COPPA +1: Issues and Impacts for Children’s Privacy

After an extensive rulemaking that began in the spring of 2010,[1] the U.S. Federal Trade Commission (FTC) adopted changes to its rules implementing the Children’s Online Privacy Protection Act (COPPA) that became effective July 1, 2013.[2] COPPA applies both to websites and online services (including apps) directed to children under 13 and to general audience websites and online services with actual knowledge that they are collecting information from children under 13. As a result, COPPA applies to businesses that may not initially recognize they are covered. In response to numerous comments, the FTC modified some aspects of the original proposed rule that made compliance with the final COPPA rule[3] somewhat easier for the business community. Nevertheless, a bit more than a year after the final COPPA rule took effect, questions of interpretation remain.

As global businesses continue to work to comply with the COPPA rule changes, and to deal with the dizzying pace of technological changes, they are also following the proposed EU requirements governing children’s privacy set forth in the proposed EU Privacy Regulation released on January 25, 2012. [4] One primary reason is that, to date, the proposed EU Regulation fails to incorporate some of the key exclusions that, from a business perspective, make COPPA workable. Without revisions to the EU Regulation to address operational complexities and practical solutions, adoption of the EU Regulation as proposed could mean the disappearance of some free children’s content, or adoption of “pay to access” models as a mode of obtaining parental consent. As a result, it is worth examining how the final COPPA rule changes the landscape and its implications for global businesses that care about kids’ content and kids’ privacy.

COPPA: What’s Changed and What’s Not?

Companies operating in the kids’ space in the United States paid attention to children’s privacy even before Congress adopted COPPA. This is largely because the U.S. children’s advertising self-regulatory body, the Children’s Advertising Review Unit (CARU), adopted guidance on children’s privacy before COPPA was enacted. In fact, essential concepts underlying COPPA, including the important exclusions recognized by COPPA, derived from the early CARU Guidelines and enforcement experience. The focus was on practical ways to involve parents when data was collected from younger children online, while balancing needs to allow limited data to be collected from children where there were low risks to children’s privacy. However, when these concepts were incorporated into regulatory language, differences in interpretation surfaced. With the significant changes of the July 2013 final COPPA rule, questions have continued to be raised.

Personal Information. Definitions of “personal information” in the original COPPA rule reflected traditional views, centering on data points like full name, home address, telephone numbers, Social Security numbers, and the like. The definitions thus reflected commonly-understood distinctions between personal and non-personal information. It is important to remember that due to the high importance major child-oriented businesses place on children’s privacy, many companies have offered children the ability to engage in a website by simply picking a user name and password. This has helped to preserve an anonymous experience but allow children to enjoy some personalization based on their preferences. The information, held in a cookie and linked to a persistent identifier, allowed the child to return to the site and to be “remembered” to continue to play games or engage with the site.
With the growing debate about “tracking,” the final COPPA rule significantly alters the definition of personal information in important ways. The original definition included a customer number held in a cookie, but the updated rule expands the definition to include IP addresses or other device identifiers except when used for support for the internal operations of the website or online service. For example, persistent identifiers that can be used over time and across different Web sites or online services are now considered “personal information.” The use of “and” rather than the originally-proposed “or” was an important definitional change, since websites and online services use persistent identifiers to “recognize” returning visitors who may register with only a user name and password in the manner described above. Absent that change, this longstanding and privacy-friendly method of allowing children to register anonymously would have been forbidden. It is easy to see that without this exception sites would have had to collect much more information simply to get parental consent at any child-directed site. Similarly, without this exclusion, businesses would have been unable to engage in the type of analytics that help them determine visitor interest in their offerings, improve their content, serve contextual ads, or facilitate a visitor’s experience.

Another important change in the definition of “personal information” was to add pictures, videos, and audio of children as per se personal information. Under the original COPPA rule, a company could offer social engagement of interest to children so long as pictures or videos were not associated with a name, address, or other identifying information. Now, these offerings require parental consent. Sites can continue to allow children to upload videos or pictures of pets, toys or nature at child-directed websites, but they can no longer upload pictures or videos without parental consent. Similarly, geolocation information sufficient to identify a street address was added to the list of personal information. Zip codes and zip plus 4 were not added to the list of per se personal information.

