

Mobile apps raise new privacy concerns

March 23 2012, By Patrick May

Smartphone in hand, you tap into your local application store. You click on a nifty tool that promises to massage your belly and pat your head at the same time. But just as you're about to download it, you decide to click on that little Terms of Service icon. And you're hit with a phone-book-sized data dump of not-so-fine fine print.

On top of all the [privacy](#) battles already under way across the Internet, the boom in [mobile apps](#) has ramped things up even more, with waves of service terms and security policies at every new download.

You're damned if you read it, because most of it was written by lawyers and makes little sense to you, and possibly damned if you don't, because you later find out you've agreed to let the [app](#) grab and sell your personal data to advertisers, who in turn will stalk you online forever.

The number of apps is exploding, with nearly 600,000 for sale in the Apple App Store alone. So, too, are the number of worrisome stories about things like "data leaks," where your contact list, for example, is mysteriously downloaded by that cool gaming app you just selected. Meanwhile, the torrent of fine print just keeps coming.

"For most of us, it's really challenging to read this stuff and make sense out of it," said senior staff attorney Kurt Opsahl with the [Electronic Frontier Foundation](#) in San Francisco. "Whether it's terms of service or a privacy policy, some of them are so lengthy that if you spent a day surfing the Web collecting all the terms and policies affecting you, it would take you more than a whole other day to read them all. It's not

physically possible."

Federal and [state regulators](#), along with [privacy advocates](#), are pushing for more clarity and transparency in the way apps may use personal information, including your name, gender and email address, as well as your hometown, [family relationships](#), or religious and political affiliations.

Various versions of a so-called "privacy bill of rights" for [mobile phone users](#) are circulating and being adopted by some app developers. And California Attorney General Kamala Harris's office is working with Google, Apple and other platforms to streamline and simplify the way developers explain the privacy policies and user terms for their apps. One idea is to offer more opt-in pop-ups that warn you each time your personal data is about to get mined and asks for your permission.

But for now, making sense of "these terms can be overwhelming," said Chris Conley, the technology and civil liberties fellow with the American Civil Liberties Union of Northern California. "The goal is obviously to inform users about what's happening with their personal data. But there has to be an easier way for users to find out what information about you these apps have gathered, instead of making the users email them to find out.

"There's often just too much stuff for you to manually search through to find it."

An hourlong visit to the app store can leave you hip-deep in a muck of legalese - or with no information at all in those cases where developers have not included a privacy policy, in violation of an often-overlooked 2004 California law that requires such a statement.

"Right now, if you go and look for a privacy policy, less than 50 percent

of apps even have such a policy posted," said Travis LeBlanc, special assistant attorney general of California. "Twenty-two of the top 30 paid apps don't have privacy policies, so we first need these folks to get policies."

And for those apps that do provide such policies, LeBlanc says you often "have to go on a treasure hunt to find them. There's just no consistency on where to find an app's privacy policy."

Take Yelp. Scroll to the very bottom of that company's pitch page in the iPhone App Store. Click "License Agreement," and in hard-to-read text on gray background, you'll learn that you're breaking the rules if you're under 18 and using it to find an open taco joint.

Yelp will remind you, too, that you can't even use the app if you're "a competitor of ours," and that your account can be closed "at any time without notice and ... for no reason." And you must agree to let Yelp "disclose information about you to third parties" for a whole bunch of reasons, including "to protect our rights, reputation, and property."

Yelp did not respond to a request from the San Jose Mercury News for an interview about its privacy policy. But as the Electronic Frontier Foundation's Rebecca Jeschke points out, "even if you do read the terms, you still can't understand a lot of what they say. And either way, you have to say yes or no. If you say no, you don't get the app."

So while Jeschke and her cohorts continue to push for what they call "human-readable" privacy and security policies, you might wander over to the Spotify music app and check out its legal section. There you can see the dual-challenges firsthand: parts of it are unintelligible, while other parts are clear but scary in how much data you're agreeing to hand over.

Use Spotify, and you waive your right to bring a class-action lawsuit against the company. Use Spotify, and you agree that only the laws of New York will govern any dispute you have with them. Use Spotify, and you're letting them access information about you and your use of the app.

What sort of information? Here's one more burst of fine print: "Queries you make, date and time of your request, your Internet protocol address, performance of your network and computer, your browser type, language and identifying information, your operating system and application version." Spotify also lets you know that "your personal information including gender and age and postal address will be shared with anyone who merges with or buys Spotify."

PRIVACY EFFORTS:

-The Obama administration in February proposed a framework for protecting privacy in the digital age. The plan, laid out in a white paper available at whitehouse.gov, includes a Consumer Privacy Bill of Rights designed to enhance transparency and security for consumers as well as limit the amount of personal information companies can collect through the Internet. Status: Pending approval by Congress.

-California Attorney General Kamala Harris recently announced an agreement with leading operators of mobile app platforms, including Google and Apple, to improve privacy protections of consumers who access apps through their sites. Status: Further talks set for August.

-San Francisco-based Electronic Frontier Foundation has drawn up a Mobile User [Privacy Bill](#) of Rights to help guide users, app developers and platform providers in their privacy policies. Proposed rights include

more individual control by users over how their [personal data](#) is collected and used. The framework also encourages developers to "seek to empower users even when it's not technically or legally required by the platform."

(c)2012 the San Jose Mercury News (San Jose, Calif.)
Distributed by MCT Information Services

Citation: Mobile apps raise new privacy concerns (2012, March 23) retrieved 24 June 2024 from <https://phys.org/news/2012-03-mobile-apps-privacy.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.