Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Reining In Mobile App Privacy Practices

Law360, New York (January 25, 2013, 12:23 PM ET) -- Like parents shocked at exposes of their daughters partying for adult television cameras, regulators in 2012 made one disappointing discovery after another about mobile app privacy practices. Industry-wide, whether they are fun games, serious tools or educational resources, mobile apps continue to access, collect and use private data stored on smart devices while customers remain largely ignorant of and disempowered by these practices. Key reports issued this winter, coupled with recent enforcement actions, suggest that regulators are ready to insist that they and consumers no longer be subjected to these unpleasant revelations. The regulators' plea in 2013 is: "No more surprises … or you're grounded!"

Consumers Embrace Mobile Devices and Apps ...

Nearly 90 percent of Americans own a wireless phone and nearly half own a smartphone device.[1] Concomitantly, the number of devices that support mobile apps is increasing rapidly.[2] The expansive popularity of anytime, anywhere consumer services apps is resulting in an exponential increase in the collection and sharing of device users' personal data. There are 1.5 million apps available today[3] and another 1,600 new apps being published every day.[4] Many mobile apps can capture and share text messages, voicemail, voice memos, call logs, geotagged photos, videos and music. This information, when combined with unique mobile device IDs and a user's precise geolocation history, can recreate rich, minute-by-minute profiles of users' online and offline lives.

... But Do Not Want to Be Profiled or Monitored

Notwithstanding these grand data collection capabilities, recent studies suggest that consumers do not expect or wish to be monitored and profiled by their smart devices or by the apps loaded on them. A September 2012 Pew Research Center study reveals that 54 percent of app users decided not to install an app when they learned how much personal information would be collected by the app.[5] And, 30 percent of app users uninstalled an app after learning that it was collecting more personal information than they wished to share.[6] A report by the Berkeley Center for Law and Technology found a yawning gap between industry data collection and sharing practices and consumer privacy expectations in mobile media.[7]

In fact, 78 percent of Americans consider information on their mobile devices to be at least as private as data stored on their home computers.[8] A whopping 81 percent of the respondents would either definitely or probably not want to share social media contact lists stored on their devices in order to obtain more connections on a social media service. Even more so, 93 percent would not choose to share their personal contacts in order for a coupons app to send coupons to those people.[9] Another Berkeley Center report finds that a majority of respondents believe the slogan "Do Not Track" effectively means "do not collect information that allows companies to track them across the Internet."[10] The study did not target mobile apps, but the consumer sentiment is entirely relevant to data collection by mobile apps.

Industry Initiatives in Mobile Privacy Guidelines

The contrast between consumer expectations and the various practices frowned upon by regulators is not due to a lack of available industry guidance. For starters, the CTIA (The Wireless Association) has for some time offered guidelines for notice and consent in the deployment of location-based mobile services.[11] The GSM Association, a trade group representing the mobile industry, released "Privacy Guidelines for Mobile Application Development," which address the bulk of the notice, consent, transparency and control issues that trouble regulators, in February 2012.[12] The Mobile Marketing Association has also published a framework for the development of privacy disclosure statements in mobile apps.[13]

More recently, the Association for Competitive Technology, an organization representing small and mid-sized app developers and other technology firms, proposed a set of icons for use in disclosing privacy features in mobile apps.[14] And, since late 2011, a best practices guideline has been available that sets out recommendations which are in substance are quite close to the checklist recently propounded by the California attorneys general.[15] TRUSTe, a leading provider of website privacy certification seals, offers a fast track program for mobile apps to easily comply with regulatory expectations.[16] Finally, the speediest offering we have seen is the PrivacyChoice service that advertises a "state-of-the-art privacy statement for your app or site in about 10 minutes" through the use of an online wizard.[17]

Mind the Gap: Regulators Focus on the Disconnect Between Mobile App Practices and Consumer Expectations

Despite the numerous industry initiatives, there is an obvious overenthusiasm for customer data that has outstripped any industry or regulatory measures to promote transparent privacy practices and clear choices for consumers. This widening gap is the subject of several FTC reports and statements by the California AG.

