Bloomberg BNA

Privacy and Security Law Report®

Mobile Device Privacy

Significant developments in the mobile privacy space in 2013 include reports issued by the Federal Trade Commission and the California Office of the Attorney General. The authors provide an overview of the recommendations provided in these documents and break down the requirements between platform providers, application developers, and advertising networks and other third parties. Although the guidelines in these reports are only best practice recommendations, companies should heed them because those recommendations may evolve into standards, the authors advise.

Mobile Application Privacy: An Overview of the Recommendations From the FTC and the California Attorney General

By Lei Shen and Rebecca Eisner

Rebecca Eisner is a partner in Mayer Brown LLP's Chicago office, where she serves on the firm's Partnership Board. Lei Shen is an associate in the Business & Technology Sourcing practice group in Mayer Brown's Chicago office. Both of their practices focus on technology and business process outsourcing, information technology transactions, privacy, and security.

Introduction

Mobile technology raises new and unique privacy concerns due to the unprecedented amounts and types of personal information that a mobile device can collect. Unlike a computer, a mobile device is usually personal to and always on a person. Unlike traditional websites, mobile applications (''mobile apps'') can capture a broad range of personal information that is typically not found on personal computers, such as a user's geolocation, telephone call logs, and text messages, and can often collect this information automatically without the user's knowledge. As a result, consumer privacy on mobile devices has become an increasingly important issue, and mobile privacy has emerged as one of the key privacy topics this year.

Many states have recently introduced bills relating to mobile privacy. For example, a pair of new mobile privacy bills (H.B. 1608, S.B. 786) was recently introduced in Texas that, if passed, would require a warrant (as opposed to a subpoena) in order for law enforcement to obtain any location information (e.g., GPS or tower location data).[1] Additionally, numerous agencies and organizations—both public and private—have issued or plan to issue guidance for mobile privacy best practices, including the Federal Trade Commission, the Office of

the California Attorney General (''California AG''), and various private trade associations including the Digital Advertising Alliance[2] and the GSM Association (GSMA).[3]

Among the most significant of these developments are the mobile privacy reports recently released by both the FTC and the California AG Kamala Harris (D). The FTC's report, *Mobile Privacy Disclosures: Building Trust Though Transparency*,[4] and the California AG's report, *Privacy on the Go: Recommendations for the Mobile Ecosystem*,[5] both describe best practice recommendations for mobile privacy. The reports offer specific guidelines for participants in the mobile environment, including platform providers, application developers, and third-party service providers. The reports encourage companies to consider privacy from the outset, use ''just-in-time'' notices, provide clear privacy policies, and obtain express affirmative consent for the collection and sharing of certain data categories. The guidance from both reports shares common themes: provide transparency about an app's data practices, place limits on the collection and retention of data, and offer meaningful and informed privacy choices for users.

This article provides an overview of the recommendations provided by both the FTC and the California AG.

What the law currently defines and protects as personal information may not align with what many users consider to be private or personal information.

What Is Personal Information?

A mobile device provides access to a wide range of information about a user, including the user's geolocation, text messages, and photos. What the law currently defines and protects as personal information, however, may not align with what many users consider to be private or personal information. For example, the majority of database breach notification laws only define protected personal information as an individual's first name or first initial and last name plus one or more of the following data elements: (1) Social Security number; (2) driver's license number or state-issued ID card number; and (3) account number, credit card number, or debit card number combined with any security code, access code, PIN, or password needed to access that account.[6] Other privacy-related laws, such as the Health Insurance Portability and Accountability Act, only protect specific categories of personal information rather than a broad range of personal information (unlike, for example, in the European Union).[7]

