Westlaw Journal
COMPUTER & INTERNET
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 30, ISSUE 21 / MARCH 22, 2013

Expert Analysis

The FTC and Mobile Privacy

By John L. Hines Jr., Esq., and Jennifer Woods, Esq.
Clark Hill PLC

On Feb. 1 the Federal Trade Commission released its most recent privacy report titled "Mobile Privacy Disclosures: Building Trust Through Transparency."[1] In its report, the FTC provides recommendations for platforms, application developers, advertising networks, mobile app-related trade associations and other third parties to encourage development of efficient and effective mobile privacy disclosures. While the report provides some hints as to the FTC's enforcement priorities in the mobile privacy sphere, stakeholders looking for regulatory certainty will likely be disappointed. However, combining the FTC's previous guidelines and more established concepts of Internet-based privacy with the report's recommendations helps provide some predictability for mobile app developers and other stakeholders who face the challenge of adopting effective privacy disclosures in an era of rapidly evolving technology.

THE TECHNICAL LANDSCAPE

The process to develop a mobile app typically involves interaction between app developers, platforms and a variety of third parties. Simply described, mobile platforms, such as Android (owned by Google), iOS6 (owned by Apple), Windows Phone OS (owned by Microsoft) and BB10 (owned by Blackberry), each offer their own unique "application programming interfaces, or APIs, which developers use to create apps that are compatible with a given platform. Developers write code that implements desired functionalities, which may include code created by third parties to facilitate credit card transactions or to implement in-app advertising, for example. Completed apps are then submitted to the platform for publishing. The platform typically reviews the app and may reject it for a number of reasons, including failure to adhere to technical specifications, unauthorized use of registered trademarks or inclusion of objectionable content.[2] Once published, apps are available for public purchase through the platforms' respective app stores.

About 90 percent of Americans own mobile phones, and nearly 50 percent own a smartphone that is capable of downloading apps.[3] Moreover, smartphone use is projected to increase dramatically over the next several years.[4] Mobile apps, which did not exist even a decade ago, are increasingly becoming a way of life for Americans. The number and variety of mobile apps have likewise exploded to include those that simplify online banking, permit access to medical histories and allow individuals to announce where they are. As technology develops, more and more apps amass an

unprecedented amount of data regarding an individual's day-to-day activities, raising privacy concerns for users.[5]

FTC'S PRIVACY PRINCIPALS

The FTC, which continues to be highly focused on data protection matters, has articulated basic privacy principles that are applicable to all entities collecting information from consumers on the Internet. For example, the FTC has encouraged all stakeholders, including Web and mobile app developers and other industry participants to implement "privacy by design."[6] This concept requires stakeholders and industry participants to think about data collection and storage needs early in the development process so they can build in privacy safeguards and meet regulatory requirements from the start. Additionally, all stakeholders should take into account, as applicable, sector-specific privacy laws, including the Children's Online Privacy Protection Act, or COPPA, the Health Insurance Portability and Accountability Act, or HIPAA, and the Gramm-Leach-Bliley Act. All apply to the mobile environment.

As technology develops, more and more apps amass an unprecedented amount of data regarding an individual's day-to-day activities, raising privacy concerns for users.

While general privacy principles are frequently commonsense-based and often well established, mobile app developers have been particularly slow in adopting their recommended practices. It is noteworthy that, as of June 2012, more than half of all apps available on the iTunes app store, and about 80 percent of all apps in the Google Play store did not provide a privacy policy on the mobile app download page.[7] The FTC notes that all mobile apps should have privacy policies, and the agency credits the California Online Privacy Protection Act — interpreted to require such policies for any app that collects personal information — with expediting some apps' adoption of appropriate disclosures.[8]

In theory, regulators could simply require that mobile app developers to disclose their data collection and include privacy policies within their apps, but studies indicate that a more nuanced approach to mobile privacy is required to ensure meaningful disclosures in this environment. Specifically, these studies suggest a disconnect between consumers' preferences regarding mobile apps' data collection and tracking and what users do in practice. Consumers are often surprised to discover the extent to which apps collect personal data, even when the developers disclose this information, suggesting that app privacy disclosures are not well understood by the public.[9]

Recognizing this increasing disconnect, the FTC's mobile report contains a list of recommendations for improved data collection and other privacy-related disclosures for each of the various stakeholders, including:

- Mobile app platforms
- Developers
- Advertising networks
- Trade associations and research entities.

