WILMERHALE

FTC Issues Mobile Privacy Disclosures Report

2013-02-04

In the latest in a series of efforts by federal and state regulators to improve privacy practices in the exponentially growing industry of applications ("apps") for mobile devices such as smartphones and tablets, the Federal Trade Commission ("FTC") issued a staff report last Friday recommending best practices for mobile app privacy disclosures.[1] While the report, *Mobile Privacy Disclosures: Building Trust Through Transparency*, offers only recommendations, it both suggests areas that may be targets for future FTC enforcement actions and reflects the accelerating efforts of a growing number of regulators to police privacy in the mobile domain.

Overview of the Report

The report sets out "best practice recommendations" for each of the main participants in the mobile ecosystem: mobile platform/operating system providers,[2] app developers,[3] advertising networks,[4] and app developer trade associations.[5]

- **Platform/operating system providers**. Taking the view that mobile platform/operating system providers serve as the gatekeepers for apps accessible through their stores, the report places considerable responsibility for protecting consumer privacy on them.[6] It recommends that platform/operating system providers give "just-in-time" disclosures to consumers, *i.e.*, just prior to collection of geolocation or other sensitive information by apps, and obtain affirmative express consent from consumers prior to such collection.[7] The report also suggests system-wide means of providing privacy information to consumers, such as a "dashboard" where consumers can review the types of content accessed by their apps[8] or standardized icons to depict the transmission of user data.[9] The report urges platforms to provide clear disclosures about their methods for reviewing apps.[10] And it recommends development of a "Do Not Track" mechanism that would allow consumers to use a platform-wide setting to prevent advertisers from developing user profiles by tracking consumers across different apps.[11]
- **App developers**. The report recommends that app developers adopt clearly stated privacy policies and make them readily available.[12] It also recommends that app developers provide just-in-time disclosures and obtain express consent when collecting sensitive information— such as financial, health or children's data—outside a platform's application

programming interface ("API"), or when sharing sensitive data with third parties.[13] And it urges app developers to coordinate with ad networks and other third-party service providers to ensure that apps can give accurate disclosures to consumers.[14]

- **Advertising networks**. The report recommends that ad networks and analytics providers ensure that app developers understand how the code these third parties supply to app developers functions, particularly with respect to data collection, analysis, and sharing. The report also urges ad network operators to work with platforms to help implement a Do Not Track system for the mobile domain.[15]
- **Trade associations**. The report urges app developer trade associations to take the lead in developing standardized icons to depict privacy practices, "badges," or other short, standardized disclosures for apps, as well as standard privacy policies.[16]

Context and Implications

1. The FTC's *Mobile Privacy Disclosures Report* joins a growing array of efforts by federal and state regulators to improve online privacy protections, particularly in the mobile ecosystem.

- First, the report follows a number of recent FTC reports and enforcement actions directed at online privacy and privacy in the mobile domain in particular.[17] The report acknowledges that disclosures represent only one element of privacy protection, and it notes that the Commission will shortly be issuing updated guidance on advertising disclosures.[18] We are likely to see continued expansion of the FTC's online privacy initiatives in the year ahead.
- Second, the FTC is not the only federal player in this space. The Commerce Department's National Telecommunications and Information Administration ("NTIA") began a "privacy multistakeholder process" in June 2012 to bring together industry, consumer advocacy, academic, and government representatives to develop mobile privacy codes of conduct.[19] The FTC characterizes the *Mobile Privacy Disclosures* report in part as an effort to contribute to that process and shape the resulting codes of conduct.[20]
- Third, when it comes to mobile privacy, the FTC appears to be in something of a regulatory competition with the California Attorney General's Office. The California AG reached a settlement in February 2012 with the leading platform providers to improve their privacy practices,[21] beat the FTC into print with its own set of recommendations for privacy in the mobile domain,[22] and has begun to follow through on its announced intention to step up enforcement of California's Online Privacy Protection Act.[23] Whether this competition will promote quicker development of uniform standards or lead to a harmful proliferation of divergent standards remains to be seen.