The FTC, the California AG, and other organizations have started defining personal information to be much broader, especially as applied to the mobile space. For example, the California AG defines ''personally identifiable data'' as ''data linked to a person or persistently linked to a mobile device,'' including data that can identify a person via personal information or a device via a unique identifier.[8] The GSMA defines ''personal information'' as any data (i) collected directly from a user, (ii) about a user that is gathered indirectly (e.g., geolocation data, internet protocol address, International Mobile Station Equipment Identity number, and unique phone identifier), (iii) about a user's behavior (e.g., geolocation data, service and product use data, and website visits), or (iv) that is user-generated and held on a user's device (e.g., call logs, messages, photos, contact lists, or address books).[9] Generally, personal information in the mobile space includes a mobile device's unique device identifier, geolocation data, a user's name, mobile phone numbers, email addresses, text messages or email, call logs, address books, financial and payment information, health and medical information, photos or videos, web-browsing history, and lists of apps downloaded or used.[10]

In addition, a special subset of personal information called ''sensitive information'' is now also recognized. This subset of ''sensitive information'' is similar to the European Union's ''special categories of data'' described in its Data Protection Directive (95/46/EC).[11] In its recent report *Protecting Consumer Privacy in an Era of Rapid Change*, the FTC agreed that information concerning children, financial and health information, Social Security numbers, and precise geolocation data is

[1] H.B. 1608, 83rd Leg. (Tex. 2013), *available at* http://www.capitol.state.tx.us/tlodocs/83R/billtext/pdf/HB01608I.pdf#navpanes=0; S.B. 786, 83rd Leg. (Tex. 2013), *available at* http://www.capitol.state.tx.us/tlodocs/83R/billtext/pdf/SB00786I.pdf#navpanes=0.

[2] *See* Grant Gross, *Advertising Group Close to Mobile Privacy Guidelines*, PCWorld (June 5, 2013, 1:45 PM), http://www.pcworld.com/article/2040863/advertising-group-close-to-mobile-privacy-guidelines.html.

[3] GSMA, *Mobile Privacy Principles* 6, 7 (Jan. 2011), http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/gsmaprivacyprinciples2012.pdf.

[4] FTC, *Mobile Privacy Disclosures: Building Trust Though Transparency* (Feb. 2013), *available at* http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf (12 PVLR 166, 2/4/13).

[5] Cal. Att'y Gen. Office, *Privacy on the Go: Recommendations for the Mobile Ecosystem* (Jan. 2013), *available at* http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf (12 PVLR 80, 1/14/13).

[6] *See, e.g.*, Mass. Gen. Laws ch. 93H, *available at* https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93H.

[7] HIPAA defines ''health information'' as ''any information, whether oral or recorded in any form or medium, that—(A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.'' 42 U.S.C. § 1320d (1996).

[8] Cal. Att'y Gen. Office, *supra* note 5, at 6.

[9] GSMA, *supra* note 3, at 5.

[10] Cal. Att'y Gen. Office, *supra* note 5, at 8.

[11] The European Union recognizes certain ''special categories of data'' requiring extra restrictions, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and health or sex life. *See* Directive 95/46/EC, of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 8, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

  PVLR ISSN 1538-3423

sensitive and warrants special protection.[12] The California AG defines ''sensitive information'' as personally identifiable data about which users are likely to be concerned, such as precise geolocation data, financial and medical information, passwords, stored information such as contacts, photos and videos, and information about children.[13]

While these broader definitions of personal information are currently only guidelines and not enforceable law, they do provide insight into what may become law and thus protected information in the future.

Recommendations

Both the FTC and the California AG provide specific recommendations for various participants in the mobile environment:

Platform Providers

Provide Just-in-Time Disclosures: Platform providers are uniquely positioned to provide consistent disclosures across the apps that run on their platform. Consequently, they should provide clear and understandable ''just-in-time'' disclosures to users and obtain a user's affirmative express consent before allowing an app to access the user's sensitive information (such as geolocation data). The FTC believes that providing such just-in-time disclosures at the time it matters to consumers (i.e., just prior to the collection of data by the app) rather than being buried in a privacy policy will allow users to make more informed choices about whether to share such data.[14] The California AG also recommends using similar timely disclosures, which it describes as ''enhanced measures'' or ''special notices.''[15] These ''enhanced measures'' or ''special notices'' would highlight any unexpected data practices (e.g., apps collecting sensitive information or personal information that is not needed for its basic functionality) to enable the users to make more meaningful privacy choices.[16] While the California AG's recommendations are targeted to app developers rather than platform providers, it suggests calling attention to these unexpected data practices either by using special notices that are delivered just before collection of the specific data[17] or by using a combination of privacy controls and a short privacy statement highlighting these potentially unexpected practices.[18]