The Federal Trade Commission has honed in on mobile apps for children and published its findings in two reports issued during 2012.[18] They are "Mobile Apps for Kids: Current Privacy Disclosures are Disappointing" (February 2012) and "Mobile Apps for Kids: Disclosures Still Not Making the Grade" (December 2012). The FTC has also hosted public workshops addressing advertising and payments issues in the "mobile ecosystem"[19] and released a major white paper on consumer privacy.[20] It has even published a high-level guidance for marketing mobile apps consistent with basic privacy principles previously stressed by the commission.[21]

On the other side of the nation, the California AG joins the regulatory triangulation on the mobile apps industry with this month's "Privacy on the Go: Recommendations for the Mobile Ecosystem."[22] This is the most comprehensive privacy guidance to date for mobile media issued by any state. While not law, the recommendations lay down a baseline compliance checklist for all mobile businesses subject to California's Online Privacy Protection Act ("CalOPPA"). [23] They will be an important reference point in ongoing industry and government efforts to establish national mobile privacy standards.

All of this guidance is a response to the agencies' findings that the actual practices of mobile apps are quite concerning from the perspective of consumer privacy. In the second "Mobile Apps for Kids" report, FTC staff reviewed a random selection of 400 kids' apps from the Apple Store and Google Play and exposed some stark patterns:

- Only 20 percent of reviewed apps contained any privacy-related disclosure on the app's promotion page, developer's website, or within the app itself.
- Privacy disclosures that did exist were long, technical, lacking useful details, rife with irrelevant details, or ambiguous.
- 56 percent of reviewed apps transmitted the user's device ID to ad networks, analytics companies or other third parties.[24]
- Some third parties ad networks and analytics companies receive data from many apps, thus gaining the potential to create detailed profiling through aggregation of data linked to unique device IDs.
- Whereas only 9 percent of reviewed apps disclosed the presence of in-app advertising, in reality 58 percent actually contained ads.
- Less than half of the apps with social media links actually disclosed the presence of such links.

The report concludes that the revealed practices may constitute violations of the Children's Online Privacy Protection Act ("COPPA")[25] or the FTC Act's prohibitions against unfair and deceptive trade practices.[26] While restrained in tone, the report resonates with disappointment at children's mobile app developers.

As it studies the industry, the FTC has also been actively pursuing specific investigations and enforcement. In September 2011, the FTC entered into its first consent decree[27] with a mobile app provider, W3 Innovations, which sold popular kids' apps without complying with any of COPPA's requirements.[28] That same month, the FTC signed consent agreements with the makers of AcneApp based on their unfounded health claims of healing acne with colored lights emitted from smartphones.[29] In October 2011, the FTC settled a case with a peer-to-peer file sharing app developer, Frostwire LLC, based on its apps that misled consumers about the extent to which their personal files would be shared with exposed to a millions-person network with barely any notice.[30]

Key Recommendations and Enforcement Steps by the California AG's Office

Across the nation, the California AG office's efforts parallel the FTC's move from study and guidance towards enforcement. In early 2012, the AG published a "Joint Statement of Principles"[31] with major mobile application platform providers (Amazon.com Inc., Apple Inc., Google Inc., Hewlett-Packard Co., Microsoft Corp. and Research in Motion). The joint statement was a shot across the bow to large players in the mobile apps industry, reminding them that CalOPPA, which requires operators of commercial websites to have compliant privacy disclosures, applies equally to mobile e-commerce. In June 2012, Facebook Inc. joined as a cosignatory to the joint statement.[32] Facebook also participated in a multistakeholder advisory group on mobile privacy practices led by the AG's office and the California Department of Office of Privacy Protection.

