Advisory

FEBRUARY 2013

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

JOHN KENNEDY
203.363.7640
jkennedy@wiggin.com

Federal Trade Commission Issues Comprehensive Mobile Privacy Recommendations and Proposes Mobile 'Do Not Track' Mechanism

On the eve of Groundhog Day, the Federal Trade Commission ("FTC") released comprehensive recommendations for improving consumer privacy in the data-hungry realm of mobile apps (the "Recommendations"). The Recommendations urge mobile industry players to adopt a variety of best practices in their data collection and sharing practices, most notably by (i) improving the transparency of disclosures of these practices, and (ii) offering consumers more meaningful control over their data. While not law, the Recommendations contain an implicit message: the FTC has done its homework and will increasingly pursue mobile app services that engage in data practices deemed "deceptive" or "unfair" under Section 5 of the FTC Act. To underscore this point, the FTC concurrently announced a new consent decree and a proposed $800,000 fine involving the social networking app "Path", based on the company's alleged deceptive privacy practices and violations of the Children's Online Privacy Protection Act ("COPPA")[1].

A YEAR OF INTENSE SCRUTINY OF MOBILE PRIVACY PRACTICES

"Mobile Privacy Disclosures: Building Trust through Transparency"[2] caps a year of intense FTC study of the mobile apps industry. The FTC held public hearings on mobile privacy last May[3], issued two reports on the privacy shortcomings of mobile apps for children[4], published a brief privacy and advertising guidance for app developers last August[5] and conducted investigations and enforcement actions against app developers, including a new consent decree published for comment just last week.[6] Mobile privacy concerns also figured prominently in the FTC's comprehensive white paper on consumer privacy in the era of Web 2.0, issued last March[7].

Key FTC take-aways from these efforts include findings that the mobile apps industry engages in "unprecedented" data collection while consumers remain largely in the dark about what type of personal data is collected, what that data is used for and with whom the data is being shared. The FTC also recognizes that the 'mobile revolution' has obscured the already cloudy picture for consumer privacy in e-commerce and therefore threatens consumer trust. The agency is especially concerned with the scope and lack of transparency of data sharing between the large app platforms (such as Apple and Google), the multitude of app developers operating on these platforms and the behind-the-scenes data crunchers -- such as ad networks and analytics firms -- who process data for targeted advertising and other purposes.

CONTINUED ON NEXT PAGE

Federal Trade Commission Issues Comprehensive Mobile Privacy Recommendations and Proposes Mobile 'Do Not Track' Mechanism CONTINUED

FTC RECOMMENDATIONS FOR MOBILE PRIVACY PRACTICES

The Recommendations offer advice to each of the major industry players: platform providers, app developers, ad networks and industry trade associations.

The platforms provide the mobile device operating systems on which apps run and also maintain online stores for downloading apps. As such, they function as gatekeepers to the apps marketplace and are in a position to influence the ground rules for data collection and to promote consumer-friendly privacy practices by app developers. The Recommendations urge the platform providers to use this leverage to promote a range of data disclosures and choices, including "just-in-time" pop-up notices by apps before they share sensitive user data (such as precise geo-location or a user's contacts or photos). Most notably, the Recommendations call upon the platform providers to develop "do not track" mechanisms at the mobile operating system level, similar to those the FTC has called for in web browsers. Such mechanisms would enable simple consumer controls that can block tracking and profiling of a user across multiple web sites and apps.

The FTC's advice to app developers was perhaps a little blunter. Apps should have clear and simple privacy disclosures that are conspicuously posted and easily accessed, both in app stores (before downloading) and within the app itself. The Recommendations again stress the idea of "just-in-time" notices delivered to app users immediately before personal data will be shared (e.g., a pop-up such as *"We'd like to use your location right now to improve our service.* **OK? Not OK?"** in a restaurant app). Such short-form notices would be in addition to, not in lieu of, fuller, plain English privacy disclosures in an app. The Recommendations also admonish app developers to understand better the third party software tools they incorporate into their apps to facilitate data-sharing with ad networks and analytics firms. Too often, app developers don't grasp the data collection capabilities of these embedded software development kits (or "SDKs") and accordingly fail to disclose these capabilities to app users.

The FTC's message to ad networks is to work more closely with app developers to improve transparency in privacy disclosures and to help develop a universal mobile "do-not-track" mechanism. Industry trade associations are encouraged to develop standardized privacy disclosure templates and icons for use in apps to reduce consumer confusion.

IMPACT OF THE RECOMMENDATIONS

Now that the FTC has weighed in after its year-long study of mobile privacy, and following a similar pronouncement by the California Attorney General last month[8], is it time to declare victory for the cause of consumer privacy and trust in the mobile revolution? Far from it. Despite an abundance of well-researched findings and suggestions by regulators and a plethora of guidelines published by industry and non-profit groups[9], intractable structural challenges remain.

One such challenge is the market reality that consumer data is the "oil" of the e-commerce engine. Recommendations and lists of best practices, as sensible as they may be, are unlikely to tamp down the demands of 'big data' in the frothing mobile marketplace. And, as the Recommendations make clear, progress on mobile privacy issues must be a group effort, with platform providers, app developers and ad networks pulling their oars in sync. Something like that may come about in the ongoing mobile industry stakeholder discussions being hosted by the National Telecommunications and Information Agency[10]. In the meantime, the FTC has delivered its views on the subject and will presumably carry on with example-making enforcement actions as the year unfolds.

[1] http://www.ftc.gov/opa/2013/02/path.shtm

[2] http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf

[3] http://www.ftc.gov/bcp/workshops/inshort/index.shtml

[4] http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf; http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf

[5] http://business.ftc.gov/documents/bus81-marketing-your-mobile-app

[6] http://www.ftc.gov/opa/2013/02/path.shtm

[7] http://www.ftc.gov/opa/2012/03/privacyframework.shtm

[8] http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf

[9] E.g., Trust-e Mobile Privacy Certifications, http://www.truste.com/products-and-services/enterprise-privacy/TRUSTed-mobile-apps

[10] http://www.ntia.doc.gov/blog/2012/privacy-multistakeholder-process-turns-substance