Advisory

JANUARY 2013

If you have any questions about this Advisory, please contact:

JOHN KENNEDY
203.363.7640
jkennedy@wiggin.com

PRIVACY AND INFORMATION SECURITY PRACTICE GROUP

Wiggin and Dana's Privacy and Information Security Practice is a multi-disciplinary team of seasoned attorneys from a wide-range of practices, including Technology and Outsourcing, Litigation, Health Care, Franchise, Antitrust and Consumer Protection, Insurance, and White Collar Defense, Investigations and Corporate Compliance. Because of this breadth and diversity of experience, our Privacy and Information Security Practice is able to provide effective, strategic and industry-tailored advice to a broad array of national and international clients.

The World Gone Mobile: California Attorney General Issues Roadmap to Privacy Protection in the 'Mobile Ecosystem'

California regulators have traditionally carried the flag towards new consumer privacy protections in the nation's digital economy. Last week, the California Attorney General took the battle to the privacy wilderness known as the "mobile ecosystem" by issuing comprehensive recommendations to protect consumer privacy in "[a] world gone mobile."

"Privacy on the Go: Recommendations for the Mobile Ecosystem"[1] (the "Recommendations") is the most comprehensive set of privacy compliance guidance for mobile media issued to date by any state. Indeed, the Recommendations go well beyond the mobile app privacy guidelines published last year by the Federal Trade Commission.[2] While not law, the Recommendations lay down a baseline compliance checklist for all mobile businesses subject to California's Online Privacy Protection Act. Given the inherently national scope of the mobile apps industry, the Recommendations will likely influence ongoing industry and government efforts to establish comprehensive mobile privacy standards.

BACKGROUND

The Recommendations follow upon the California AG's February 2012 "Joint Statement of Principles"[3] with major mobile application platform providers (such as Google, Apple and Microsoft) and also grow out of the AG office's subsequent discussions with, and input from, industry stakeholders. The Joint Statement was a shot across the bow to large players in the mobile apps industry, reminding them that the Online Privacy Protection Act[4] (the "Act"), which requires operators of commercial websites to have compliant privacy disclosures, applies equally to mobile e-commerce. The industry signatories to the Joint Statement have moved forward with various initiatives to improve transparent privacy disclosures, consumer choice and accountability in the mobile apps marketplace. Now, the AG has encouraged the industry further by publishing detailed privacy recommendations to all players in the 'mobile ecosystem'—app developers, app platform providers, online advertising networks, operating system developers and carriers.

PRIVACY CONCERNS UNDERLYING THE RECOMMENDATIONS

The explosion in the use of mobile computing devices has seeded the booming industry of mobile 'apps.' Apps enable anytime, anywhere consumer services that range from streaming movies and online gaming to location-based restaurant recommendations and on-the-fly banking. This "world gone mobile" is also feeding an exponential increase in the collection and sharing of personal data of device users. The Recommendations cite an industry statistic showing one million apps available today and another 1,600 new apps being published every day. In addition to the behavioral data collection associated with online tracking of desktop Internet users,

CONTINUED ON NEXT PAGE

The World Gone Mobile: California Attorney General Issues Roadmap to Privacy Protection in the 'Mobile Ecosystem' CONTINUED

many of these proliferating mobile apps can capture and share text messages, call logs and geo-tagged photos and videos, together with a user's around-the-clock location history. Those types of data, in turn, can be combined with other data stored on a device (or fed by other apps on a device) to create rich profiles of users' online and offline lives. But the growth in data collection capabilities has greatly outstripped measures by the mobile apps industry to insure that privacy practices are transparent and that users have adequate and clear choices about the data being collected from them. This wide gap between the industry's powers of harvesting personal data and the requirements of the Act is the primary target of the Recommendations.

"SURPRISE MINIMIZATION": KEY PRIVACY PRACTICES FOR MAKERS OF MOBILE APPS

The basic thrust of the Recommendations is (1) to encourage the mobile industry to build fair information practice principles ("FIPPs")[5] into the design of mobile apps, devices and services, and (2) to enhance transparency in privacy disclosures and simplicity in user privacy controls. The overarching consumer protection goal is "surprise minimization"—i.e., reducing instances where consumers are subject to unexpected (or undisclosed) collection and sharing of their personal information, particularly information that is not required for an app's basic functions. For instance, a user might be unpleasantly surprised to learn that a birding app also harvests the user's personal contacts or call logs. The notion of limiting mobile data collection to uses "*reasonably expected*" by users in the context of an app's functions (as disclosed to users) is central to the AG's overall guidance.

