The Metropolitan Corporate Counsel®

www.metrocorpcounsel.com

Volume 19, No. 9 © 2011 The Metropolitan Corporate Counsel, Inc. September 2011

Legal Growing Pains In The Mobile App Market

Dana B. Rosenfeld and Matthew P. Sullivan

KELLEY DRYE & WARREN LLP

Long gone are the days when a wireless mobile device was used simply to make phone calls. Today's smartphone, dubbed the "third screen" behind the television and the personal computer, is driving an entirely new market based on mobile applications ("apps"). Mobile apps allow consumers to fully capitalize on the combination of mobile broadband and Web-based content and represent an undeniable bright spot in the wireless telecommunications industry. More recently, however, mobile apps have attracted scrutiny from legislators, regulators, and the consumer protection bar due to privacy concerns and claims of undisclosed charges.

This article describes the rapid growth of the mobile app market, along with the legal and regulatory issues rooted in the relationship between app providers and consumers. Additionally, the article highlights practical considerations for businesses that seek to enter this dynamic market.

I. The Mobile App Market Defined

A mobile "app" is a piece of software linked to a smartphone that allows its user to perform any number of functions, from playing children's games to displaying medical images that can assist in a patient's diagnosis. Apps reside either on top of the smartphone operating system or they can be accessed through the Internet. "Native" apps, for example, can be downloaded from virtual "stores" – Apple's iTunes and Google's Android app stores are the two most prominent examples – that are integrated with the operating system that powers the customer's smartphone. Conversely, web-based apps can be accessed as needed through the Internet, and then run within a smartphone's web browser using Javascript or HTML5 to provide interaction, navigation, or customization capabilities.

The mobile app market is only four years old, yet it is projected to grow from $2.1 billion in 2010 to $3.8 billion in 2011.[1] Thirty-five percent of adults in the United States now have apps on their mobile devices, and the number of available apps grows daily.[2] The Apple iTunes app store, for example, now offers more than 350,000 different apps. The most popular app categories are games, followed by music, with other common categories including online search, news and information, social networking, photo sharing, video streaming, and location-based services.

II. Lawmakers And Regulators Turn Their Attention To Mobile Apps

The mobile app market is a substantial revenue generator for companies in the mobile ecosystem, particularly app developers and platform providers. Apps are particularly attractive from a business standpoint because revenues can come from multiple sources. While app developers and platform providers generate revenue on the initial sale of the app, mobile apps can also include "in-app" charges – those that occur after the initial app purchase – that users must pay to access additional features or game tokens. Additionally, companies that develop or sell apps may monetize certain consumer information they collect by packaging and selling the aggregated data to a third party, such as an online advertising network. Both the consumer data collection practices and in-app charges, however, have been the subject of recent scrutiny by lawmakers and regulators.

A. Mobile Apps Figure Prominently In The Consumer Privacy Debate

The growth of the mobile apps market has corresponded with growing concerns over how consumers' online personal information is collected and shared, and the extent to which such practices are disclosed to consumers. Over the past year, lawmakers and regulators have introduced a number of proposals intended to address these concerns. In December 2010, for example, the Federal Trade Commission ("FTC") introduced its proposed privacy framework which called for greater transparency about consumer data collection practices. The framework also proposed a Do Not Track provision that would allow consumers to use a browser-based mechanism that can signal whether they want to be tracked or receive targeted ads.[3] Similarly, Rep. Jackie Speier (D-CA) introduced legislation in February 2011 that would create a Do Not Track tool that would allow consumers to prohibit online ad networks and social media sites from tracking Web browsing behavior or sharing personal information.[4] In May 2011, Rep. Ed Markey (D-MA) and Rep. Joe Barton (R-TX) introduced a bill that would limit the collection of online information for children and teens, and prohibit online targeted marketing based on such information.[5]

Despite such efforts, fears over the misuse of personal information – location information in particular – intensified in April 2011 after an investigative report in *The Wall Street Journal* claimed that Apple's iPhone and Google's Android smartphones regularly transmit users' location information back to Apple and Google.[6] In response to the story, the U.S. Senate Judiciary Subcommittee on Privacy, Technology and the Law held a hearing in May 2011 that included testimony from Apple and Google, along with the FTC and the U.S. Department of Justice. During the hearing, subcommittee members voiced concerns that mobile app developers are not required – either legally or as part of many of the large apps platform provider guidelines – to include a privacy policy with each app. Representatives from Apple and Google responded that information on location-tracking is clearly disclosed and customers must provide express consent when an app initially requests location-information.