Ultimately, the FTC envisions that the stakeholders' cooperation will yield efficient and effective privacy disclosures that provide meaningful information to consumers at multiple stages in the downloading and use of apps.

Platforms

The FTC views the mobile app platforms as gatekeepers that could ensure that only apps with appropriate privacy disclosures are allowed to be sold to the public.

In particular, with their APIs, these platforms are in a unique position to encode functionality that would require app developers to provide consistent privacy disclosures for all apps on the platform.[10] Similarly, platform APIs' licensing and guidelines could be used to educate small app developers who are not well versed in privacy issues. Platforms are also in a position to implement privacy "dashboards" that allow consumers to review the privacy disclosures of all apps installed on a particular device in one place and make ongoing decisions regarding their app usage.[11] Perhaps most significantly, the FTC Mobile Report also suggests that platforms should revise their contracts with app developers to require that app developers include privacy policies, obtain verifiable consent before collecting sensitive information and regulate disclosure of data to third-parties.[12]

The FTC Mobile Report supports the inclusion of do-not-track, or DNT, options to prevent data collectors, such as third-party advertising networks, from assembling a profile of a given app user.[13] The most logical place to locate this feature, in the FTC's estimation, is at the platform level, so that consumers are able to make one-time choices regarding app tracking, instead of having to select an option within each app.[14]

Developers

As of June 2012, more than half of all apps available on the iTunes app store and about 80 percent of all apps in the Google Play store did not provide a privacy policy on the mobile app download page.

While platforms may require all apps using their APIs to include privacy policies, the bulk of the work in constructing appropriate and effective privacy disclosures necessarily falls to app developers. App developers must work not just to understand the importance of privacy disclosures but also must ensure that mobile app privacy policies accurately reflect the data collection and disclosure policies of all parties involved, including third-party service providers. As a preliminary matter, the FTC report suggests that mobile app privacy policies must accurately and completely describe the app developer's data collection and disclosure practices, including those of third-party developers that provide code for in-app advertising or analytics services. The report suggests that app developers must strive to understand how third-parties use the information collected and make appropriate disclosures to their users. Additionally, app developers should work to understand when disclosures are most likely to provide meaningful information to consumers and time their disclosures accordingly.[15]

In an attempt to encourage the use of meaningful privacy disclosures, the FTC encourages mobile app developers to utilize several techniques when drafting and implementing privacy policies. Because website privacy policies tend to translate poorly to mobile devices' smaller screens, the FTC encourages the use of layered disclosures. In a layered disclosure, the app developer first provides concise statements of the app's privacy practices, such as "we share personal information with third-party advertisers," or "we link to third-party sites." Each of the brief statements then offers the consumer the opportunity to read more information regarding particular areas of interest in the second layer of disclosures: the full privacy policy.

Similarly, the report emphasizes the importance of providing consumers with privacy disclosures that are meaningful in a particular context. While many apps present the consumer with a summary of privacy practices prior to the consumer downloading the app, such disclosures are not necessarily understood or remembered in a manner that permits the consumer to exercise meaningful choice in consenting to data collection. To improve the usefulness of disclosures for consumers, the report recommends using "just in time" disclosures, or disclosures that are presented to a consumer immediately

prior to the activity relevant to the disclosure. For example, an app might provide a consumer with a notice concerning collection of geo-location data right before the app opens a map showing the consumer's location. The FTC envisions these disclosures being provided at the platform level, though the report recommends that the app developer provide them if a platform does not.[16]

Other industry players

Industry participants have shown an increasing willingness to create industry best practices regarding data collection and mobile privacy disclosures, though such practices are voluntary and have yet to achieve widespread adoption. The FTC Mobile Report encourages further development of "industry best" practices, including standardized-form privacy policies for app developers and "short form" disclosures, such as icons, so consumers can more readily compare data practices across apps in a similar way to the nutrition labels on food products. At the same time, the FTC cautions that any such improvements on current mobile app disclosures must be meaningful to consumers and avoid oversimplification. Additionally, the agency envisions industry participants helping to educate app developers on privacy issues, including the implementation of industry-recommended best practices.

