The Metropolitan Corporate Counsel®

www.metrocorpcounsel.com

February 2013 Volume 21, No. 2

FTC Issues Final Amendment To The Children's Online Privacy Protection Rule (COPPA): A Detailed Look At What Has Changed

Dana B. Rosenfeld, Alysa Zeltzer Hutnik and Matthew P. Sullivan

KELLEY DRYE & WARREN LLP

On December 19, 2012, the Federal Trade Commission ("FTC") issued its long-awaited final amendments to the Children's Online Privacy Protection Rule ("COPPA" or the "Rule").[1] COPPA requires commercial websites and online services that are either directed to children under 13 or have actual knowledge that they are collecting personal information from children under 13 to obtain verifiable parental consent before collecting personal information from such children. The final revisions significantly modify or expand key definitions within the Rule, including the definitions of "operator," "personal information," and "website or online service directed to children," and update the Rule's requirements concerning parental notice and consent, and the existing safe harbor provisions. These changes both broaden the scope of online entities that are subject to COPPA and provide new pathways to compliance for certain child-directed sites. The amendments also include new safeguard requirements, including provisions that involve personal data minimization and disposal obligations.

Dana P. Rosenfeld

Alysa Zeltzer Hutnik

Matthew P. Sullivan

The amendments to COPPA, which represent the first revisions to the Rule since it became effective in April 2000, respond to the substantial changes in consumer technology that have occurred during the past decade. FTC Chairman Jon Leibowitz noted in his remarks announcing the amended Rule that ad networks and other online entities have developed "an insatiable desire to collection information, even from kids." Thus, the revisions are intended 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 or applications ("apps") through a mobile device.

The Rule revisions are the product of an extensive rulemaking record compiled over the past 18 months. The Commission proposed and published for comment initial revisions to the Rule on September 27, 2011 ("2011 NRPM"). Based on the response to the Commission's proposal, which included more than 350 comments from consumer groups, industry representatives and others, the Commission proposed and published supplemental amendments for public comment on August 6, 2012 ("2012 SNPRM"). The final amendments will go into effect on July 1, 2013.

Applicability Of The Rule

The COPPA Rule applies to both commercial websites and online services directed to children that collect personal information from a child. The Rule 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.

In the 2011 NPRM, the FTC clarified that the existing Rule already covers the host of emerging technologies that connect online, including mobile applications that allow children to play network-connected games, engage in social networking, make purchases online, receive behaviorally targeted advertisements, or interact with other content or services, as well as Internet-enabled gaming platforms, voice-over-Internet ("VoIP") protocol services, and Internet-enabled location-based services. The Rule also covers some types of texting programs that connect online, including mobile apps that enable users to send text messages from their web-enabled devices without routing through a carrier-issued phone number, and companies' premium texting and coupon texting programs that register users online and send text messages from the Internet to users' mobile phone numbers. Thus, no changes were made to the Rule on this point.

The FTC revised a number of defini-

***Dana B. Rosenfeld** is a Partner and Chair of the Privacy and Information Security Practice. **Alysa Zeltzer Hutnik** is a Partner. She represents clients in all forms of consumer protection matters. **Matthew P. Sullivan** is an Associate who focuses his practice in the areas of advertising, privacy and information security, consumer protection, and food and drug law.*

Please email the authors at drosenfeld@kelleydrye.com, ahutnik@kelleydrye.com or msullivan@kelleydrye.com with questions about this article.

tions within COPPA to either clarify current requirements or broaden the scope of defined terms to account for how children currently access and use online features and content and to encompass technological developments that have occurred since the Rule was enacted. A description of the changes is set forth below.

"Personal information"

An important change to the definitions section is the significant expansion of the term "personal information" to include new forms of data that the FTC now considers personally identifiable.

- *Screen/User Name*. Under the revised Rule, "personal information" includes screen or user names in cases where these identifiers function as "online contact information" as defined in the Rule, except where such names are used solely for the technical maintenance of the online service or website. The Commission also clarified that, under the revised Rule, operators are permitted to use anonymous screen and user names in place of individually identifiable information, including use for content personalization, for filtered chat, for public display on a website or online service, or for operator-to-user communication via the screen or user name.
- *Photographs/Video/ Audio*. In addition, the revised definition covers photographs, and video or audio files containing a child's image or voice.
- *Geolocation Information*. "Personal information" also includes geolocation information emitted by a child's mobile or electronic device. This modification to the Rule expands the existing location-based criteria under "personal information" that includes "a home or other physical address including street name and name of a city or town."
- *Persistent Identifier*. The Commission also broadened the meaning of the term "persistent identifier" as it applies to personal information. Under the existing rule, a persistent identifier – including a website cookie, Internet Protocol ("IP") address, or a device serial number – must be linked to other information relating to a child or parent before it is classified as "personal information" under the Rule. Under the revised Rule, a persistent identifier standing alone is considered "personal information" in instances where it can be used to recognize a user over time and across different websites or online services, except where the identifier is used solely to support the internal operations of the website or online service.[2]
- *Mobile Unique Identifier*. Lastly, a mobile device's unique identifier, or other identifier that can link a child's activities across different websites or online services, also would fall within the "personal information" definition under the revised Rule.

