February 11, 2013

# California Does It Again! Recommends Best Practices for the Mobile App Industry

By Leonard A. Ferber, Co-Head, Technology Practice

In last month's Technology Advisory, I described recent actions of the California Attorney General designed to improve privacy protections for users of mobile applications. This included an agreement the California Attorney General (CAG) reached with the companies whose platforms comprise the majority of the mobile app market (Amazon, Apple, Facebook, Google, Hewlett-Packard, Microsoft and Research In Motion) on a set of principles intended to ensure that mobile apps comply with applicable privacy laws such as the California Online Privacy Protection Act (CalOPPA), formation of the California Attorney General's Privacy Enforcement and Protection Unit (the CAG's Privacy Unit) and enforcement against mobile app makers of CalOPPA's requirement that "online services" have privacy policies accessible to users.

## California's Recommendations for the Industry

As part of this ongoing administrative effort, the CAG's Privacy Unit has now prepared *Privacy on the Go: Recommendations for the Mobile Ecosystem*, which stands as a formulation of "best practices" for the industry. As its name suggest, it encompasses recommendations for the entire "ecosystem"—from the app platforms and app developers to mobile ad networks, operating system developers and even mobile carriers.

The CAG's Privacy Unit sees its mission as supporting the right of privacy included in the California Constitution.[1] However, they also attempt to buttress their efforts with a "pro-business" rationale, pointing to a recent study finding that more than half of mobile app users had uninstalled or decided not to install an app because of concerns about its privacy practices.[2]

Seen in the larger picture, the CAG's Privacy Unit is seeking to influence the multi-stakeholder process being promoted by the Obama Administration, and currently being facilitated by the National Telecommunications and Information Administration (NTIA),[3] to develop an enforceable code of conduct for the mobile app industry. Accordingly, it is not surprising that, by its own admission, the CAG's Privacy Unit acknowledges that the *Privacy on the Go* recommendations "in many places offer greater protection than afforded by existing law."

## The General Principles

In developing the recommendations, the CAG's Privacy Unit was guided by two principles. The first was the need for all members of the mobile app ecosystem to consider privacy implications early in the design and development process. This echoes recent Federal Trade Commission statements encouraging mobile app developers to adopt a "privacy by design" approach.[4] The second principle is "surprise minimalization." The CAG's Privacy Unit recognized that, although mobile devices are subject to the same privacy risks as traditional personal computers, there are some risks that are unique to mobile devices. For example, telephone

---

1 Article 1, Section 1 of the Constitution of the State of California reads: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

2 Boyles, Jan Lauren, Aaron Smith, Mary Madden, "Privacy and Data Management on Mobile Devices," Pew Internet & American Life Project, September 5, 2012.

3 See the White House privacy report "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," February 2012.

4 See, for example, the Federal Trade Commission Report "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers," March 26, 2012.

call logs, text messages and location history are not typically found on personal computers, but are frequently stored by mobile devices. It also pointed out that mobile devices and apps can facilitate combinations of user and device-related data that may pose new privacy risks. The CAG's Privacy Unit further acknowledged that mobile devices' small screens make the effective communication of privacy practices and user choices difficult.

*Privacy on the Go* recommends that app developers "minimize surprises to users from unexpected privacy practices." The CAG's Privacy Unit suggests the most basic way to do this is to "avoid collecting personally identifiable data from users that are not needed for an app's basic functionality." Moreover, they recommend that developers "supplement the legally required general privacy policy with enhanced measures to alert users and give them control over data practices that are not related to an app's basic functionality or that involve sensitive information." California is making the stand that it is no longer acceptable to bury disclosures and then hide behind a claim of "but it's in the privacy policy!"

## Best Practices for App Developers

Although *Privacy on the Go* provides best practices for app platform providers, mobile ad networks, operating system developers and mobile carriers, the bulk of the recommendations are for mobile app developers, and I will be discussing only those recommendations in this article.

The specific recommendations which implement the "privacy by design" and "surprise minimalization" principles can be divided into two types: those that focus on a developer's approach to collecting and retaining data and those that focus on communicating the privacy and data policies and practices to users.

Collecting and Retaining Data. *Privacy on the Go* recommends that developers start by compiling a data checklist which lists the personally identifiable data the app could collect. Next, it is recommended that developers ask themselves specific questions about that data. For example:

- Is the data type necessary for your app's basic functionality (i.e., within the reasonably expected context of the app's functionality as described to users)?
- Is the data type necessary for business reasons (such as billing)?
- How will you use the data?
- How long will you need to store the data on your servers?
- Will you share the data with third parties such as ad networks, analytics companies or services providers?
- Is the app directed to or likely to be used by children under the age of 13?
- What parts of the mobile device do you have permissions to access?

With this information, developers can create their privacy policies. In doing so, developers are instructed to reflect a desire to limit both data collection and data retention.