In October 2012, the office furthered its stance on privacy with notification letters to approximately 100 mobile app makers that they were not in compliance with CalOPPA and would be given 30 days to respond or comply. Despite acknowledging receipt of and intended compliance with this letter,[33] Delta Airlines did not correct its Fly Delta app's privacy deficiencies. As of December, its mobile app still did not include an app-specific privacy policy addressing the various form of personally identifiable information that it collected, including credit card and geolocation information. The AG immediately filed a complaint against Delta, requesting damages of $2,500 per violation, i.e. download of the app, as decreed by CalOPPA.[34]

On a broader scale, the AG sees a rosier view than the FTC. The joint statement industry signatories state that they have implemented the joint principles. From September 2011 to June 2012, the number of free Apple Store apps with a privacy policy doubled, from 40 percent to 84 percent, and those in Google Play rose from 70 percent to 76 percent.[35] Now, the attorney general, Kamala Harris, has encouraged the industry further by publishing the detailed privacy recommendations to all players in the "mobile ecosystem" — app developers, app platform providers, online advertising networks, operating system developers and carriers.

The thrust of the recommendations is: (1) to encourage the mobile industry to build fair information practice principles ("FIPPs")[36] into the design of mobile apps, devices and services, and (2) to enhance transparency in privacy disclosures and simplicity in user privacy controls. Its overarching goal is "surprise minimization" — 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 than 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 purported functions is central to the Recommendations.

The AG specifically recommends that mobile app developers undertake the following:

1) Identify, Identify, Identify

Developers must be clear on what their app is doing. What are all the types of personal data that an app will collect or disclose to third parties (including third-party software used in an app)? This includes, but is not limited to, unique device identifiers, geolocation data, mobile phone numbers, text messages, call logs, financial payment information, health and medical information, photos and videos, and browsing and download histories.

2) Check It Off

The recommendations and other sources provide checklists designed to smoke out data uses that may conflict with FIPPs or applicable privacy laws. A developer needs to be able to answer checklist questions for each data type or category, creating a thorough matrix of an app's data practices. For example:

- Is the data is necessary for the app's basic functionality or related business purposes such as billing?
- With whom will the data be shared?
- For what purpose will the data be shared?
- How will third parties use the shared data?
- What kind of access does the developer have to an app purchaser's device?
- Can the device owner modify these permissions?

3) Make Some Decisions

After considering its matrix of data needs, wants and excesses, app developers should establish their privacy practices. The recommendations cite several of the familiar FIPPs, such as transparency of data practices, limited data collection and retention, easily read and easily accessible privacy policies, 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.

4) Think Small

Given the screen constraints of mobile devices, the recommendations encourage developers to consider various methods that would be best suited to the app environment — icons, layered notices, grids, labels and dashboards for user-controlled privacy choices.

5) Go Above and Beyond

For apps that collect sensitive information (i.e., financial or health information) or personally identifiable information that is not related to app functionality, the recommendations suggest enhanced notification measures. "Special notices" would be short notices, delivered in real time, before data is collected, informing consumers of the impending collection of their information.

Some other specific guidance "tips" for privacy practices by app makers include:

- Use app-specific or other nonpersistent device identifiers when collecting data.
- Give users control over the collection of any personal data that is not needed for the functioning of the app.
- Offer default settings for controls which are privacy-protective.

Yes, You Too — Recommendations for App Platform Providers, Ad Networks and Other Market Participants

A resounding theme of the regulators is the necessity and interdependence of all mobile ecosystem participants in effecting adequate privacy protections for consumers. The recommendations emphasize that app platforms, mobile advertising networks, mobile operating system developers and mobile carriers need to play a role in protecting consumer privacy.

Platform providers can help consumers access an app's privacy disclosures before they download the app, supply the means for users to report complaints or ask questions about purchased apps, and further consumer education on mobile privacy. Mobile ad networks should provide their own privacy policies to developers who deliver their ads so that the apps can link to that policy in a pre-purchase notification. Operating system developers and mobile carriers should work together, among other purposes, to develop cross-platform standards for privacy controls and security patches.

Conclusion: It's Industry's Turn

Despite all the chastising, regulators are employing great efforts to support the app industry with clear and implementable guidance on consumer privacy. They do not, however, sufficiently address the business model of mobile apps, which, like the Internet, is driven by advertising rather than pay-for-play. The recommendations give a nod to this economic reality by focusing on "surprise minimization" and "special notices" rather than insisting on actual minimization of data collection and use.

