DataGuidance is the leading global data protection and privacy compliance resource tool, created with a single aim - to make data protection and privacy compliance simpler. It delivers, in one site, legal and regulatory information from all relevant data protection and privacy sources, keeping its growing community of subscribers on top of national laws and regulations, in a quick, easy to navigate, clear database. In addition, DataGuidance Notes and At-A-Glance Advisories are devised by data protection experts to provide users with advice on both global coverage and local compliance.

DataGuidance subscribers include: Citigroup, BP, Rolls Royce, Proctor & Gamble, IBM, AmGen

This article was originally published in DataGuidance, October 2011.

Children’s Privacy in the Mobile Data Environment

Recent evidence suggests that children, including children as young as three and four years of age, increasingly use mobile devices to access the Internet to play games, communicate with peers, or engage in interactive content targeting a young audience. Studies by the Pew Internet and American Life Project, for example, found that 58 percent of 12 year olds in the United States have access to cell phones,¹ and 46 percent use social networking services.² Further, a recent report by Nielsen Research found that games and social networking — the two most attractive online activities for children — represent two of the three most popular mobile app categories.³ These statistics portend a range of issues relating to children’s online privacy, including parental notice, consent and verification, third-party access to children’s personal information, and the collection and use of geolocational data obtained from a mobile device.

This article describes the recent legal and regulatory developments that directly affect children’s privacy protections in the mobile data environment. The article also includes practical considerations for businesses that develop mobile content targeted to children.

¹ Kristin Purcell et al, Pew Internet and American Life Project – The Rise of Apps Culture, Pew Research Center (Sept. 15, 2010).
² Amanda Lenhart et al, Pew Internet and American Life Project – Social Media and Young Adults, Pew Research Center (Feb. 3, 2010).
Why the Mobile Environment is Different

The mobile platform has become a critical gateway to the Internet, due primarily to the rapid growth of the mobile app industry, and the evolving use of social media. In light of these developments, parents, lawmakers, and regulators are placing an increased focus on the privacy risks associated with children’s participation in the mobile Internet.

The mobile environment has several elements that raise unique concerns with respect to children’s privacy. For example, unlike personal computers, which are tethered to home or school, most people carry their mobile device or smartphone with them at all times. These devices continually generate geolocational data that leave a virtual breadcrumb trail of the users’ whereabouts. This location information may then be accessed by mobile device service providers or third-parties, such as mobile app developers. Further, the screen sizes found on most mobile devices do not lend themselves to the same type of lengthy consumer notices concerning privacy and collection of personal information that can be displayed on personal computer screens. Finally, mobile app developers generally are not legally required to include privacy policies within their applications, so consumers may not be aware of the manner or extent to which personal information collection is occurring.

Legislators Consider Children’s Online Privacy Protections

Federal lawmakers have taken notice of the unique concerns with respect to mobile data and children’s privacy. Among the 18 consumer privacy bills that have been introduced by Congress so far this year, a number of them directly address children’s online privacy or the mobile data environment. In May 2011, Rep. Ed Markey (D-MA) and Rep. Joe Barton (R-TX) introduced the Do Not Track Kids Act of 2011 (H.R. 1895). The bill would prohibit the operator of an online service or mobile application from compiling or disclosing to third parties personal information collected from children under 13 and minors (children between the ages of 13 and 17) for targeted marketing purposes. The bill also would restrict the collection of geolocational information for children and minors.

In June 2011, members of the House and Senate introduced several bills intended to restrict the use of consumer geolocational information. The bills include the Geolocational Privacy and Surveillance Act (“GPS Act”) (H.R. 2168) introduced by Rep. Jason Chaffetz (R-UT) and Rep. Robert Goodlatte (R-VA), and the Location Privacy Protection Act of 2011 (S. 1223) introduced by Sen. Al Franken (D-MN) and Sen. Richard Blumenthal (D-CT). Both bills prohibit the collection, use, or disclosure of consumer geolocation data without consumer consent, and would extend protections to both real-time and archived geolocation information. The bills include only a small number of exceptions for undisclosed use of such data, including in emergency situations. Notably, both bills would impose criminal and civil penalties for unlawful collection, use or disclosure of a consumer’s location data.

Lawmakers’ sense of urgency has been driven, in part, by news reports concerning the unauthorized collection of consumers’ location information stored on mobile devices as well as several recent high-profile data breaches. In April 2011, for example, Sony announced that hackers had compromised the personal information of more than 75 million PlayStation users. The same month, news reports surfaced that Apple’s iPhone and Google’s Android devices were storing device location information without users’ knowledge or consent. Legislators responded with a series of hearings in late Spring that included testimony from both industry representatives, including Apple and Google, and federal regulators. On May 10, 2011, the U.S. Senate Judiciary Subcommittee on Privacy, Technology and the Law held the hearing “Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phone and Your Privacy.” During the hearing, Jessica Rich, Deputy Director of the Bureau of Consumer Protection at the Federal Trade Commission (“FTC”) testified that FTC Staff was engaged in “a number of active investigations into privacy issues associated with mobile devices, including children’s privacy.”
FTC to Update the Children’s Online Privacy Protection Rule

The primary mechanism for safeguarding children’s online information is the Children’s Online Privacy Protection Rule (“COPPA Rule” or “Rule”). The Rule, which was enacted in 1998, requires commercial websites and online services that target children to provide direct notice to a parent and obtain the parent’s verifiable consent before collecting personal information from children under the age of 13.

In September 2011, the FTC issued proposed amendments to the Rule that are intended to address the substantial changes in consumer technology that have occurred over the past decade since the Rule first went into effect. The proposed revisions are designed to ensure that the Rule continues to provide privacy protections for children who increasingly participate in social networking and interactive gaming, or engage in online activities through a mobile device.

