March 2013

Privacy issues arising from mobile applications on smartphones are attracting significant regulatory scrutiny. Most recently, reports by two major regulators have highlighted numerous areas in which they believe mobile app privacy practices can and should be improved. Businesses active in all aspects of the mobile app ecosystem should consider these reports and their possible implications.

In January 2013, Attorney General Kamala Harris of California issued a report entitled “Privacy on the Go,” which recommended a number of mobile app privacy practices. On February 5, the staff of the Federal Trade Commission (FTC) released a report—entitled “Mobile Privacy Disclosures: Building Trust Through Transparency”—setting forth its recommendations to improve privacy-related disclosures relating to mobile applications.

Expansive Suggestions

Although these reports lack the status of a law and, in themselves, impose no mandatory obligations, they plainly seek to influence current discussions concerning privacy in mobile apps. Both the California and FTC staff recommendations are numerous, often go beyond current legal requirements and, in some instances, could be costly to implement. Although both sets of recommendations strive to embrace current views of best practices and overlap to a certain degree, some of the more expansive suggestions are unlikely to be received happily by the industry.

More broadly, the reports may influence the ongoing multistakeholder process to address transparency in mobile apps that is currently happening under the auspices of the National Telecommunications and Information Administration (NTIA). And, perhaps more importantly, both Ms. Harris and the FTC staff recommend actions that one might expect their agencies to pursue in future enforcement actions. A concern for businesses involved in mobile apps—developers, publishers, app stores, operating systems, ad networks and carriers—is that some of those steps are potentially burdensome or might interfere with the user experience.

The California Attorney General’s report summarized her enforcement actions over the past year, starting with the Joint Statement of Principles adopted by the leading app platforms early last year and implemented by them by year’s end. That Joint Statement was intended to help app developers comply with the California Online Privacy Protection Act (CalOPPA). And, like the FTC staff report, Ms. Harris’s report urged app developers, platforms, advertising networks and others to take additional steps to “minimize surprises” and give users more control over data practices unrelated to the app’s basic functionality.

Similarly, the FTC staff report reviewed the agency’s recent actions addressing mobile privacy, highlighting the FTC’s 2012 privacy report and its two 2012 reports addressing the extent to which mobile apps appeared to meet obligations imposed by the Children’s Online Privacy Protection Act (COPPA). It then quickly moved into a set of recommendations for different participants in the mobile app
“ecosystem,” including platforms, developers, advertising networks, trade associations and academicians. It also encouraged other participants, including “carriers, handset manufacturers, and chip makers,” to review its recommendations and work to improve mobile privacy disclosures.

In general, both the FTC staff and the California Attorney General reports provide guidance as to what roles the various entities—developers, platforms, stores, carriers and device manufacturers—in the app ecosystem could play in promoting transparency in privacy practices. The California Attorney General emphasizes incorporating Privacy By Design principles when designing an app and “minimizing user surprise” with how data are used in ways outside of the basic functionality of the app.

The FTC staff calls for greater oversight of apps by the platforms and greater “transparency” about the app review process, and endorses a “Do Not Track” for mobile devices, echoing the FTC’s support for a “Do Not Track” option for desktop browsers generally. There is no indication that the FTC staff considered what costs these would impose on the platforms.

Both the California Attorney General and the FTC staff advocate using “just-in-time” or other contextual disclosures and obtaining affirmative express consent “when collecting sensitive information outside of the platform’s API, such as financial, health, or children’s data, or sharing sensitive data with third parties.”

**Reports’ Consequences**

What are the consequences of these reports? First, as noted above, the California Attorney General’s recommendations admittedly in some respects “offer greater protection than afforded by existing law.” And the FTC staff report in and of itself has no legal effect. It lacks the force of a regulation or a statute, and is not even binding on the full Commission. As such, the reports are to a significant degree advisory.

Second, it is nonetheless probable that both Attorney General Harris and the FTC will seek to establish many of these provisions in future enforcement actions against mobile apps that implicate privacy. This is despite the fact that the FTC staff report expressly states that it “is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC.” Perhaps not, but the FTC is likely to use these recommendations as a source of remedies in future enforcement actions, just as it has introduced analogous concepts into consent decrees in enforcement actions against online firms over the past decade.

Third, the two reports will likely have implications for the current multistakeholder process being conducted by the NTIA involving transparency in mobile app privacy practices. Nevertheless, it is unclear what effects they may have, and the California and FTC staff reports also address a broad range of other matters that lie outside of the scope of the NTIA process.

More importantly, however, the staff report states that “to the extent that strong privacy codes are developed, the FTC will review adherence to such codes favorably in connection with its law enforcement work.” By suggesting that the agency would exercise its prosecutorial discretion favorably toward entities that join and adhere to a code of conduct, the FTC staff offers a potentially substantial carrot but also introduces a new element of uncertainty by its use of the word “strong.” If the FTC does not consider the product of the NTIA process to be “strong,” then businesses will have less confidence in the legal benefit that it may offer. On the other hand, the FTC might have difficulty concluding that a code of conduct negotiated by a wide spectrum of interests is not “strong.”