***Dana B. Rosenfeld** is a Partner and **Matthew P. Sullivan** is an Associate in the Advertising and Marketing practice at Kelley Drye & Warren LLP.*

Please email the authors at drosenfeld@kelleydrye.com or msullivan@kelleydrye.com with questions about this article.

Nevertheless, lawmakers and regulators are moving forward with investigations or proposals to restrict certain mobile app features. Jessica Rich, Deputy Director of the FTC's Bureau of Consumer Protection, noted during the April subcommittee hearing that FTC "staff has a number of active investigations into privacy issues associated with mobile devices, including children's privacy."[7] The FTC recently followed through on this statement when it announced a settlement with children's app developer W3 Innovations, LLC and its President, following charges that the company collected and disclosed personal information from children in violation of the Children's Online Privacy Protection Act ("COPPA").[8]

Additionally, Pandora Media, Inc., which provides an app for online music streaming, acknowledged earlier this year that it received a subpoena from a federal grand jury investigating whether smartphone apps share information about their users with advertisers and other third parties. The subpoena is believed to be part of an industry review. In June 2011, Sen. Al Franken (D-MN) introduced legislation that would require companies to obtain express consent from mobile device users before location information is collected and shared with third parties.

State regulators and class action plaintiffs have been active as well. In April, the Illinois Attorney General sent a letter to Apple and Google requesting a meeting to discuss their mobile device location-information retention practices. During the same month, class actions complaints were filed in California, Florida, Illinois, and Michigan against either Apple or Google, alleging undisclosed geolocational tracking or unauthorized sharing of a mobile device's unique identifier.[9]

B. "In App" Charges Draw Scrutiny

Currently, 35 percent of the 300 most popular "free" game apps in the Apple's iTunes store use some form of virtual currency that players must purchase with real dollars to enhance the gaming experience, advance to a higher level, or increase the speed of game play.[10] Revenue generated by such in-app purchases has increased ten-fold in the past year.[11] A growing concern is whether these in-app charges are adequately disclosed to consumers prior to purchase.

Similar to the recent privacy concerns with mobile devices, in-app purchase practices have been the subject of recent investigative news reports and government inquiries. Following a *Washington Post* story in February 2011, for example, Rep. Edward Markey (D-MA), Sen. Amy Klobuchar (D-MN), and Sen. Mark Pryor (D-AR) sent separate letters to the FTC requesting investigations into app developers' in-app charging practices.[12] In April, a class action lawsuit claimed that Apple sold in-game/in-app currency, tokens, and other items to minors without parental knowledge or consent.[13] The plaintiffs allege breach of contract and violation of California's unfair business practice laws.

The Federal Communications Commission ("FCC") also has asserted a role in the mobile apps space through its Truth-in-Billing enforcement actions. In October 2010, the FCC reached a settlement with Verizon on claims that the carrier violated the Truth-in-Billing rule, which requires that invoices include plain language descriptors of charges. The action stemmed from "mystery fees" that were due in part to unauthorized data transfers initiated by mobile apps. Under the settlement, Verizon agreed to provide refunds to the 15 million affected customers and make a $25 million 'voluntary contribution' to the US Treasury.[14]

Lastly, the FTC announced in May 2011 that it plans to update its business guidance document, "*Dot Com Disclosures: Information About Online Advertising*." The guide, which was originally published in 2000, instructs businesses on providing clear and conspicuous disclosures within online advertising and sales outlets. The Commission acknowledged the growth of mobile marketing and the emergence of the "app" economy within its request for public comment on its planned revisions to the Guide.

