Legal Insight

K&L GATES

www.klgates.com

March 15, 2012

Practice Groups:

Technology Transactions and Data Protection

Telecom, Media and Technology

Privacy, Data Protection and Information Management

Privacy Policies of Mobile Apps Falling Under Increased Scrutiny by State and Federal Regulators

By Samuel R. Castic, J. Bradford Currier, Marc S. Martin, Lauren B. Pryor, Holly K. Towle and Mark Wittow

In recent months, mobile application developers (e.g., Zynga) and mobile platforms (e.g., Apple's iTunes) have faced increasing scrutiny in connection with their privacy practices, primarily with respect to transparency. State and federal authorities, members of Congress, and litigants have all brought attention to perceived failures of mobile applications ("apps") to disclose information collection and disclosure practices.

The Federal Trade Commission ("FTC") has weighed in on these issues by settling its first enforcement proceeding against a company that used a mobile app to collect information from children.[1] The FTC has also released a "warning" in a staff report[2] in connection with the Children's Online Privacy Protection Act ("COPPA")[3] that focuses on the failure of companies collecting personal information through mobile apps and the platforms that make those apps available to properly disclose privacy practices for apps targeted at children. Following the FTC report, the California attorney general announced a non-binding agreement between the state and six leading mobile app platforms that is likely to increase pressure on various participants in the mobile app arena to disclose their information collection practices through privacy policies. In addition, the White House recently proposed a "Consumer Privacy Bill of Rights" which encourages the development of legally enforceable codes of conduct, including for mobile apps.

This alert will discuss the increasing state and federal scrutiny that mobile app providers are experiencing.[4]

COPPA Requires Online Services Directed to Children to Post Privacy Notices

In the FTC staff report, the FTC reviewed the privacy practices of 400 mobile apps that appeared to be

---

[1] *See* FTC Press Release, "Mobile Apps Developer Settles FTC Charges It Violated Children's Privacy Rule" (Aug. 15, 2011), *available* here.

[2] "Mobile Applications for Kids: Current Privacy Disclosures Are Disappointing" (Feb. 2012) *available* here; *see also* here.

[3] 15 U.S.C. § 6501 *et seq*.

[4] By the term "provider," we mean any entity that might collect personal information through a mobile app. Whether a data protection or privacy law actually applies to a provider will depend on who it is, what it does, the data being collected, and the purpose for collecting it. A provider is often the app developer who makes the app and uses it to collect data (e.g., a developer who both creates a game app and runs the game). The provider may also be a third party company who uses an app to collect information from customers (e.g., a bank hires a developer to create a loan balance app). The provider could also be a different third party that is providing services or advertisements within an app, or a platform for obtaining apps (e.g., an apps store). Very generally speaking, the entity that collects and controls information is the primary focus of data protection rules. Service providers, advertisers, and companies that simply "possess" personal information can also be implicated contractually or by law.

directed at children.[5] The FTC encouraged app providers to provide simple privacy disclosures and alerts regarding apps' social media features that may collect personal information about children. The FTC report suggested that over the next six months the FTC will conduct additional reviews to determine whether to take enforcement actions in connection with apps that violate COPPA. Importantly, the FTC report noted that its efforts in the area of mobile apps are "a warning call to industry that it must do more to provide parents with easily accessible, basic information about the mobile apps that their children use."[6]

COPPA requires websites and, according to the FTC, online services that target children under the age of 13, or that knowingly collect personal information[7] about children under the age of 13, to post a clear and comprehensive privacy policy.[8] Although "online service" is undefined in COPPA, the FTC has taken the position in at least one enforcement order that apps are an online service falling within COPPA's scope.[9]

COPPA privacy notices must indicate what information websites or online services collect from children as well as how such information is used and disclosed.[10] COPPA also requires online services to obtain verifiable parental consent before collecting any personal information about children under the age of 13.[11] Note that careful planning is required to obtain parental consent in the mobile app context.

Although not all apps are subject to COPPA, whether an app targets children can be a difficult question. Under current regulations, the relevant factors include the app's subject matter, visual or audio content, age of models, language or other characteristics of the app, whether advertising promoting or appearing in the mobile app is directed to children, competent and reliable empirical evidence regarding audience composition, evidence regarding the intended audience, and whether the app uses animated characters and/or child-oriented activities and incentives.[12]

The FTC is currently conducting a comprehensive review of the regulations related to COPPA. This review may lead to new compliance requirements for anyone covered by COPPA.[13] Stay tuned for further developments in the coming months.

California Attorney General's Non-binding Agreement with Mobile Platforms Suggests Existing State Privacy Laws Apply to Mobile Apps

California's attorney general recently announced a voluntary agreement with six providers of mobile

---

[5] FTC staff report, at 4.

[6] *Id*. at 2.