Support for Internal Operations. The change in the definition of personal information requires affected businesses to understand the scope of the exclusion that permits collection of certain limited types of data that is now defined as “personal information” to support the internal operations of a website or online service. This has now become a key point that informs how affected businesses apply COPPA.

Support for the internal operations of the website or online service means those activities necessary to:

(a) maintain or analyze the functioning of the website or online service;

(b) perform network communications;

(c) authenticate users of, or personalize the content on, the website or online service;

(d) serve contextual advertising on the website or online service or cap the frequency of advertising;

(e) protect the security or integrity of the user, website, or online service;

(f) ensure legal or regulatory compliance; or

(g) fulfill a request of a child as permitted by these guidelines; so long as the information collected for the activities listed above is not used or disclosed to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, or for any other purpose. [5]
Under the preamble to the final rule, support for the internal operations also includes other activities, e.g., intellectual property protection, payment and delivery functions, spam protection, optimization, statistical reporting, and de-bugging.[6]

It is easy to see that, absent these exclusions, it would be almost impossible for businesses to offer appropriate online content for kids while managing their businesses responsibly given inclusion of persistent identifiers in the list of personal information. As a result, the FTC concluded that these activities were appropriately carved out to reflect business necessities and operational requirements.

Verifiable Parental Consent. The concept of “verifiable parental consent” is a core requirement of COPPA, but so too is the concept of a “sliding scale” of privacy. As a result, the mode and type of parental consent required under COPPA has always varied depending on circumstances, in particular the potential for privacy harms and related risks to children. There are indeed situations where privacy risks to children are so limited, or countervailing benefits of collection so important, that parental consent is not required. Some activities - like responding to a one-time e-mail request from a child where the e-mail address of the child is promptly deleted - simply do not create significant privacy risks and merit neither parental notification nor parental consent. Others merit parental notification. For example, websites and online services may allow a child to sign up for newsletters or alerts, and collect a parent’s e-mail to provide notice and allow the parent to opt the child out of the activity. In contrast, situations where children could post or share personal information publicly were deemed from the start to merit to the highest level of protection - full verifiable parental consent - largely because exposing that information could potentially put their personal safety at risk.

Parental consent options also varied, and that remains the case under the final COPPA rule. In situations where a business needed to collect more than just an e-mail address from a child - for example, collecting a home address to award a prize - e-mail plus has been an authorized method of obtaining parental consent where the information was collected for marketing engagement only between the child and the brand. Originally considered a potential shorter-term solution in the hope that alternative methods would evolve, the latest round of revisions of COPPA recognized that this method has worked well, balancing privacy and practicality. E-mail plus avoids complications of other parental consent methods, allowing businesses to engage with children and parents so long as the information was not shared with other third parties for marketing purposes. The FTC has recognized that this method remains a useful and privacy-friendly method for obtaining parental consent when information is collected by a website or app for internal marketing purposes only.

The most robust forms of parental consent have been reserved for instances where a child’s personal information would be shared with third parties. The potential risk to a child’s personal safety, not marketing, should information be disclosed was the primary reason for the different forms of consent when the original COPPA rule was adopted, but growing debate about “tracking” fueled some of the changes in the updated COPPA rule. Consent methods include providing a credit card in connection with a transaction, executing consent forms (mail, faxed or scanned and returned to the website operator), or providing a manned toll-free number. The July 2013 final COPPA rule approves additional parental consent methods, including checking a government-issued ID against a database and video conferencing with trained staff. However, the rule does not permit websites and online services to ask a child to share a parent’s mobile phone number for purposes of sending a notice and obtaining consent. In the years since COPPA was enacted, text messaging has become much more common. Allowing a child to share this type of information for purposes of sending notices and obtaining parental consent would be useful to
parents and businesses alike, but the FTC concluded that the legislative language simply did not permit the agency to authorize this type of collection because a mobile phone number is not “online contact information” as defined by the statute.