With respect to limiting data collection, *Privacy on the Go* suggests developers:

- Avoid or minimize the collection of personally identifiable data for uses not related to your app's basic functionality, and limit the retention of such data to the period necessary to support the intended function or to meet legal requirements.
- Avoid or limit the collection of sensitive information.
- Use an app-specific or other non-persistent device identifier rather than a persistent, globally unique identifier.
- Give users control over the collection of any personally identifiable data used for purposes other than the app's basic functions.
- Set default settings to be privacy-protective.

As for limiting data retention, *Privacy on the Go* suggests developers:

- Not retain data that can be used to identify a user or device beyond the time period necessary to complete the function for which the data was collected or beyond what was disclosed to the user.
- Adopt procedures for deleting personally identifiable user data that you no longer need.

Communicating Data and Privacy Policies. A written privacy policy is a requirement under CalOPPA. *Privacy on the Go* provides several admonitions focusing on how to communicate privacy policies to users, most of which should not be a surprise to anyone generally familiar with privacy policies:

*Be Transparent*

- Make privacy practices available to users before the app is downloaded and any data is collected.
- The general privacy policy is readily accessible from within the app.

*Give Users Access*

- Develop mechanisms to give users access to the personally identifiable data that the app collects and retains about them.

*Make It Easy to Find*

- Make the privacy policy conspicuously accessible to users and potential users.
- Post or link the policy on the app platform page to make it available to users before the app is downloaded.
- Link to the policy within the app (for example, on the controls/settings page).

*Make It Easy to Read*

- Make the privacy policy clear and understandable by using plain language and a format that is readable on a mobile device. In this regard, two possible formats are suggested:
    - A layered notice that highlights the most relevant privacy issues.
    - A grid or "nutrition label for privacy" that displays privacy practices by data type.

*Use "Enhanced Measures" as Appropriate*

What is somewhat new, however, is that *Privacy on the Go* suggests that under certain circumstances, developers should supplement their general privacy policies with enhanced measures intended to alert users to these circumstances. *Privacy on the Go* offers several examples of the types of information the CAG's Privacy Unit believes would necessitate such enhanced measures:

- Collection, use or disclosure of personally identifiable data not required for the app's basic functionality.
- Accessing text messages, call logs, contacts or potentially privacy-sensitive device features such as a camera, dialer or microphone.
- A change in your data practices that involves new, unexpected uses or disclosures of personally identifiable data.
- The collection or use of sensitive information (such as precise geo-location, financial or medical information, or passwords).
- The disclosure to third parties of personally identifiable information for their own use, including use for advertising.

To the CAG's Privacy Unit, "clearer, shorter notices" of these privacy practices are necessary in the small-screen mobile environment. These should be "delivered in context and just-in-time" (i.e., just before the specific data is to be collected). Alternatively, use of the combination of a short privacy statement and privacy controls would be acceptable to the CAG's Privacy Unit. According to *Privacy on the Go*, "the short privacy statement should highlight the potentially unexpected practices and sensitive information" and "readily accessible privacy controls should give users a convenient way to make choices and to change them when desired."

## What You Should Know

As mentioned in the previous Technology Advisory, what happens in California exerts a tremendous influence on the rest of the country when it comes to issues of privacy (in more common parlance, "what happens in California doesn't stay in California"). Besides putting its own "marker" in the quest to establish industry-accepted "best practices," *Privacy on the Go*'s focus on surprise minimalization and practical steps designed to accomplish this are likely to find wide acceptance among the regulators at the Federal Trade Commission and in the industry-wide initiatives promoted by the NTIA. In particular, the use of enhanced measures—special notices or the combination of a short privacy statement and privacy controls—intended to draw users' attention to the gathering of sensitive information or the use of data practices that may be unexpected and to enable them to make meaningful choices is likely to become the norm. This would require a refinement of the old privacy policy adage of "say what you do/do what you say" to include ". . . and say it in a manner so that it will have a good chance of being noticed."

A company that simply provides an app as part of a mobile strategy directly related to its core business will find California's recommendations to be instructive and adoption to be relatively painless. A business seeking to leverage the data collection aspects of apps in order to become a "data company" will find the recommendations proposing limiting data collection and data retention more troublesome. However, a careful reading of all the recommendations suggests that surprise minimalization is truly the paramount concern. Increased sensitivity to providing disclosures of a company's collection of sensitive information or unsuspected data use in a manner reasonably likely to be seen by users is, at the end of the day, what will be required of "data companies."

**********

For more information, please contact any of the following members of Katten's **Technology Practice**.


**Tanya L. Curtis**
Chicago
312.902.5593
tanya.curtis@kattenlaw.com

**Leonard A. Ferber**
Chicago
312.902.5679
leonard.ferber@kattenlaw.com

**Doron S. Goldstein**
New York
212.940.8840
doron.goldstein@kattenlaw.com



Katten

Katten Muchin Rosenman LLP www.kattenlaw.com

AUSTIN CENTURY CITY CHARLOTTE CHICAGO IRVING LONDON LOS ANGELES NEW YORK OAKLAND ORANGE COUNTY SHANGHAI WASHINGTON, DC