[7] Personal information is broadly defined to include names, e-mail addresses, phone numbers, social security numbers, other identifiers that permit online or physical contact with the child, and other information about children or parents that is collected online and combined with any of the foregoing. 15 U.S.C. § 6501(8).

[8] 15 U.S.C. § 6502(a)(1); 16 C.F.R. § 312.3.

[9] *See* here and here; *see also* 76 Fed. Reg. 59807 (Sept. 27, 2011) (FTC noting that while undefined in COPPA, the term "online services" supports a broad reading to encompass new technologies).

[10] 16 C.F.R. § 312.3(a).

[11] 15 U.S.C. § 6501(2)(b)(1)(A)(ii).

[12] 16 C.F.R. § 312.2.

[13] *See* here and here.

app platforms to facilitate the distribution of app privacy policies and encourage users to report privacy violations.[14] Although the agreement does not create any new legal obligations for app providers, it does take the position that existing California law "requires mobile applications that collect personal data from California consumers to conspicuously post a privacy policy."[15] The signing platforms (e.g., Apple Inc., for the iTunes App Store) agreed to modify the app submission process for new or updated apps to make it easier for app providers to include a link to, or the text of, the app's privacy policy.[16] The platforms also agreed to create reporting procedures for users to identify apps that do not comply with applicable terms of service or law and develop a response process to handle reported privacy violations.[17] No timetable exists for the implementation of the voluntary agreement and the parties agreed to reassess the state of app privacy policies in six months. While the actual effect of the non-binding California agreement on mobile app privacy practices is unknown, it shows that regulators are increasingly interested in app privacy practices, and it ratchets up the pressure on mobile app providers to develop clear, accurate privacy policies.

Based on this agreement, it appears that California's attorney general has concluded that existing state privacy law currently requires websites and online services to post privacy policies when collecting personally identifiable information about California residents.[18] As in the case of COPPA, "online service" is undefined by the California statute and, until this agreement with mobile platforms, many questioned whether the privacy policy requirements applied to mobile apps. When it applies, California's law applies more broadly than COPPA, e.g., it applies regardless of a user's age. However, the website or online service must be commercial in nature and must collect personally identifiable information about consumers residing in California.[19]

The FTC Act Requires Accuracy in Privacy Policies

Even though there is increasing pressure on mobile app providers to post privacy policies, they should not do so without careful attention to relevant background laws and other considerations. Knowing why one is posting is important—i.e., is it to comply with a legal requirement, to meet a business need, or for some other reason? The answers can make a difference and have consequences. For example, once privacy policies or statements are made to users, even voluntarily, FTC powers kick in that otherwise might not have been triggered.

The FTC takes the position that Section 5 of the FTC Act, which prohibits deceptive or unfair acts or practices in trade or commerce, authorizes it to redress inaccuracies in privacy policies, or in characterizing privacy practices.[20] Based on this authority, the FTC has commenced actions against a number of companies, alleging that they failed to describe their data collection, protection, or sharing practices fully or accurately, whether in a privacy policy or otherwise.[21] The FTC has also brought

---

[14] California Office of the Attorney General, "Joint Statement of Principles" (Feb. 22, 2012) *available* here.

[15] *Id.* at 1.

[16] *Id.* at 2.

[17] *Id.* at 3.

[18] Cal. Bus. & Prof. Code § 22575.

[19] *Id.*

[20] *See* Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers ("FTC Framework"), 3-4 (Dec. 2010) *available* here (Note that this report was characterized as a "preliminary FTC staff report"; the FTC is soon expected to release its final version of this report.).

[21] *See id.* at 9 n.17.

actions against companies for alleged inadequacies in safeguarding personal information collected from users, in access controls, and in authenticating users, which the FTC treats as "unfair acts" even if no privacy policy is provided to a user.[22] Although there is no generally applicable requirement that the FTC can rely on to require companies to post a privacy policy, once a privacy policy is posted (such as pursuant to COPPA or California law), the FTC has authority under Section 5 of the FTC Act to deal with deceptive practices or unfair acts. States also often have "mini-FTC Acts" that prohibit unfair or deceptive acts or practices at the state level, with enforcement authority resting in the hands of state attorneys general and/or private litigants who often can commence class actions.

FTC and state attorney general enforcement actions could also begin under a proposal from the Obama administration entitled the Consumer Privacy Bill of Rights.[23] Under this proposal, the National Telecommunications and Information Administration (in the Department of Commerce) will work with industry, privacy advocates and other stakeholders to create and implement "codes of conduct." Participation is voluntary, but once a business adopts a code of conduct, that adoption and any subsequent failure to comply with the code will be actionable.[24] The NTIA has recently requested comment on the mechanics of creating these codes and is expressly seeking comment on a code of conduct for mobile apps in general and on mobile apps that provide location based services.[25]

Before posting a privacy policy, it is important to comply with the laws applicable to the data collected and the company collecting it. Often those laws will require or encourage an accurate description of what personal information (variously defined) is collected, used, shared, and disclosed, as well as the purposes for doing so. If the descriptions do not comply with laws governing them, or if they are deceptive or involve unfair practices, there is potential legal exposure.

