

Mobile Applications and Mobile Privacy Fact Sheet

The Emergence of Mobile Applications

Mobile devices have become the means by which the majority of the population accesses applications and browsers. As of November 2011, 50 percent of U.S. adults had an application on their phone, up from 43 percent in May 2010. Additionally, 29 percent of parents have downloaded a mobile application for their children.

The two largest mobile application platforms (Apple and Google) house approximately 1 million mobile applications, up from just 600 when they first launched in 2008. Today, mobile applications are downloaded at a rate of more than 2 billion per month. In 2010, the research company Gartner estimated that worldwide mobile application sales totaled \$6.7 billion and it is expected to grow to at least \$25 billion by 2015.

Privacy Policies in the Mobile Space

Despite the emergence of mobile Internet access, the prevalence of privacy practices in the mobile space has lagged behind traditional browser-based access. Last year, the *Wall Street Journal* reported that 45 of the top 101 apps did not provide privacy policies either inside the application or on the application developer's website. This is in spite of the fact that 56 of the mobile applications transmitted the phone's unique device ID to other companies without users' awareness or consent, 47 apps transmitted the phone's location in some way, and five sent age, gender and other personal details to outsiders. A study by TrustE and Harris Interactive found that only 19 percent of the top 340 free applications contain a link to a privacy policy and that only 5 percent of all mobile applications have a privacy policy.

What California Law Requires

The California Online Privacy Protection Act (Business and Professions Code section 22575) requires that "an operator of a commercial web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial web site or online service shall conspicuously post its privacy policy." Personally identifiable information is information, such as, a person's name, address, telephone number, e-mail address, or social security number, that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. Under the Act, a privacy policy must detail the kinds of information gathered, how the information may be shared with other parties, and, if such a process exists, describe the process the user can use to review and make changes to their stored information.

The Agreement

Attorney General Harris and the six leading mobile application platforms – Amazon, Apple, Google, Hewlett-Packard, Microsoft, and RIM – have agreed to a statement of principles to foster innovation in privacy protection, promote transparency in privacy practices, and facilitate compliance with privacy laws in the mobile arena. The principles are:

1. Where applicable law so requires, an application ("app") that collects personal data from a user must conspicuously post a privacy policy or other statement describing the app's privacy practices that provides clear and complete information regarding how personal data is collected, used and shared.

2. In an effort to promote greater transparency and to increase developer awareness of privacy issues, the Mobile Apps Market Companies will include, in the application submission process for new or updated apps, either (a) an optional data field for a hyperlink to the app's privacy policy or a statement describing the app's privacy practices or (b) an optional data field for the text of the app's privacy policy or a statement describing the app's privacy practices. For developers who choose to submit a hyperlink or text in the available data field, the Mobile Apps Market Companies will enable access to the hyperlink or text from the mobile application store.
3. The Mobile Apps Market Companies have, or will implement a means for users to report to the Mobile Platform Companies apps that do not comply with applicable terms of service and/or laws.
4. The Mobile Apps Market Companies have or will implement a process for responding to reported instances of non-compliance with applicable terms of service and/or laws. Any action that a Mobile Apps Market Company takes with respect to such an application will not limit law enforcement or any other regulator's right to pursue an action against a developer for alleged violation of applicable law.
5. The Mobile Apps Market Companies will continue to work with the California Attorney General to develop best practices for mobile privacy in general and model mobile privacy policies in particular. Within six months the participants will convene to evaluate privacy in the mobile space, including the utility of education programs regarding mobile privacy.

###