ENFORCEMENT

In addition to providing policy recommendations like those in the report, the FTC continues to make privacy issues an enforcement priority as demonstrated by its announcement of the report in connection with an enforcement action specific to the mobile app environment. *United States v. Path Inc.* involved Path, a website with a corresponding app that allows individuals to diary their daily experiences and share them with friends.[17] In its complaint, the FTC alleged that Path violated knowingly permitted more than 3,000 children under age 13 to use the app without first obtaining verifiable parental consent, in violation of COPPA. Additionally, the agency alleged that Path engaged in unfair and deceptive practices in violation of Section 5 of the FTC Act by harvesting users' cell phone contacts information, even where users specifically declined to permit such harvesting. In early February the FTC entered into a consent decree with Path in which the company agreed to pay an $800,000 fine and undertake 20 years of independent privacy assessments that must be reported to the FTC.[18]

CONCLUSION

While the FTC Mobile Report provides some direction for app developers, platforms and other industry participants, the lack of concrete requirements necessarily limits predictability.[19] However, recent FTC enforcement actions demonstrate that the agency will continue to make privacy a priority. By providing accurate and clear privacy disclosures, mobile app providers can avoid the scrutiny of the FTC while allowing consumers to make educated decisions regarding the apps they download.

NOTES

[1] Federal Trade Commission, Mobile Privacy Disclosures: Building Trust Through Transparency ("FTC Mobile Report") (Feb. 2013), *available at* www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf. In addition to the FTC's rulemaking authority under a number of federal statutes, the FTC has the authority to provide industry guidance in several forms, including advisory opinions, staff opinions and reports. While this type of industry guidance (including the FTC Mobile Report) does not have the force of law, one can generally expect the FTC to rely on it in determining enforcement priorities. *See* FTC Administrative Staff Operating Manual, *available at* http://www.ftc.gov/foia/adminstaffmanuals.shtm.

[2] *See, e.g.*, Google's Onsite Application Developer Guide, *available at* https://developers.google.com/orkut/docs/on-site-apps/submission#wait_4_approval. A list of common reasons for Apple's

refusal to publish apps, and accompanying explanations, is *available at* http://appreview.tumblr.com/.

[3] John B. Kennedy and Annie C. Bai, Apps Gone Wild? *The FTC and California AG Seek to Rein in Mobile App Privacy Practices*, The Privacy Advisor, Feb. 4, 2013, *available at* https://www.privacyassociation.org/publications/2013_03_01_apps_gone_wild_the_ftc_and_california_ag_seek_to_rein_in_mobile.

[4] *See, e.g.*, Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017, *available at* http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html

[5] Joseph Menn, *Data Collection Arms Race Feeds Privacy Fears*, Reuters, Feb. 19, 2012, *available at* http://www.reuters.com/article/2012/02/19/us-data-collection idUSTRE81I0AP20120219.

[6] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers (Mar. 2012), at 1, 22-23.

[7] FTC Mobile Report, *supra* note 1 at 23, n. 96.

[8] California Online Privacy Protection Act, Business Code § 22575, *see* also Office of the Attorney General, State of California, Joint Statement of Principles, Feb. 22, 2013, *available at* ag.ca.gov/cms_attachments/press/.../n2630_signed_agreement.pdf. While recent efforts by the California State Attorney General's Office to enforce its mobile privacy law may have some effect on these percentages, progress to date has been slow.

[9] See, e.g., Patrick Gage Kelley, *Designing a Privacy Label: Assisting Consumer Understanding of Online Privacy Practices,* April 2009, available at cups.cs.cmu.edu/privacyLabel/files/CHI-finalAbstract.pdf; Bob Sullivan, A Shock in the Dark: Flashlight App Tracks Your Location, NBC News, Jan. 16, 2013, available at http://redtape.nbcnews.com/_news/2013/01/16/16530607-a-shock-in-the-dark-flashlight-app-tracks-your-location?lite.