FTC staff also urges privacy policies to be "clearer, shorter, and more standardized."[26] This can result in a Catch-22: if brevity comes at the expense of accuracy, there is increased risk that a privacy policy will be deemed misleading, deceptive, or insufficient. When brevity omits the details of a particular information collection activity, the FTC may allege that the mobile app provider has not fully disclosed this practice to the user and, accordingly, may not rely on the disclosure to engage in the activity.[27] Further complicating the issue are the need to keep policies current and the inherent

---

[22] *See, e.g.*, Complaint, *In the Matter of Reed Elsevier Inc. and Seisint, Inc.*, FTC File No. 052-3094 (Aug. 1, 2008) *available* here; Complaint, *U.S.A. v. Rental Research Services, Inc.*, FTC File No. 072 3228 (Mar. 5, 2009) *available* here.

[23] *See* Consumer Data Privacy in a Networked World, A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (Feb. 2012) *available* here.

[24] *See id*. at p. 29, §A(citations omitted)("The FTC is the Federal Government's leading consumer privacy enforcement authority. Enforcement actions by the FTC (and State Attorneys General) have established that companies' failures to adhere to voluntary privacy commitments, such as those stated in privacy policies, are actionable under the FTC Act's (and State analogues) prohibition on unfair or deceptive acts or practices. In addition, the FTC brings cases against companies that allegedly failed to use reasonable security measures to protect personal information about consumers. . . .The same authority would allow the FTC to enforce the commitments of companies under its jurisdiction to adhere to codes of conduct developed through the multistakeholder process. Thus, companies that adopt codes of conduct will make commitments that are legally enforceable under existing law.").

[25] *See* 77 Fed. Reg. 13098, 13099 (Mar. 5, 2012).

[26] FTC Framework, *supra* note 20 at 70.

[27] *See* letter from David Vladeck, FTC Director of the Bureau of Consumer Protection, to Michael St. Patrick Baxter, consumer privacy ombudsman in bankruptcy of Borders Books (Sept. 14, 2011) *available* here (In order to avoid deception regarding its statement that it would not "sell" data for marketing, Borders' policy made it clear that the data was a transferable asset for other purposes, including in connection with sales, mergers, and reorganizations of its business. The FTC opposed a transfer in connection with a bankruptcy, and took the position that the policy language was not broad enough to encompass dissolutions or sales of assets other than from a going concern.).

difficulties in presenting privacy disclosures on smart phones.[28] The FTC will be holding a workshop in May regarding those difficulties.[29]

In short, there is no one-size-fits-all approach for addressing data protection laws and privacy policies as they relate to mobile apps. There is a "one-size" need, however, to take those laws into account: companies must carefully evaluate an app's features and capabilities and the related legal requirements, voluntary commitments, and business objectives in order to develop a compliance structure, including crafting and updating appropriate privacy disclosures.

Authors:

Samuel R. Castic
samuel.castic@klgates.com
+1.206.370.6576

J. Bradford Currier
brad.currier@klgates.com
+1.202.778.9885

Marc S. Martin
marc.martin@klgates.com
+1.202.778.9859

Lauren B. Pryor
lauren.pryor@klgates.com
+1.202.778.9398

Holly K. Towle
holly,towle@klgates.com
+1.206.370.8334

Mark H. Wittow
mark.wittow@klgates.com
+1.206.370.8399

[28] FTC Framework, *supra* note 20 at 70-71 (The FTC Framework notes that privacy notices in the mobile context are a "strong illustration" of how such notices are "ineffective" because of "the small size of the device.").

[29] *See* FTC Bureau of Consumer Protection, "Fast-Forward" (Mar. 5, 2012) *available* here (workshop will include consideration of how short, effective, and accessible privacy disclosures can be made on mobile devices).

K&L GATES

Anchorage Austin Beijing Berlin Boston Brussels Charleston Charlotte Chicago Dallas Doha Dubai Fort Worth Frankfurt Harrisburg Hong Kong London Los Angeles Miami Milan Moscow Newark New York Orange County Palo Alto Paris Pittsburgh Portland Raleigh Research Triangle Park San Diego San Francisco São Paulo Seattle Shanghai Singapore Spokane Taipei Tokyo Warsaw Washington, D.C.

K&L Gates includes lawyers practicing out of more than 40 fully integrated offices located in North America, Europe, Asia, South America, and the Middle East, and represents numerous GLOBAL 500, FORTUNE 100, and FTSE 100 corporations, in addition to growth and middle market companies, entrepreneurs, capital market participants and public sector entities. For more information about K&L Gates or its locations and registrations, visit www.klgates.com.