2. Although the *Mobile Privacy Disclosures Report* offers only recommendations, it does contain some hints about possible FTC enforcement priorities in the mobile domain. For example, it suggests that the FTC will police carefully apps that collect sensitive information, and it indicates that the codes of conduct that emerge from the NTIA multistakeholder process may provide a baseline or safe harbor for FTC enforcement actions.[24]

---

[1]Federal Trade Commission, *Mobile Privacy Disclosures: Building Trust Through Transparency* (2013), *available at* http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf ("Mobile Privacy Disclosures Report"). The report was approved by the Commissioners 4-0, with one member not participating.

[2]*Id*. at 14-21; *see also id*. at 11-12. "Platform" refers to "mobile operating systems, such as Apple's iOS, Google's Android, RIM's Blackberry OS, and Microsoft's Windows Phone, along with the app stores they offer, such as the Apple App Store, Google Play, Blackberry App World, and Microsoft's Window's Store." *Id*. at 1 n.3.

[3]*Id.* at 22-24.

[4]*Id*. at 24-25.

[5]*Id*. at 25-28.

[6] The report notes that this approach is somewhat different than the approach taken in the FTC's recently updated regulations under the Children's Online Privacy Protection Act. *Id*. at 15 n.70.

[7]*Id*. at 15-16.

[8]*Id*. at 16-17.

[9]*Id*. at 17-18.

[10]*Id*. at 20.

[11]*Id*. at 20-21.

[12]*Id*. at 22-23.

[13]*Id*. at 23-24.

[14]*Id*. at 24.

[15]*Id*. at 24-25.

[16]*Id*. at 25-28.

[17]*See, e.g.*, Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers* (Mar. 2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf; Federal Trade Commission, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Feb. 2012), *available at*

http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf; Federal Trade Commission, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (Dec. 2012), *available at* http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf; Press Release, Federal Trade Commission, Marketers of Criminal Background Screening Reports To Settle FTC Charges They Violated Fair Credit Reporting Act (Jan. 10, 2013), *available at* http://www.ftc.gov/opa/2013/01/filiquarian.shtm. The FTC recently updated the regulations implementing the Children's Online Privacy Protection Act. See earlier alert.

[18]*Mobile Privacy Disclosures Report* at 1 & nn.1-2.

[19] A description of the NTIA process can be found at: http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency.

[20]*Mobile Privacy Disclosures Report* at iii.

[21]*See* Joint Statement of Principles, California Attorney General Kamala D. Harris (Feb. 22, 2012), *available at* http://ag.ca.gov/cms_attachments/press/pdfs/n2630_signed_agreement.pdf. *See also* Press Release, California Attorney General's Office, *Attorney General Kamala D. Harris Announces Expansion of California's Consumer Privacy Protections to Social Apps as Facebook Signs Apps Agreement* (June 22, 2012), *available at* http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-expansion-california%E2%80%99s-consumer.

[22] California Attorney General, *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. Many in the mobile apps industry criticized the California AG's report, arguing that some of the recommendations clash with developing industry standards and have no basis in existing law. *See, e.g.*, Allison Grande, *Ad Groups Bash Calif. AG's Mobile App Privacy Guidance*, Law360 (Jan. 11, 2013, 9:31 PM), http://www.law360.com/privacy/articles/406657?nl_pk=f41eb1cf-32fa-462f-a72c-881f5897644d&utm_source=newsletter&utm_medium=email&utm_campaign=privacy.

[23] Press Release, California Attorney General's Office, Attorney General Kamala D. Harris Notifies Mobile App Developers of Non-Compliance with California Privacy Law (Oct. 31, 2012), *available at* http://www.oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-notifies-mobile-app-developers-non-compliance (last visited Jan. 18, 2013). Indeed, the Attorney General recently filed suit against Delta Airlines for failure to provide a privacy policy for its "Fly Delta" mobile application. *See* Complaint, California v. Delta Air Lines, No. CGC-12-526741, 2012 WL 6061446, at *1 (Cal. Super. Ct. Dec. 6, 2012), *available at* http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-files-suit-against-delta-airlines-failure.

[24]*Mobile Privacy Disclosures Report* at 12.