III. Practical Considerations For Businesses

The wave of congressional inquiries, regulatory initiatives, and class action complaints targeting mobile apps are instructive to businesses and developers looking to enter or expand in the mobile app market.

- *Know Your Data*. App developers must be mindful of potential unintended data uses internally or by partners, as well as whether the app makes certain types of consumer data more readily accessible to third parties. Developers also should consider whether the data collection is even needed and whether an intended use can be clearly articulated.
- *Avoid Small Print*. Disclosures relating to privacy or in-app charges must be clear and conspicuous. The FTC is calling for disclosures that are "embedded in the interaction" (*i.e.,* pop-up disclosures would continue to appear throughout a user's interaction with an app, and at the point in which the app is seeking to collect information about the user or the user's device).[15] Companies also should stay current on efforts to revise the FTC Dot Com Disclosures Guide, and remember that regulators are closely monitoring mobile apps targeted to kids.
- *Put It In Writing*. Build in protections by allocating risk among parties through contractual obligations and liabilities. Further, ensure that contracts clearly identify the scope of acceptable data collection and use, as well as representations regarding compliance with laws and regulations, and indemnification/limitations of liability.
- *Use Self-Regulation As A Building Block*. Consult the evolving body of industry guidelines and best practices, such as those provided by CTIA-The Wireless Association and the Mobile Marketing Association, to guide business planning and app development.

Conclusion

Mobile apps have emerged as the long sought "killer app" for the wireless industry, as they give app developers new and unlimited ways to connect with customers. Businesses that seek to join this market, however, must remain mindful of the developing legal trends, and embrace the traditional principles of knowing your business, protecting the company through well-drafted contracts, and providing consumers with clear notice and full disclosure.

---

1 Jack Kent, Revenue for Major Mobile App Stores to Rise 77.7% in 2011, HIS iSuppli Market Intelligence (3 May 2011), *available at* www.isuppli.com/media-research/news/pages/revenue-for-major-mobile-app-stores-to-rise-77-7-percent-in-2011.aspx.

2 Pew Research Center Internet & American Life Project, The Rise of Apps Culture (Sept. 15, 2010).

3 FTC Staff, *Protecting Consumer Privacy in an Era of Rapid Change* (Dec. 2010), available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

4 H.R. 654 – Do Not Track Me Online Act of 2011.

5 H.R. 1895 – Do Not Track Kids Act of 2011.

6 Julia Angwin and Jennifer Valentino-Devries, *Apple, Google Collect User Data, The Wall Street Journal* (Apr. 22, 2011).

7 Jessica Rich, Prepared Statement of FTC on Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy Before Senate Subcomm. For Privacy, Tech. & the Law (May 11, 2011).

8 *U.S. v. W3 Innovations, LLC,* No. CV11-03958 (N.D. Cal. Filed Aug. 12, 2011).

9 *In re IPhone Application Litig.,* (N.D. Cal. Consolidated Compl. Filed Apr. 21, 2011); *Ajjampur v. Apple* (M.D. Fla. Filed Apr. 24, 2011); *O'Flaherty v. Apple* (E.D. Ill. Filed Apr. 29, 2011); *Brown v. Google* (E.D. Mich. Filed Apr. 27, 2011).

10 Graham Spencer, *App Purchase Revenues Soar*, Macstories.net (July 27, 2011), available at http://www.macstories.net/news/distimo-mobile-game-prices-fall-in-app-purchase-revenues-soar/.

11 Id.

12 Cecilia Kang, *Lawmakers Urge FTC to Investigate Free Kids Games on IPhone,* Washington Post (Feb. 8, 2011).

13 *Meguerian v. Apple,* Inc., No. 5:11-cv-01758-HRL (N.D. Cal. Filed April 11, 2011).

14 *In re Verizon Wireless Data Usage Charges,* 25 F.C.C.R. 15105 (2010).

15 Jessica Rich, Deputy Director of the FTC's Bureau of Consumer Protection, speaking at the hearing Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy, held by the U.S. Senate Judiciary Subcommittee on Privacy, Technology, and Law (May 20, 2011).