Although it is not technically difficult to include app-specific privacy policies and user notifications, all the participants need to give more thought needs to how the industry can adapt its business paradigm to incorporate fair use principles. Given the abundance of tools and principles, developers and other industry players are sufficiently equipped to begin this process and thus hopefully avoid the external imposition of such a paradigm shift. The guidance and goals are there; it's time for industry to proactively incorporate privacy into its business model.

--By John B. Kennedy and Annie C. Bai, Wiggin and Dana LLP

John Kennedy is a partner and Annie Bai is a legal intern at Wiggin and Dana in Stamford, Conn.

[1] Aaron Smith, 46% of American Adults Are Smartphone Owners: Smartphone Users Now Outnumber Users of More Basic Mobile Phones Within the National Adult Population, Pew Internet & Am. Life Project (Mar. 1, 2012), http://pewinternet.org/Reports/2012/Smartphone-Update-2012.aspx.

[2] Kristen Purcell, Half of Adult Cell Phone Owners Have Apps on Their Phones, Pew Internet & Am. Life Project (Nov. 2, 2011), http://www.pewinternet.org/Reports/2011/Apps-update.aspx.

[3] Shara Tibken, Google Ties Apple with 700,000 Android Apps, C|NET (Oct. 30, 2012, 10:10 AM), http://news.cnet.com/8301-1035_3-57542502-94/google-ties-apple-with-700000-android-apps/.

[4] Wolfgang Gruener, Apple App Store to Reach 1M Apps This Year, Sort Of, Conceivably Tech (Aug. 9, 2012) http://www.conceivablytech.com/10283/business/apple-app-store-to-reach-1m-apps-this-year-sort-of.

[5] Jan Lauren Boyles, Aaron Smith, & Mary Madden, Privacy and Data Management on Mobile Devices, Pew Internet & Am. Life Project (Sept. 5, 2012), http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx.

[6] Id.

[7] Jennifer M. Urban, Chris Jay Hoofnagle & Su Li, Mobile Phones and Privacy, U.C. Berkeley Public Law Research Paper No., 2103405 (July 10, 2012), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103405.

[8] Id.

[9] Id.

[10] Chris Jay Hoofnagle, Jennifer M. Urban & Su Li, Privacy and Modern Advertising, U.C. Berkeley Center for Law & Technology Amsterdam Privacy Conference (Oct. 8, 2012), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103405.

[11] Best Practices and Guidelines for Location-Based Services, CTIA: The Wireless Ass'n (Mar. 20, 2010), http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf.

[12] Mobile and Privacy: Privacy Design Guidelines for Mobile Application Development (Feb. 2012), GSM Ass'n, http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/gsmaprivacydesignguidelinesformobileapplicationdevelopmentv1.pdf.

[13]Mobile Mktg. Ass'n Releases Final Privacy Guidelines for Mobile Apps, Mobile Mktg. Ass'n (Jan. 10, 2012, 8:44 PM), http://www.mmaglobal.com/news/mobile-marketing-association-releases-final-privacy-policy-guidelines-mobile-apps.

[14] ACT Introduces the App Privacy Icons, Ass'n for Competitive Tech. (Oct. 4, 2012, 3:02 PM), http://actonline.org/act-blog/archives/2674.

[15] Best Practices for Mobile Application Developers, Future of Privacy Forum & The Ctr. for Democracy and Tech. (Dec. 2011), https://www.cdt.org/files/pdfs/Best-Practices-Mobile-App-Developers.pdf.

[16] Mobile Privacy Certifications, TRUSTe (last visited Jan. 15, 2013), http://www.truste.com/products-and-services/enterprise-privacy/TRUSTed-mobile-apps.

[17] For Pros: Make Your Policy, Privacy Choice (last visited Jan. 15, 2013), http://www.privacychoice.org/policymaker.