Use Privacy Dashboards and Icons: Platform providers should consider using dashboards, icons, and other visual cues to help users more easily and quickly recognize an app's privacy practices and settings. For example, if a Google Android app is obtaining a user's geolocation data, a geolocation icon displays on the top status bar of the device.[19] The FTC believes that having multiple disclosures at different points in time helps users determine which apps have access to what data and modify their privacy choices for those apps as desired.[20] While California's recommendations are targeted towards app developers rather than platform providers, the California AG adds that privacy icons and graphics are most effective if they are standardized and users are educated about them through an awareness campaign.[21]

Provide Access to Privacy Policies: Platform providers should provide a way for users to learn about an app's privacy policy prior to the user downloading the app, so that users will be able to make a more informed decision as to whether to download the app or not. Both the FTC and the California AG recommend doing this by making an app's privacy policy conspicuously accessible from the platform itself.[22] The California AG already made advancements this area in its 2012 agreement with leading platform providers, where the platform providers agreed to include in their app submission process an optional data field for the app developer to add either a link to, a copy of, or a short description of the app's privacy policy.[23]

Enforce Privacy Practices with App Developers: In addition to providing an area in the app store for developers to provide their privacy policies for their apps, the FTC recommends that platform providers (1) add provisions in their agreements with app developers requiring the developers to provide just-in-time disclosures and obtain affirmative consent before collecting sensitive information, and (2) reasonably enforce those provisions.[24]

Provide Transparency About the Platform's App Review Process: The FTC recommends that platform providers clearly disclose the extent to which they review an app before making it available for download, including any compliance checks they perform.[25] This recommendation likely stems from the FTC's complaint against Facebook Inc., in which the FTC charged Facebook with deceiving users through Facebook's ''Verified Apps'' program.[26] Facebook claimed it certified the security of apps participating in the program, when it actually did not.

Develop a Do Not Track System: The FTC had previously recommended the development of a Do Not Track system for web browsers that would enable users to avoid having their actions monitored online.[27] Applying this same principle to the mobile space, the FTC recom-

[12] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* 59 (Mar. 2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf (11 PVLR 590, 4/2/12).

[13] Cal. Att'y Gen. Office, *supra* note 5, at 6.

[14] FTC, *Mobile Privacy Disclosures*, *supra* note 4, at 15–16.

[15] Cal. Att'y Gen. Office, *supra* note 5, at 9.

[16] *Id.*

[17] *Id.* at 12.

[18] *Id.* at 13.

[19] FTC, *Mobile Privacy Disclosures*, *supra* note 4, at 17–18.

[20] *Id.* at 16–17.

[21] Cal. Att'y Gen. Office, *supra* note 5, at 11.

[22] *Id.* at 14; FTC, *Mobile Privacy Disclosures*, *supra* note 4, at 22.

[23] Press Release, Cal. Att'y Gen. Office, Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications (Feb. 22, 2012), *available at* https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy (11 PVLR 375, 2/27/12).

[24] FTC, *Mobile Privacy Disclosures*, *supra* note 4, at 18–19.

[25] *Id.* at 20.

[26] *See* Press Release, FTC, Facebook Settles FTC Charges That It Deceived Consumers By Failing to Keep Privacy Promises (Nov. 29, 2011), *available at* http://ftc.gov/opa/2011/11/privacysettlement.shtm (10 PVLR 1759, 12/5/11).

