Application of Privacy Laws

By Reg P. Wydeven
March 17, 2012

Last week I wrote about how much I love my new smart phone. I keep it with me at all times to catch the scores of NCAA tournament games, check the weather, find directions or sometimes even make a call.

I also wrote about how law enforcement officers can confiscate my phone if I'm arrested to check it for numbers. The 7th Circuit Court of Appeals held that the police's ability to obtain evidence quickly by checking phones outweighs this "modest cost" of privacy invasion. However, if I get arrested, I should probably expect a little invasion of privacy.

The State of California is trying to take steps to ensure smart phone users' privacy isn't invaded when they don't expect it.

Attorney General Kamal Harris obtained agreements from the six largest companies that furnish mobile platforms for apps to improve privacy protections on mobile apps. Apple, Google, Microsoft, Amazon, Hewlett-Packard, and Research In Motion have agreed to require developers to include privacy policies in their apps that disclose the data that apps will access, use, and share.

The companies must redesign their app stores and marketplaces to ensure that the text of the privacy policy for each app is visible on the store page or there is a link to it on a website before it can be downloaded. The companies are then mandated to monitor developers to be certain they are following the guidelines.

The agreements came on the heels of reports that some mobile apps were using data from users' address books without notification or permission. Apple recently announced that any apps collecting such data without permission violate its guidelines, however, the company promised to release software to prevent future occurrences. One example was Path, a photo-sharing app that was found to be collecting user contact information without permission.

The Federal Trade Commission also addressed the issue in a recently issued report asserting that mobile apps for kids lack privacy policies. Earlier this month, Twitter disclosed that it uploads and stores many users' contact list data for 18 months without notifying them.

Harris pursued the agreements to bolster California's Online Privacy Protection Act, which is one of the strongest consumer privacy laws in the country. Under the Act, commercial websites or online services that collect consumers' personally identifiable information are required to conspicuously post a privacy policy that details the kinds of information gathered, how the information may be shared with other parties and describes how a consumer can review and make changes to their stored data.

Previously, it was unclear whether the Act applied to mobile apps. At a press conference, Harris explained that extending the Act to apps "will give more information to the consumers so they understand how their personal and private information can be used and potentially manipulated." Harris elaborated by saying, "Most mobile apps make no effort to inform users...Consumers should be informed what they're giving up before they download the app."

If developers or platform providers violate the Act, they can be prosecuted under California's Unfair Competition Law or its False Advertising Law or both. Penalties under the law include fines of up to $500,000 per use of the app in violation.

Harris' office will meet with the mobile app platforms in six months to assess their progress, however, there is no firm implementation date for the new rule.

One thing I've downloaded on my phone is the Indiana Jones app. When you thrust your phone forward, it makes a whipping sound. If the company that makes that app accesses my address book to email those folks, they'll be disappointed to find out there are no other nerds in my contacts that would even think of downloading their app.