The final COPPA rule also added a procedure that allows the FTC to consider and approve new alternative consent methods on an expedited basis. Several additional methods have been approved, including methods that involve asking knowledge-based questions that only a parent would likely know. These more robust parental consent methods are now required in connection with photo or video promotions involving children. Use of methods other than transaction-based methods continues to be limited given concerns that parents will be reluctant to share information like Social Security numbers just to allow children to play games or interface with websites. Likewise, because many of these services involve use of infomediaries, many branded companies interested in fostering a trusted relationship with parents have been reluctant to adopt such methods.

The FTC continues to periodically update its “frequently asked questions” about COPPA. The July 2014 updated FAQs suggest that a credit card plus knowledge-based questions, coupled with a way to contact the parent, might suffice in lieu of an actual transaction. Importantly, the verifiable consent mechanisms illustrate that parental consent methods must be “reasonably calculated” to ensure that consent is provided by the parent, so flexibility and evolution are intended. The FTC recently received a request to approve another parental consent method and is soliciting comments on the proposed method.

Notice to Parents. Notices to parents have always been a feature of the COPPA landscape. The updated rule now permits websites that simply collect anonymous information from children to ask for a parents’ e-mail address to notify them that the child is engaged with the site, even if there are no plans to collect additional information from the child. This is a useful change that allows responsible businesses who wish to be sure that parents supervise children’s online activities to notify parents so that they are aware that a child is visiting that site. The FTC and other regulators tend to favor so-called “just in time” notices. The notice provisions of the rule were revised to require different, specific notices depending on the type of data collection involved. Previously, a general notification could be provided that included relevant references to COPPA. The notice change requires additional administrative and operational compliance steps to assure that the correct notice is provided. Whether these notices are indeed more informative to parents than the prior general notice is not yet clear.

Children’s Privacy Policy. COPPA also requires websites and online services, including apps, to post a children’s privacy policy with specific disclosures required by the Act. Affected companies should be sure to review their privacy policies for compliance with the FTC’s disclosure obligations. Notably, the California Online Privacy Protection Act (CalOPPA), which became effective July 1, 2004 requires all websites to post a privacy policy. The Attorney General has interpreted the law to apply to apps as well, and has offered guidance on mobile app privacy. The California Attorney General has also more recently issued general guidance on developing a privacy policy.

Text Messaging. COPPA governs only the online collection of personal information. Consistent with that statutory mandate, online contact information does not include a mobile phone number. However, since any phone number is covered in the list of personal information, collection of a phone number online requires verifiable parental consent. This does create some tricky questions given the growing popularity of text message initiatives with children. While offline collection of a mobile phone number, or purely mobile to mobile communications lacking
any online component, are not subject to COPPA, incorporating an online component triggers COPPA. For example, offering a promotion where entrants can enter online or via text message may trigger COPPA obligations.

Push Notifications. The issue of how push notifications should be handled under COPPA has been an important point of discussion between the FTC staff and the business community. In its July 2014 COPPA FAQs, the FTC staff suggests that certain push notifications may be sent using the “multiple online contact” exception of COPPA, but depending on what other information is actually collected from the child, another form of parental consent may be necessary. However, it may be appropriate to distinguish between “local” or “in-app notifications” and “push notifications.” Notifications that can be delivered within the app, including when the wireless is turned off, may be a form of contextual advertising that is permitted as part of the support for internal operations exception.

Scope of COPPA. COPPA applies to websites and online services directed to children, and to those with actual knowledge that they are dealing with a child. A website that is targeted to children under 13 must generally assume that it is dealing with children; exceptions apply to parent-targeted areas, like a “parent’s corner.” The FTC continues to apply a multi-factorial test to determine when a website or online service is directed to children. Indicia include child-oriented themes and language, use of animated characters, music and other material, as well as advertising. The mere use of animated characters alone does not mean a website is targeted to children, however. Application of this type of multi-factorial analysis is important since many websites and apps involve use of animated characters.