[10] *See, e.g.*, Geoffrey A. Fowler, *Tech Giants Agree to Deal on Privacy Policies for Apps*, WSJ, Feb. 23, 2012, *available at* http://online.wsj.com/article/SB10001424052970203918304577239650306276074.html.

[11] The FTC envisions privacy "dashboards" driven either by applications or by content elements. Google and Apple have implemented a different version of this dashboard: Google focuses on applications, while Apple focuses on individual content elements. Apple's iOS6 contains a "privacy settings" tab showing different categories of data, such as geo-location, contacts, etc., which permit a user to see which apps access each type of information. Google's dashboard allows the user to access information for each app individually, allowing the user to see which categories of information a particular app collects. *See* FTC Mobile Report, *supra* note 1 at 16.

[12] FTC Mobile Report, *supra* note 1 at 19.

[13] "Do Not Track" is a concept pointing to a bundle of existing and proposed technologies and prohibitions that purport to prevent or limit third-party advertisers from tracking the user's Web browsing habits through cookies or other technologies. Due to the differing platform and browser technologies and ad network self-regulatory prohibitions and responses, the practical effect of a consumer's choice to activate a Do Not Track feature requires careful investigation. This seems to underlie the FTC's case for clear disclosure and ease of implementation of DNT in mobile. For more information regarding the current state of the Do Not Track initiative in the context of Web browsers, *see* Lee Matthews, *The State of Do Not Track in Web Browsers*, Geek.com, Mar. 5, 2013, *available at* http://www.geek.com/articles/geek-pick/the-state-of-do-not-track-in-web-browsers-2013035/.

[14] FTC Mobile Report, *supra* note 1 at 21. Although DNT has traditionally been a difficult subject, with advertising networks and browsers unable to reach agreement as to the scope and opt-out/opt-in requirements of a DNT feature, the FTC notes Apple's development of a "Limit Ad Tracking" feature as an encouraging step toward a universal DNT option for mobile apps. *See* Matthews, *supra* note 13; FTC Mobile Report, *supra* note 1 at 21.

[15] *Id*. at 24.

[16] *Id*. at ii, 23.

[17] No. 13-0448, *complaint filed* (N.D. Cal., S.F. Div. Jan. 31, 2013).

[18] Federal Trade Commission, Press Release, Path Social Networking App Settles FTC Charges it Deceived Consumers & Improperly Collected Personal Information from Users' Mobile Address Books, *available at* http://www.ftc.gov/opa/2013/02/path.shtm. *See* also, *United States v. Path Inc.*, No. 13-0448, *consent order issued* (N.D. Cal., S.F. Div. Feb. 8, 2013). Mobile stakeholders should also anticipate increased state enforcement. California has not been shy in enforcing its law, sending out 100 notices to companies that were not in compliance and filing suit against Delta Airlines. Christine Mai-Duc, California Sues Delta Air Lines Over Mobile App Privacy Policy,

LA Times, Dec. 6, 2012, *available at* http://articles.latimes.com/2012/dec/06/business/la-fi-tn-california-sues-delta-airlines-over-mobile app-privacy-policy-20121206.

[19] It may be useful to read the FTC Mobile Report in connection with the more specific and concrete recommendations provided by the California State Attorney General in its January 2013 report. *See* California Attorney General, Privacy on the Go: Recommendations for the Mobile Ecosystem (Jan. 2013), *available at* oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

(L) **John L. Hines Jr**. is a partner at **Clark Hill PLC**, where he concentrates his practice on intellectual property and licensing, Internet law and e-commerce, software applications (including open-source licensing) cloud computing, and information management. He counsels clients on privacy and data security compliance, document retention policies and practices, reputation management, and social media. He can be reached at jhines@clarkhill.com. (R) **Jennifer Woods**, an attorney at the firm, practices primarily in the areas of intellectual property, including trademark, copyright and licensing matters, and Internet and e-commerce, with a particular emphasis on privacy and data security. She can be reached at JWoods@ClarkHill.com