COPPA Rule Definitions

Among the notable proposed changes to the Rule, the FTC is seeking to expand the Rule’s definition of “personal information” to include new forms of data that the FTC considers personally identifiable. Under the proposed revisions, “personal information” would include online screen and user names, unless the names are used for technical maintenance of the online service or website. In recognition of information-sharing trends on social media sites, the revised definition also would cover photographs, and video or audio files containing a child’s image or voice. Notably, the FTC is proposing that “personal information” also include geolocation information emitted by a child’s mobile or electronic device. This proposed revision responds to the recent concerns expressed by Congress and the FTC over the extent to which mobile operators are collecting location information from user devices.

Parental Notice and Consent

The proposed rule would address space constraints associated with most mobile device screens by limiting the use of lengthy privacy policies to communicate information to parents and kids, and streamlining the current notice requirements. This proposed approach would require that mobile application developers, for example, give parents easy-to-understand information provided on a real-time basis, which is consistent with the FTC’s preference that disclosure and notice information be “embedded in the interaction.”

The FTC’s recognition of new technologies is evident in the proposed changes to the consent requirements in the current rule. For example, the Commission’s proposal would expand the methods by which operators can seek and obtain verifiable parental consent to include electronically-scanned versions of signed parental consent forms, videoconferencing, and government-issued identification – such as a driver’s license – that is checked against a database. The Commission also hopes to stimulate the development of new technology-based methods of consent and is proposing a new process through which operators may voluntarily seek FTC approval of potential consent mechanisms. Prior to approval, the FTC would review the mechanism and offer it for public comment.

Security Safeguards

The COPPA Rule requires operators to establish reasonable procedures to protect the confidentiality and security of children’s personal information; however, the current rule is silent on the data security obligations of third parties. The proposed revisions would require that companies take “reasonable measures” to ensure that any service provider or third party to whom children’s personal information is provided has enacted “reasonable procedures” to protect the confidentiality and security of such information.

4 16 C.F.R. Part 312
The proposed revisions also would impose a new data retention and deletion requirement, whereby companies could retain children's personal information only for so long as it reasonably necessary to fulfill the purpose for which the information was collected. The operator also would be required to take reasonable measures to protect against unauthorized access to the information during the data deletion or disposal process.

COPPA Rule Enforcement

In addition to its rulemaking authority, the FTC is also using its enforcement powers to safeguard children’s online privacy. The FTC, within the past several months, has announced a number of settlements with mobile app developers, including those that offer content targeted to children. In August 2011, for example, the FTC announced that it had reached a settlement in its first action against a mobile applications (“app”) developer. The FTC had charged W3 Innovations, LLC (“W3”) and its President with violating the COPPA Rule when W3 allegedly collected and disclosed personal information from up to 30,000 children without their parents' consent.

W3 Innovations, which does business as Broken Thumbs Apps, develops and distributes apps including Emily’s Girl World and Emily’s Runway High Fashion (the “Emily Apps”), which are sold through the “Games-Kids” section of Apple, Inc.’s App Store. According to the FTC Complaint, the Emily Apps encouraged children to submit emails, including messages to friends and requests for advice, that were then posted as publicly-available blog entries to the “Emily’s blog” feature on the Emily Apps sites. Children also could submit comments to the site using a form that required user name and email address information. The settlement requires W3 and its president to pay $50,000, and they must delete all personal information collected in violation of COPPA.

Practical Considerations for Businesses

Given the current focus on children's privacy by regulators and legislators, companies seeking to enter the mobile app market or engage a younger audience using games or other online features should keep in mind several best practices that can help reduce risks resulting from increased legal and regulatory scrutiny.

- **Know your/your partner’s app** – Before launching your mobile app, ensure that all stakeholders fully understand the extent to which the app collects, uses, and disposes of personal information. Evaluate whether any benefits associated with any information collections are worth the increased scrutiny. If you are partnering with other companies, ensure that you have a full understanding of their app and business model and appropriately allocate risk through express contractual requirements and liabilities.

- **Understand the COPPA Rule** - Don’t be caught off-guard by learning after a regulatory inquiry that your business activities fall within the parameters of the COPPA Rule. For example, the Rule, in addition to covering websites that target kids directly, also applies to an online service that targets a general audience if that company has actual knowledge that it is collecting or maintaining personal information from a child.

- **Closely track the proposed COPPA Rule revisions as well as legislative developments** – Many of the FTC’s proposed revisions likely will be part of the final revised Rule. Some of the proposed revisions could add substantial new obligations to certain parties. For example, multiple parties, including app developers, ad networks, and service providers are responsible for different functions in delivering the app to the consumer. A proposed revision would modify online notice requirements by mandating that all operators involved in the operation of an online service – and not just a designated operator, as permitted under the current Rule – provide contact information that includes the operator’s name, physical address, telephone number and email address.
Conclusion

The mobile environment has opened up a dynamic sales channel for app developers that create content targeting a young audience. Businesses that seek to participate in this market, however, must remain mindful of the scrutiny given to children’s privacy and the unique characteristics of the mobile data environment, understand and follow the COPPA Rule, and closely monitor ongoing regulatory and legislative developments specifically targeting this growing market segment.

* * *

Dana B. Rosenfeld is chair of the Privacy & Information Security practice and partner in the Advertising & Marketing practice at Kelley Drye & Warren LLP in Washington, D.C. Matthew P. Sullivan is an associate in the Advertising & Marketing and Privacy & Information practices at Kelley Drye.