

iPhone location-tracking incident boosts stock of 'privacy by design'

Jay Cline

May 9, 2011 ([Computerworld](#))

What does the world's most valuable company now have in common with the following initiatives?

- * [Online-behavioral tracking](#)
- * [Deep-packet inspection](#)
- * [Persistent cookies](#)
- * [Unique microchip identifiers](#)
- * [Single sign-on for all Web commerce](#)
- * [Paying by fingerprint](#)
- * [Street View Wi-Fi sniffing](#)
- * [Admiral Poindexter's Total Information Awareness program](#)

The common denominator? *Privacy quicksand*. This is the sandy arena frequented by regulators and legislators and stirred up by privacy advocates. Once your project or technology walks into this particular sand trap, it's hard to pull your reputation out of the mud.

The operating dynamic of privacy quicksand is that first impressions count more than facts. This is because people instinctively are wary of large and powerful organizations and assume the worst. If your organization's new product or technology could spy on its users, they'll assume it's happening. The end result of walking into the privacy quicksand is that your project usually gets scaled back or canceled.

[Apple](#) has one foot in the sand, and tomorrow's hearing by the [Senate Judiciary Subcommittee on Privacy, Technology and the Law](#) may determine if it's able to sidestep the rest of the pit.

"Recent advances in mobile technology have allowed Americans to stay connected like never before and put an astonishing number of resources at

our fingertips," Sen. Al Franken (D-Minn.) told me. "But the same technology that has given us smartphones, tablets and cell phones has also allowed these devices to gather extremely sensitive information about users, including detailed records of their daily movements and location. This hearing is the first step in making certain that federal laws protecting consumers' privacy -- particularly when it comes to mobile devices -- keep pace with advances in technology."

The maker of the world's most popular [smartphone](#) has found itself under this scrutiny because of a [report two researchers issued last month that claimed that Apple was storing iPhone users' location data in an unencrypted file in their iTunes accounts](#). Franken sent Apple CEO Steve Jobs a letter the same day requesting an account of the situation. See the table below for a timeline of the incident.

Timeline of the Apple iPhone location-tracking controversy

Date

- 4/20** Two researchers issue a [report](#) claiming [Apple](#) is tracking iPhone user locations.
- 4/20** [U.S. Sen. Al Franken sends Apple CEO Steve Jobs a letter](#) containing nine questions about the location-tracking features of the iPhone.
- 4/25** [Franken invites Apple and Google to Senate hearings](#) on [smartphone](#) privacy.
- 4/27** [Apple posts FAQs about its location-tracking feature and promises a fix](#).
- 5/10** First hearing of the Senate Judiciary Subcommittee on Privacy, Technology and the Law.

I think Apple has a good chance of coming out OK. The feature in question was designed to make the iPhone work a lot faster. iPhone users who love the device are probably going to give the company a strike or two before they start questioning its motives on privacy. Plus, Apple says it's already working on fixing the privacy and security features that could have been done better in the first place.

People who do privacy for a living are saying Apple could have avoided this diversion. They're pointing to the "privacy by design" methodology as the way to make sure new products and technologies don't walk into the privacy quicksand.

What is privacy by design?

It's the notion that you should build good privacy practices -- such as storing the minimum personal data necessary -- into the design phase of new products.

"It's about baking privacy into your products and services," Ontario Privacy Commissioner Ann Cavoukian told me. Cavoukian first coined the "privacy by design" tagline and now runs a [website](#) and annual conference dedicated to the concept.

To people outside the privacy profession, making privacy protection a standard design requirement sounds like basic common sense. But the norm in both the private and public sectors is to handle privacy reactively and minimally. The norm for organizations today on every continent is to look at what the law minimally requires, and then to apply the law in the least disruptive way possible to existing products and services.

"It's time to stop reacting to privacy issues after the fact," Cavoukian said. "Tell users what you intend to do with their data, be it geolocation or purchasing preferences. A bit more openness and transparency could put the brakes on the mounting erosion of privacy."

"Businesses that act on this message will gain a competitive advantage," she added.

In the case of Apple and the iPhone, for example, nothing in the law prevented it from designing the iPhone tracking feature just the way it did. And nothing but the court of public opinion now requires it to make its promised fixes. The iPhone incident is one more example of how the law alone is no sure guide for helping a company achieve its business objectives.

Is privacy by design the sure guide, though? I admit that I was skeptical when I first heard about this idea. I thought privacy by design was a marketing gimmick that poured the old wine of the [1980 Fair Information Principles \(FIP\)](#) into new wineskins.

But it's gaining traction. The [U.S. Federal Trade Commission's landmark privacy-framework paper](#) issued in December 2010 -- which arguably sets the direction for U.S. privacy legislation and rulemaking for the coming several years -- cites privacy by design as one of its four pillars. In October 2010, commissioners at the 32nd annual conference of international data-protection commissioners rallied around the privacy by design flag in its [final resolution](#).

This is good news for privacy officers and product-design people alike. Up until now, these two groups of people have tended to talk past each other or stay in their own corners. Regulator interest in this concept, however, should prompt more meeting invites e-mailed from the former to the latter.

This is already happening at some companies.

[Microsoft](#) was one of the first. In 2006, it released its [Privacy Guidelines for Developing Software Products and Services](#), a comprehensive set of criteria to include in any software-development life cycle. The guidelines, updated in 2008, are scheduled for another release later this year. Microsoft's privacy office has also added other related resources to a [Privacy by Design website](#).

"For us, privacy by design represents over a decade of investment in a comprehensive privacy program that includes people, processes and technologies that help us anticipate and address privacy sensitivities in our products and services while continuing to deliver innovation to our customers," Brendon Lynch, Microsoft's chief privacy officer, told me.

"Recent examples," he added, "include location-sharing limits and controls in Windows Phone 7, local storage and prompt deletion of biometric data that helps control the Kinect for Xbox 360 gaming system, and Tracking

Protection Lists for the Internet Explorer 9 Web browser, which provide groundbreaking capabilities to prevent online tracking."

How are the Senate privacy hearings going to turn out tomorrow? I think the visiting companies from Silicon Valley are going to survive the upbraiding. But others should be taking notes about how to avoid this particular tour of the nation's capitol, and what direction the Senate might be taking next.

Jay Cline is president of [Minnesota Privacy Consultants](#). You can reach him at cwprivacy@computerworld.com.