Safe Harbors. Congress enshrined in COPPA formal recognition of safe harbor programs. Complaints about participants in safe harbor programs are submitted to the program. While the final COPPA rule imposes additional requirements on safe harbor organizations, more organizations have filed for safe harbor status since adoption of the rule, bringing the total to seven. [13] Recent filing of Freedom of Information Act (FOIA) requests targeting the safe harbor organizations’ annual reports has led some to voice concerns about the potential disclosure of confidential information related to interactions between members and safe harbor organizations which may inhibit expanded participation.

Enforcement. Congress created a scheme under which the FTC and state attorneys general may enforce COPPA. There is no private right of action under COPPA. State enforcement has been very limited until recently, but the New Jersey Attorney General has brought two actions. The most recent action targeted an app that used geolocation to allow users to play a scavenger hunt game where they could exchange information with others. Although the company contended that the app did not target children under 13, the parties settled the allegations in November, 2013. [14] The FTC has not yet publicly announced settlement of an enforcement action based on violations of the new COPPA rule, but two petitions were filed with the FTC by a public interest group in December 2013 contending that Marvel Entertainment LLC and Sanrio Digital violated COPPA. [15] The complaints took issue with privacy policy disclosures, challenged the scope of permitted activities to promote personalization and support for web operations, and questioned the effectiveness of COPPA safe harbors.

Preemption. When Congress enacted COPPA, it included an express preemption clause as follows at Section 1303(d):

(d) INCONSISTENT STATE LAW.—No State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this
At the time COPPA was enacted, there was robust debate about how to define a “child” for purposes of the Act. No state may impose inconsistent notice or other requirements, and because Congress decided which “minors” were covered, arguably special teen-oriented privacy laws would also be preempted. However, in response to challenges to the District Court’s approval of a settlement agreement of recent litigation regarding Facebook’s “sponsored stories” feature on grounds that COPPA might preempt privacy protections for minors 13 - 18, both the FTC and the California Attorney General filed separate amicus briefs before the Ninth Circuit Court. Both argued that COPPA did not preempt state laws so long as they did not conflict with the COPPA scheme. It is important to remember that other state privacy laws covering, e.g., rights of publicity, may also be at play where the privacy of minors is concerned.

**Challenges for Global Marketers**

The final COPPA rule incorporated a number of changes suggested during the rulemaking process that have helped to assure that businesses can continue to offer child-oriented content and protect children’s privacy by collecting and using certain information necessary to conduct their businesses. For example, without an exclusion from parental consent requirements for support for the internal operations of a website, companies would have had to restructure sites entirely to get parental consent the moment a visitor hit the page, and would have had to actually collect much more personal information to obtain consent. The FTC wisely recognized that a regime that was so restrictive that it would force companies to collect much more information than they actually planned to collect was not a sensible regulatory framework from either a privacy or a business perspective. While not expressed in this fashion, the sliding scale approach may be viewed to reflect how the well-established concept of “proportionality” under EU law might be embodied in a children’s privacy instrument.

As other governments consider legislation governing children’s privacy, it is important to consider whether the legislative language and framework provide adequate operational flexibility for businesses while appropriately protecting children from privacy risks. The FTC’s rulemaking process offered a mechanism to identify and address specific operational, technical and administrative concerns, but aspects of the law itself limited the FTC’s flexibility to adopt common sense options for notifying parents and obtaining consent, such as permitting the collection of a parent’s mobile phone number or e-mail address. If the balance isn’t appropriately struck, the result will likely be the disappearance of content for children or a regime that forces companies to collect much more data simply because they must do so to adequately obtain consent.

*For more information about advertising and privacy & data security issues, contact Sheila A. Millar at millar@khlaw.com or 202 434-4143; or Tracy P. Marshall at marshall@khlaw.com or 202 434-4234.*


