

e-commerce law & policy

FEATURED ARTICLE
03/09



cecile park publishing

Head Office UK Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND
tel +44 (0)20 7012 1380 fax +44 (0)20 7729 6093 info@e-comlaw.com
www.e-comlaw.com

Avoiding trouble when adding an app to the business model

The rise of smartphones, wifi hotspots, and high-speed data networks has spurred new technology-based business models and the exponential growth of consumer information online. Chief among new technologies, the use of mobile applications - 'apps' - has exploded in the past few years. From near-constant posts on Facebook to attacking the green pigs on Angry Birds, consumers have opened their hearts and wallets to mobile apps¹. John J. Heitmann and Christopher M. Loeffler, of Kelley Drye & Warren LLP, discuss that while the upside is great, companies and developers considering a mobile app should also be mindful of the legal and business pitfalls of mobile apps and implement a process to sidestep common challenges.

What's to gain?

Mobile app revenue in the four major application stores² was \$2.1 billion for 2010, and it is forecast to grow to \$3.8 billion for 2011 - a 77.7% year-over-year increase³. In 2011, experts predict there will be more than 18 billion mobile app downloads⁴.

Besides revenue from the app itself, mobile apps can provide a number of benefits to businesses. If the app itself is the product, success may be measured in paid downloads or advertising dollars generated through the app. But if the app is a mechanism to communicate with consumers, success maybe measured by free (or paid) downloads, usage statistics (if available) or other indicators of consumer engagement. The bottom line is that in the current digital marketplace, a mobile app can be

a tremendously valuable tool for connecting with consumers.

Who is watching?

The mobile app market presents an opportunity for incredible growth. But industry participants are not the only ones eyeing the app business. Investigative journalists, federal and state legislators and regulators, consumer advocacy groups, and private litigants are also closely monitoring mobile app activities and potential violations of consumer protection and privacy laws.

Media *exposés* in the *Wall Street Journal*, the *New York Times* and similar publications have brought a great deal of attention to the practices (intentional or otherwise) of Apple, Google, and others. The buzz generated by these investigative reports about mobile app practices often leads to unwanted attention on the practices of players in the mobile app space. After the investigative report, things often go from bad to worse, transitioning from public scrutiny in the press to such things as Congressional hearings, regulatory investigations, and class action litigation. More than nine public letters or inquiries have been issued by regulators. Undoubtedly, many more non-public investigations have been initiated. Additionally, nearly a dozen class action complaints (some are now consolidated) involving mobile app practices have been filed.

Who is the boss?

From a regulatory perspective, in the US, the Federal Trade Commission (FTC) appears to be leading the charge. In the FTC staff preliminary report on privacy issued in December 2010, FTC staff stated that '[a]ll companies involved in information collection and sharing on mobile devices -

carriers, operating system vendors, applications, and advertisers - should provide meaningful choice mechanisms for consumers⁵. The FTC continues to assert its broad authority to pursue these types of consumer protection actions under Section 5 of the FTC Act which prohibits unfair or deceptive acts or practices⁶. Further, the FTC has gone beyond policy statements and continues to seek enforcement opportunities. At a hearing before the Senate Committee on Commerce, Science, and Transportation, David Vladeck, Director of the FTC's Bureau of Consumer Protection stated that 'FTC staff has a number of additional active investigations regarding privacy issues associated with mobile devices, including children's privacy⁷.

But the Federal Communications Commission (FCC) also appears to be evaluating its basis for jurisdiction over mobile apps and privacy. The FCC has indicated that it has authority over mobile app privacy issues under the Communications Act's provisions governing consumer proprietary network information (CPNI) and wiretaps. The FCC already has asserted itself in the mobile space through its Truth-in-Billing enforcement actions. In October 2010, the FCC settled claims with Verizon alleging that the carrier engaged in 'unjust and unreasonable practices' and committed Truth-in-Billing rule violations based on charges for data usage on a pay-as-you-go basis to customers who did not subscribe to a data plan. The investigation revealed that some of the 'mystery fees' billed to customers were caused by unauthorized data transfers initiated by apps on the phones. Verizon settled the action for \$52.8 million to be dispersed among 15 million customers for the charges,

as well as a \$25 million ‘voluntary contribution’ to the US Treasury⁸.

Thus, players in the US mobile apps space need to be mindful of at least these two federal agencies (not to mention state regulators and attorneys general). It is notable that the FTC and FCC have addressed consumer protection issues jointly in the past. By most accounts, the National Do-Not-Call program has been one of the most successful consumer protection endeavors of the recent past. The FTC manages the day-to-day program but both agencies maintain enforcement authority over certain aspects of the program under separate statutes applicable to each agency. Absent new legislation designating a single regulator⁹, it is likely that the FTC and FCC will jointly enforce and regulate in the mobile app space. In late June, the FCC hosted a public forum on consumer privacy issues raised by location-based services (LBS) offered through mobile apps. The forum was conducted in consultation with the FTC.

Avoiding a sticky wicket

It is still too early for bright line rules regarding what is prohibited when developing and providing a mobile app, but the US congressional inquiries, statements by regulatory agencies, and pending class actions provide guidance for businesses and app developers. Following traditional advertising and privacy best practices can help reduce risks associated with an app.