[27] *See* Press Release, FTC, FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers (Dec. 1, 2010), *available at* http://www.ftc.gov/opa/2010/12/privacyreport.shtm (9 PVLR 1642, 12/6/10); Press Release, FTC, FTC Issues Final Commission Report on Protecting Consumer Privacy (Mar. 26, 2012), *available at* http://www.ftc.gov/opa/2012/03/privacyframework.shtm.

mends that platform providers develop a Do Not Track mechanism at the platform level so that users can choose to prevent apps from tracking their behavior across apps and transmitting such information to third parties. An effective Do Not Track system should be (1) universal, (2) easy to find and use, (3) persistent, (4) effective and enforceable, and (5) limit collection of data, not just its use to serve advertisements.[28]

App Developers

Provide a Clear, Accurate and Conspicuously Available Privacy Policy: One of the most important recommendations (and in California's case, requirement) from the reports is for app developers to have a clear and accurate privacy policy for their mobile app that is made conspicuously available. The privacy policy should clearly identify the app's data practices, and important terms should not be buried in long agreements or behind vague links. Among the data practices that the privacy policy should cover include how the user's data will be collected, used, shared, disclosed, and retained. The California AG recommends discussing at least the following topics: (1) the types or categories of personal information collected by the app; (2) the uses and retention period for each type or category of personal information; (3) whether the app, or a third party, collects payment information for in-app purchases; (4) the categories of third parties with whom the app may share personal information (such as advertising networks); (5) the choices the user has regarding collection, use, and sharing of personal information; (6) the process for a user to review and request corrections to his personal information maintained by the app, if available; (7) the way users can contact the app developer with questions or concerns; and (8) the effective date of the privacy policy and the process for notifying users of material changes to it.[29] The Mobile Marketing Association provides a model privacy policy framework that provides guidelines to help app developers draft a privacy policy.[30]

An app developer should ensure that any promises made in the privacy policy are true and accurate. The FTC has taken action against many companies that claimed to safeguard the privacy or security of their users' information but did not meet those promises.[31]

Finally, the privacy policy should be conspicuously available and easy to read on a mobile device. The California AG recommends having the privacy policy available both from the app platform (before the app is downloaded and any data are collected) and from within the app.[32] While the small screen of a mobile device presents challenges in displaying privacy policies, app developers can consider using a layered privacy policy format that summarizes the most relevant privacy practices on top.[33]

It is important to note that California has a law (the California Online Privacy Protection Act, or ''CalOPPA'') requiring mobile apps that collect personal information to conspicuously post a privacy policy, and the California AG has started enforcing its compliance. For example, in late 2012, the California AG filed a lawsuit against Delta Air Lines Inc. for failing to post a privacy policy for its ''Fly Delta'' app.[34] Although a California judge recently dismissed the lawsuit on unrelated grounds, the setback is unlikely to deter the California AG from pursuing other companies that do not comply.[35]

Use Just-In-Time Disclosures: While the FTC also has recommendations for platform providers regarding just-in-time disclosures, it realizes that an app's access to and disclosure of sensitive information may not be within a platform's control. To reconcile this, the FTC recommends that app developers provide just-in-time disclosures to users and obtain their affirmative express consent before accessing or sharing any sensitive information outside of a platform's Application Programming Interface or control (e.g., if an app will be collecting financial, health, or children's data, or if it will be sharing sensitive information with third parties).[36] These app-level disclosures should not repeat the platform-level disclosure and consent process. For example, if an app collects geolocation data, the FTC states that the app should be able to rely on the platform's disclosure to the user that it will be collected and should not have to repeat the disclosure and again obtain user consent. However, if the app developer will be using the sensitive data in ways outside the platform's control, then the app developer should provide just-in-time disclosures and obtain affirmative consent from the user.

The most efficient and effective way to incorporate privacy into an app is to consider it at the outset of the app's development process.

Understand Any Third-Party Code Included in the App: Even if an app developer provides clear and accurate disclosures about its own privacy practices in its privacy policy, app developers often include third-party code in their apps (e.g., from ad networks or analytics companies) without fully understanding what information that code may be collecting or sharing. In order to provide a complete and accurate disclosure to users, app developers should coordinate with ad networks and

[28] FTC, *Mobile Privacy Disclosures*, *supra* note 4, at 20–21.