Specific AG recommendations for mobile app developers include the following:

- Build privacy into mobile apps: App developers should identify all types of personal data that an app will collect or disclose to third parties (including data collection characteristics of third party software used in an app). Examples of personally-identifiable information include unique device identifiers, geo-location data, mobile phone numbers, text messages, call logs, financial payment information, health and medical information, photos and videos, browsing and download histories, etc. This list of data types should then be reviewed against a checklist designed to smoke out data uses that may conflict with FIPPs or with applicable privacy law. Checklist items, for example, would include:
  - Identifying uses of the data necessary for the app to function or related purposes (e.g., billing) and other uses that may exceed what is necessary for the app to function;
  - With whom and for what purpose personal data will be shared (e.g., ad networks, analytics providers, other apps or functions on a device);
  - Any controls users will have to modify their permissions for data collection.
- Establish privacy practices for data collected: The Recommendations cite several of the familiar FIPPs, such as transparency of data practices; limited data collection and retention; easily-read and easily-accessed statements of privacy practices; means for consumers to access personal data collected and retained by the app; reasonable security measures including encryption of personal data in transit; and designation of responsible persons in the organization to maintain and update privacy policies. Given the small screen constraints on privacy disclosures on mobile devices, app developers are encouraged to develop "special notices"—short notices, delivered in real time, before data is collected, especially where the collection of data is not required for the app's functionality or where "sensitive" data (e.g., financial account or health information) will be collected. Special notices are intended to be in addition to, not in lieu of, comprehensive general privacy notices. Other specific guidance "tips" for privacy practices by app makers include:
  - Using app-specific or other non-persistent device identifiers when collecting data, rather than identifiers that are persistent and uniquely identify the device associated with the user;
  - Giving users control over the collection of any personal data that is not needed for the functioning of the app;
  - Offering default settings for controls which are privacy protective.

CONTINUED ON NEXT PAGE

The World Gone Mobile: California Attorney General Issues Roadmap to Privacy Protection in the 'Mobile Ecosystem' CONTINUED

RECOMMENDATIONS FOR APP PLATFORM PROVIDERS, AD NETWORKS AND OTHER MARKET PARTICIPANTS

The interdependence of all mobile ecosystem participants in effecting adequate privacy protections for consumers is another underlying theme in the Recommendations. The Recommendations accordingly also address privacy issues specific to mobile app platform providers (e.g., the group of companies that signed the Joint Statement), mobile advertising networks, mobile operating system developers and mobile carriers. Platform providers are encouraged to help consumers access an app's privacy disclosures before they download the app, to provide ways for users to report complaints or questions about apps purchased through the provider, and to further consumer education on mobile privacy. Mobile ad networks are urged to provider their own privacy policies to app developers who deliver network-provided ads through their apps and to provide a link to their policy which app developers can, in turn, make available to users before they download or activate the app. Operating system developers and mobile carriers are asked to work together, among other purposes, to develop cross-platform standards for privacy controls and security patches.

IMPLICATIONS FOR THE MOBILE PRIVACY DEBATE

It remains to be seen whether the Recommendations will have the same kind of default influence on developing privacy practices as other California privacy initiatives have had, such as data breach notification and privacy disclosure requirements. Much of what is contained in the Recommendations is also present in a variety of recently-issued industry guidelines for mobile privacy and advertising, and the national stakeholder dialogue on codes of conduct for mobile app transparency, begun through the National Telecommunications and Information Administration, is still only getting underway.[6]

The Recommendations certainly will not be the last word on privacy guidance for the mobile industry. But for now, they offer a useful window on the kinds of data practices that may keep mobile apps providers on the right side of the California AG's office.

[1] http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf
[2] http://business.ftc.gov/documents/bus81-marketing-your-mobile-app
[3] http://ag.ca.gov/cms_attachments/press/pdfs/n2630_signed_agreement.pdf
[4] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579
[5] These are the principles of transparency, purpose specification, collection limitation, use limitation, individual participation, data quality, security and accountability reflected in the U.S. Privacy Act of 1974 (applicable to federal agencies) and as laid out by the Organization for Economic Cooperation and Development. http://oecdprivacy.org/
[6]http://www.ntia.doc.gov/Privacy_multistakeholder_process_notice_of_open_meetings