Due diligence

It is important to conduct proper due diligence. Before the app is launched it should be reviewed by legal, marketing, and IT to ensure that the app does what the business wants it to, does only what the business wants it to, and everyone

The FCC’s [investigation of Verizon] revealed that some of the ‘mystery fees’ billed to customers were caused by unauthorized data transfers initiated by apps on the phones

knows exactly what the app does in terms of information collection, use and disposal, as well as when charges are imposed. The app should be evaluated from a design perspective and a consumer experience perspective. Key questions during the design due diligence stage include:

- Do you know what data is cached/collected on the device or as a result of the app?
- What is the purpose of this cache/collection and how long is it retained?
- Who has access to this data?
- What data flows through the app from user to developer/operator?
- Is the data intentionally or unintentionally shared with, visible to, or accessible by third parties?
- What are the default settings and are they consumer-friendly?
- Does the app handle payment card information?
- Does the app handle or incorporate location-based information?
- Does the app or developer have access to CPNI?

Additionally, key questions during the consumer experience due diligence stage include:

- What types of data are collected?
- What are the primary and secondary uses of any data?
- What type of notice and consent mechanism is used for data usage and sharing?
- What are the data retention and data disposal practices?
- Is the app targeted to kids?
- Is the app free or is there a fee to download?
- Are ongoing service charges applicable?
- Are in-app purchases available?
- If the business already operates an internet site, this due diligence may seem redundant. But remember, mobile is different from traditional online data collection in several ways: (1) location-based

information is readily available through most mobile devices and greatly exceeds the level of detail available through online identifiers such as IP address; (2) most users carry their smartphones with them at all times; and (3) the screen size of a mobile device presents a challenge for providing consumer notices in an effective manner.

Walking through the due diligence process is important for review of any app, but the risk evaluation should be ratcheted-up in certain circumstances. Close scrutiny should be applied to the app in the following cases:

- The app charges a fee either (1) at the time of download, or (2) within the app itself (for example, some type of in-app purchase). Make sure that any charges are disclosed up front and at the point of purchase using plain language.
- The app is directed to children-especially if a charge is associated with the app. If the app collects personal information or permits some type of in-app charge, first determine whether the higher risks associated with these practices are worth the reward. Then ensure that the app complies with applicable children’s data collection and use laws (e.g., the Children’s Online Privacy Protection Act) and any charges are disclosed up front and at the point of purchase. If you expect the app to be downloaded by parents, but played by kids, be sure that the disclosures are provided at the time of download, as well as during app use.
- The app collects location-based information about the consumer. If the app will collect location-based information, be sure this is disclosed up front using plain language. If there is no need for the collection of location-based information, consider putting language in the app development contract restricting the collection or transfer of this type of

information.

Clear communication

It is important to clearly communicate with business partners and consumers. Businesses and developers should clearly identify expectations and restrictions on app functionality, discuss compliance with mobile marketplace requirements and guidelines, and use contractual terms to expressly address the scope of responsibilities and liability. Just-in-time disclosures should be used for more sensitive information and with the imposition of consumer charges.

Contractual protection

Risk should be allocated among the parties through express contractual requirements and liabilities. Be sure to address the scope of data collected and permitted uses, business approval of all consumer disclosures, and representations and warranties regarding compliance with laws as well as project specifications. Also, it is important that the indemnification and limitation of liability provisions do not undercut the core protections or allocation of risk addressed in the rest of the contract.

Conclusion

A mobile app can provide an exciting and engaging new approach for connecting with consumers. To keep out of trouble when navigating this space, businesses and developers must keep an eye on developing legal trends, and ensure that their development programs and apps include comprehensive due diligence, clear communication with consumers and business partners, and protective contract terms.

John J. Heitmann Partner
Christopher M. Loeffler Associate
 Kelley Drye & Warren LLP
 jheitmann@kelleydrye.com
 cloeffler@kelleydrye.com

1. Apple: The 10 most popular free and paid apps, *The Telegraph*, available at www.telegraph.co.uk/technology/apple/8278380/Apple-The-10-most-popular-free-and-paid-apps.html
2. Apple iTunes, Android Market, BlackBerry App World, and Nokia Ovi.
3. 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
4. Id.
5. FTC Staff, Protecting Consumer Privacy in an Era of Rapid Change (December 2010) at p. 59.
6. 15 U.S.C. § 45.
7. Consumer Privacy and Protection in the Mobile Marketplace Before the S. Comm. on Commerce, Science, and Transportation 13 (19 May 2011) (prepared statement of FTC), available at www.ftc.gov/os/testimony/110519mobilemarketplace.pdf; see also Amy Shatz, Tech Giants Defend Privacy Practices, *The Wall Street Journal* (20 May 2011), available at http://online.wsj.com/article/SB10001424052748704816604576333512798714304.html?mod=googlenews_wsj%20%20F
8. In re Verizon Wireless Data Usage Charges, 25 F.C.C.R. 15105 (2010).
9. For example, S. Commercial Privacy Bill of Rights introduced this session by Senators Kerry (D-MA) and McCain (R-AZ), if enacted, would expressly apply to mobile devices, includes jurisdiction over common carriers, and designates the FTC as the sole federal enforcer.