[29] Cal. Att'y Gen. Office, *supra* note 5, at 11.

[30] *See* Press Release, Mobile Marketing Ass'n, Mobile Marketing Association Releases Final Privacy Policy Guidelines for Mobile Apps, MMA (Jan. 24, 2012), http://www.mmaglobal.com/news/mobile-marketing-association-releases-final-privacy-policy-guidelines-mobile-apps (11 PVLR 248, 2/6/12).

[31] *See, e.g.*, FTC, *Making Sure Companies Keep Their Privacy Promises to Consumers*, http://www.ftc.gov/opa/reporter/privacy/privacypromises.shtml (last visited June 16, 2013) (listing several legal actions that the FTC has taken against organizations for misleading them with inaccurate privacy or security promises).

[32] Cal. Att'y Gen. Office, *supra* note 5, at 9.

[33] *Id.* at 11.

[34] Complaint, *People v. Delta Air Lines Inc.*, No. CGC-12-526741 (Cal. Super. Ct. Dec. 6, 2012) (11 PVLR 1776, 12/10/12).

[35] *See, e.g.*, Kurt Orzeck, *Delta Dodges Calif. Privacy Suit Over Smartphone App*, Law360 (May 9, 2013, 10:09 PM), http://www.law360.com/california/articles/440392/delta-dodges-calif-privacy-suit-over-smartphone-app (12 PVLR 835, 5/13/13).

[36] FTC, *Mobile Privacy Disclosures*, *supra* note 4, at 23.

  PVLR ISSN 1538-3423

other third parties to fully understand the function of any third-party code being utilized in their apps.[37]

Limit Collection of Personal Information: The most efficient and effective way to incorporate privacy into an app is to consider it at the outset of the app's development process. As the FTC recommended with its privacy by design principle described in its report *Protecting Consumer Privacy in an Era of Rapid Change*, app developers should build privacy considerations and protections into their apps from the beginning.[38] This includes limiting the amount of personal information an app collects (such as minimizing the collection of information not necessary for the app's basic functionality), collecting or sharing sensitive information only with consent, and limiting the retention of data to the time necessary to support the app's functionality or satisfy any legal requirements.[39] Apps should also utilize appropriate security safeguards (including the use of encryption) to protect any personal information they collect from unauthorized access, use, disclosure, modification, or destruction.[40]

Advertising Networks and Other Third Parties[41]

As discussed above, app developers often include code from advertising networks and other third parties without fully understanding what personal information that code may be collecting or sharing. As a result, the FTC recommends advertising networks and other third parties that provide services for apps improve their communication with app developers (for example, by helping app developers understand what their code does and how it works, or by having a privacy policy and providing it to app developers). App developers would then be able to provide users with more complete and accurate disclosures.[42] In addition, the California AG recommends advertising networks avoid delivering any ads outside of the app, such as by placing icons on the mobile desktop, and use enhanced measures and obtain prior consent before accessing any personal information.[43]

Conclusion

While both the FTC and the California AG have stated that the guidelines in these reports are only best practice recommendations and not binding law,[44] these recommendations are likely a sign of things to come. The recommendations may evolve into standards, and companies that fail to heed them may become subject to investigations and enforcement actions in the future.

---

[37] *Id.* at 24.

[38] FTC, *Protecting Consumer Privacy*, *supra* note 12, at 22.

[39] Cal. Att'y Gen. Office, *supra* note 5, at 9.

[40] *Id.* at 10.

[41] Note that while the FTC report also provided recommendations for app trade associations, and the California AG's report also provided recommendations for operation system developers and mobile carriers. *See, e.g.*, *id.* at 16.

[42] FTC, *Mobile Privacy Disclosures*, *supra* note 4, at 24.

[43] Cal. Att'y Gen. Office, *supra* note 5, at 15.

[44] *See, e.g.*, *id.* at 4; FTC, *Mobile Privacy Disclosures*, *supra* note 4, at 13–14.