review, Volumess I, Number 189