[18] Mobile Apps for Kids: Current Privacy Disclosures are Disappointing, Fed. Trade Comm'n Staff Report (Feb. 2012), http://www.ftc.gov/opa/2012/02/mobileapps_kids.shtm. Mobile Apps for Kids: Disclosures Still Not Making the Grade, Fed. Trade Comm'n Staff Report (Dec. 2012), http://www.ftc.gov/opa/2012/12/kidsapp.shtm.

[19] In Short: Advertising and Privacy Disclosures in a Digital World, Fed. Trade Comm'n Workshop (May 30, 2012), http://www.ftc.gov/bcp/workshops/inshort/index.shtml. Paper, Plastic… or Mobile? An FTC Workshop on Mobile Payments, Fed. Trade Comm'n Workshop (Apr. 26, 2012), http://www.ftc.gov/bcp/workshops/mobilepayments/.

[20] Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, Fed. Trade Comm'n Report (Mar. 2012), http://www.ftc.gov/opa/2012/03/privacyframework.shtm.

[21] Marketing Your Mobile App: Get It Right From The Start, Fed. Trade Comm'n BCP Business Center (Aug. 2012), http://business.ftc.gov/documents/bus81-marketing-your-mobile-app (last viewed Jan. 15, 2013).

[22] Kamala D. Harris, Att. Gen., Privacy on the Go: Recommendations for the Mobile Ecosystem, Cal. Dep't of Justice (Jan. 2013), http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

[23] Cal. Online Privacy Protection Act, Cal. Bus. & Prof. Code §22575-22579 (2003).

[24] The report highlights that unique device IDs facilitate the aggregation of other types of personal information related to the same device, not just from the downloaded app, but from other sources, including other apps, thereby facilitating data-rich profiling of individuals.

[25] 15 U.S.C. §§ 6501–6506 (1998).

[26] 15 U.S.C. §§ 41-58 (1994).

[27] US v. W3 Innovations (D.Ct. N.Cal. 2011), case file at http://ftc.gov/os/caselist/1023251/index.shtm.

[28] Defendant W3 Innovations marketed several apps marketed to young children yet did not post a website privacy policy, did not obtain verifiable parental consent before embarking on its data practices, did not give parents meaningful consent choices and means of review, did not refrain from conditioning participation in the service on disclosure of the minimum of PII, and did not have reasonable security

procedures for protecting children's PII. The defendant paid a fine of $50,000, was required to delete all the children's personal information it had collected, and was subject to the FTC's record-keeping requirements for six years.

[29] In the Matter of Koby Brown, individually, and doing business as Dermapps, and Gregory W. Pearson, individually, and doing business as Dermapps, http://www.ftc.gov/opa/2011/09/acnecure.shtm

[30] Fed. Trade Comm'n v. Frostwire LLC, (Oct. 11, 2011), http://www.ftc.gov/opa/2011/10/frostwire.shtm.

[31] Kamala D. Harris, et al., Joint Statement of Principles, Cal. Off. of the Att. Gen. (Feb. 22, 2012), http://ag.ca.gov/cms_attachments/press/pdfs/n2630_signed_agreement.pdf

[32] Attorney General Kamala D. Harris Announces Expansion of California's Consumer Privacy Protections to Social Apps as Facebook Signs Apps Agreement, Cal. Off. of the Att. Gen. (June 22, 2012), http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-expansion-california's-consumer.

[33] California Attorney General Warns App Makers Over User Privacy, The Wash. Post: Bus. (Oct. 30, 2012, 4:39 PM), http://www.washingtonpost.com/blogs/post-tech/post/california-attorney-general-warns-app-makers-over-user-privacy/2012/10/30/33ac9afc-22cd-11e2-8448-81b1ce7d6978_blog.html.

[34] Complaint, Cal. v. Delta Air Lines, Inc., case no. CGC-12-526741 (filed Dec. 6, 2012), http://oag.ca.gov/system/files/attachments/press_releases/Delta%20Complaint_0.pdf#xml=http://search.doj.ca.gov:8004/AGSearch/isysquery/648131a4-eee2-4f06-a96b-5ebfa68cf212/1/hilite/.

[35] "Privacy on the Go" at 4.

[36] 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/