Amendments To COPPA and ***Protecting Children's Privacy***

By Elizabeth Bruns and Kimberly Nguyen, Mitchell Silberberg & Knupp LLP

Elizabeth Bruns and Kimberly Nguyen are lawyers with the firm Mitchell Silberberg & Knupp LLP. This article was submitted voluntarily to CTR. Neither party was compensated (this is not an "advertorial").

Last December the Federal Trade Commission adopted amendments to the Children's Online Privacy Protection Act, otherwise known as COPPA. These changes will go into effect on July 1, 2013. This article discusses the importance of the Act from a legal point of view, and how some of the recent revisions might affect the development and operation of children's apps. First some definitions.

What is COPPA?

COPPA (see http://www.ftc.gov/ogc/coppa1.htm) is the only child-specific federal privacy law in the U.S. It was enacted by Congress in an effort to protect children from unfair or deceptive acts relating to the collection of their information online. Through this law, Congress made clear that parents should be the gatekeepers of their children's personal information online and that parents need clear and accurate information about online practices. The COPPA Rule requires website operators and online service operators to follow certain rules in requesting, using and disclosing children's personal information.

The current Rule amendments are the result of a mandatory review in 2010, when the FTC acknowledged that the technological landscape and the ways children interact online have changed drastically since COPPA was enacted.

One of the main focuses of the amendments is on mobile application privacy and how the Act applies to mobile technology. The FTC released two reports on mobile applications ("apps") for children and found that most app developers fail to disclose adequately (or at all) to parents their collection and disclosure practices with respect to children's information. App developers should be aware of their responsibilities under COPPA and parents should be informed of their rights with respect to the collection and disclosure of their children's personal information.

The basic requirement of COPPA is that operators of commercial websites and online services (including certain apps) must provide notice and obtain parents' consent before collecting personal information from children under age 13. We will talk about some of the details of this basic requirement below.

Do all apps need to comply with COPPA?

COPPA applies to commercial websites and online services directed to children that collect, maintain, or provide the opportunity to disclose personal information ("PI"). A mobile app is considered an "online service" if it sends or receives information over the Internet and allows children to play network-connected games, engage in social networking activities, purchase goods or services online, receive behaviorally targeted advertisements, or interact with other content or services.

In determining whether an app is directed to children, the FTC will consider the app's subject matter and content; whether it uses animated characters; the age of models; child-oriented language, graphics, activities, incentives; whether the app has child celebrities or celebrities appealing to children; whether advertising, promoting or appearing on the app is directed to children; evidence about the intended audience and empirical evidence about audience composition.

> "... app developers ... are strictly liable for children's personal information..."

The revised Rule clarifies that app developers of child-directed websites are strictly liable for children's personal information collected through child-directed websites or their services, by independent entities or third parties who collect or maintain such information on behalf of the app developers, such as in the cases of advertising networks and downloadable plug-ins.

Because of this strict liability standard, app operators should go beyond their contract with the network or plug-in and investigate if the network or plug-in is able to, and is actually, complying with COPPA.

The new Rule allows an app that is child-directed, but which does not target children as its primary audience, to age screen users to provide COPPA protections only to children under 13. COPPA also applies to operators of general audience sites and online services (including tween or teen sites) who have actual knowledge that they collect PI of children under 13. An operator will have "actual knowledge" if a child self-identifies as under 13 through an age screen or the operator is notified by a parent or other person.

What is personal information?

PI is individually identifiable information about an individual collected online. The new amendments expand the definition of PI to include: Photos, videos or audio files containing a child's image or voice; screen/user name if it functions in the same manner as online contact information; geolocation information sufficient to identify street name and name of city/town; and Persistent Identifiers used to recognize a user over time and across different websites or online services (including cookie strings, user IDs, IP addresses, processor or device serial numbers, unique device identifiers).

The new Rule provides three new exceptions to the requirement to obtain parental consent before collecting PI from children under 13:

(1) if an app collects a persistent identifier (but no other PI from a child) for the sole purpose of providing support for internal operations;

(2) if an app collects a parent's online contact information but no other PI from a child solely to keep the parent informed of the child's activities; and

(3) if a plug-in collects a persistent identifier on a child-directed app but no other PI from a previously registered user who is 13 or older.

App operators also must provide parents access and the opportunity to delete their child's PI and optout of future collection.

How can an app developer obtain parental consent before collecting children's PI?

Under the existing Rule, the appropriate methods of obtaining verifiable parental consent include consent forms via postal mail or facsimile, or a credit card to complete a transaction, or telephonic verification of the parent, or emailing the parent with the requirement that the parent acknowledge and respond to the email.

The Rule is amended to include electronic scans of signed consent forms, consent via video-conference, use of a debit card or other online payment system if it provides notification of each transaction and use of a parent's government-issued ID checked against a database, but only if the parent's ID is deleted promptly after verification.

What should an app developer include in its privacy disclosure notice?

Under the new Rule, which streamlines the disclosure requirements, app developers must provide a short, simple statement that includes:

(1) what information is collected from children, including whether the mobile app allows a child to publicly post personal information;

(2) how the app operator uses the information; and

(3) the disclosure practices for such information.

Operators must post their privacy policy and links to the policy wherever personal information is collected, give parents direct "just-in-time" notice of its practices and obtain verifiable parental consent before collecting PI from children, with limited exceptions. Such disclosure notice need only be placed on the home or landing screen, and not at the point of purchase, if any.

What new provisions does the amended Rule have regarding data security?

The new Rule adds a requirement that operators take reasonable steps to release children's personal information only to parties capable of maintaining its security. When an app developer discloses children's PI to third parties, they must inquire about the third party's data security capabilities and receive assurances (either by contract or otherwise) that the third party is capable of maintaining and will maintain the security, confidentiality and integrity of such information. However, the app developer will not be required to ensure that the security, confidentiality and integrity of such information is maintained by the third party.

Further, the new Rule requires operators to retain children's PI for only as long as is reasonably necessary to fulfill the purpose for which it was collected and to properly delete PI by taking reasonable measures to protected against unauthorized access to or use of such deleted PI.

Disclaimer: This article is offered only for general informational and educational purposes. It is not offered as and does not constitute legal advice or legal opinion. You should not act or rely on any information contained in this article without first seeking the advice of an attorney. This article is not meant to be a comprehensive review of all of the COPPA Rule amendments, but rather an overview of some of the key changes that might affect app development and use.