Jules Polonetsky and Christopher Wolf : App developers, not regulators, are best suited to solve privacy problem

By Jules Polonetsky and Christopher Wolf
Special to the Mercury News
Posted: 03/19/2012 06:58:38 PM PDT
Updated: 03/19/2012 06:58:39 PM PDT

For years, marketers dreamed of the day when smartphones would be ubiquitous. Users would get ads based on their actual location at the time. Offers would be delivered right to the consumer's pocket. All agreed that privacy and user permission would be sacred because, after all, this was very sensitive data. Users considered their phones to be a highly personal device. Overstepping boundaries would not be tolerated.

So how are things working out?

Smartphones are indeed ubiquitous. The personal data available far outstrips what was ever imagined. Location, address books, social network relationships, photos, texts, emails and other highly personal information is stored on these devices and many users feel so tied to their phones that they keep them in reach even when in bed.

Unfortunately, it seems that just about every week we hear about another example of mobile misbehavior. Leading mobile apps are caught uploading users' address books without bothering to ask. iPhone and Android phones are accused of allowing apps to access users' photos without clear permission. Advertising companies are using technical tricks to bypass mobile browser privacy settings. Our recent Future of Privacy Forum survey showed that only a third of the most popular apps even bothered to have a privacy policy.

What has gone wrong?

To some extent, the mobile ecosystem is a victim of its own success. Several years ago, regulated cellphone carriers provided network service, sold phones and decided what apps could be made available. Today, the mobile smartphone environment is a fast-growing, chaotic system of platforms provided by Apple or Google, independent app developers, mobile ad networks and other third parties. Hundreds of thousands of developers provide innovative new features using the personal data they access on consumer devices, many with little experience managing the giant databases they can assemble.

Each misstep leads to an explosion of tweets, blog posts and complaints. If companies don't get their acts together quickly, users may stop feeling so free about sharing the data that has been the driver of new services and profits.

Thankfully, some progress is being made. California Attorney General Kamala Harris recently entered into an agreement with six leading app store and platform operators that will allow consumers to review an app's privacy policy before they download the app. The agreement also commits platforms to educate developers about their obligations to respect consumer data. The platforms will work to improve compliance with privacy laws by giving users tools to report noncompliant apps and committing companies to responding to these reports.

Similarly, the Federal Trade Commission has put developers on notice that it is ready to take action against apps that are acting deceptively. And the Obama administration is signaling that mobile apps may be the first sector it seeks to convene for a multi-stakeholder effort to develop enforceable privacy guidelines.

We welcome the policy-makers into the fray and are advancing the dialogue by hosting an app developer privacy summit to bring together developers, platforms and government regulators in San Francisco. But the folks best suited to solve the problem are the app developers themselves.

The energy and ingenuity displayed by the venture and developer communities in creating and launching apps can address consumer concerns far more effectively than the government. Don't wait for us to tell you what to do. Show up with solutions in hand. Just remember that access to user data is a privilege, not a right. Now start coding!