"Collects or collection"

The final revisions update the definition of "collects or collection" to clarify that COPPA covers instances where an operator merely prompts or encourages a child to provide certain information, and not just when the operator mandates that information be provided to access the site. Further, the FTC adopted language to clarify that "collects or collection" includes all forms of passive tracking of a child online, irrespective of the technology used.

The FTC also modified the definition of "collects or collection" as a way to encourage operators to develop new processes that can delete virtually all personal information submitted by children before such information is made public. Specifically, the FTC modified the current "100% deletion standard" that requires an operator to delete all individually identifiable information from its records and from postings by children before they are made public. In its place, the Commission adopted a "reasonable measures" standard whereby operators who use technologies reasonably designed to delete all or virtually all personal information captured from children – before such information is made public – would not be deemed to have "collected" personal information.

"Online contact information"

The FTC modified "online contact information" to clarify that the definition broadly covers all identifiers that permit direct contact with a person online, including, but not limited to, an instant messaging user identifier, a voice over Internet protocol ("VOIP") identifier, or a video chat user identifier.

"Operator"

The FTC modified the definition of "operator" to clarify that the Rule covers child-directed websites or online services that integrate outside services, such as software "plug-ins" or advertising networks, that collect personal information from its visitors. Under the revised Rule, the child-directed content providers are strictly liable for personal information collected by these third parties through its site.

In addition, third-party services, such as plug-ins or ad networks, are covered "co-operators" that are subject to COPPA when they have actual knowledge that they are collecting information through a child-directed site. The definition, however, does not extend liability to platforms, such as Google Play or the Apple App Store, when such platforms merely offer the public access to child-directed apps.

"Release of personal information"

The rule revisions clarify that "release of personal information" pertains to business-to-business uses of personal information, while "public disclosures of personal information" is addressed in COPPA's definition of "disclosure."

"Support for the internal operations of the website or online service"

This term is used in the Rule to designate certain instances in which a website operator may be permitted to use information provided by a child. The FTC's changes expand the list of specific activities that constitute "support for internal operations." For example, the definition now includes activities necessary to perform network communications; authenticate users of, or personalize the content on, the website or online service; serve contextual advertising or cap the frequency or advertising on the online site or service; or ensure legal or regulatory compliance. The Commission also broadened the definition to include "activities necessary to protect the security or integrity of the website or online service" in recognition of the website operators' need for protection from fraud and online security threats.[3]

"Website or online service directed to children"

Whether a website or online service is "directed to children" will continue to be based upon the totality of the circumstances. The FTC, however, revised the definition to create a new compliance option for a subset of websites and online services that are considered "directed to children." Under this new option, a site or service that is directed to children – but that does not target children as its primary audience – may use an age screen to apply all of COPPA's protections only to visitors who self-identify as under age 13. Child-directed sites or services whose

primary target audience is children must continue to presume that all users are children and provide COPPA protections accordingly.

Also, concurrent with the expanded definition of "operator" to include plug-ins and ad networks, the definition of "website or online service directed to children" encompasses third-party sites or services that have actual knowledge that they are collecting personal information directly from users of another website or service directed to children.

Lastly, the FTC expanded the meaning of "audio content" to include music, and expressly noted in the definition that the use of a child celebrity on a website or online service is a strong indicator of the site's appeal to children.

Parental Notice

Streamlining Parental Notice

The existing COPPA Rule requires that a website or online service operator provide parents with two forms of notice concerning its intent to collect or use a child's information: (1) through the website or online service ("online notice"); and (2) through direct outreach to a parent whose child seeks to register on the site or service ("direct notice"). The revised Rule streamlines the notice requirements in an effort to give parents easy-to-understand information provided on a real-time basis. This proposed revision is consistent with the FTC's previously stated preference that disclosure and notice information be "delivered at a time and in a context that is relevant to the consumer's decision about whether to allow the data collection or use," rather than listed within lengthy privacy policies or terms of use.

Specifically, operators must provide notices through "just in time" messages that describe an operator's information practices at the most relevant points of interaction. The Rule revisions further describe the precise information that operators must provide to parents regarding: (1) the personal information that the operator has already obtained from the child; (2) the purpose of the notification; (3) actions that the parent must or may take; and (4) how the operator intends to use the personal information collected.

For example, with respect to the content of the notice used to obtain a parent's affirmative consent, the revised Rule requires that the operator's notice state that (1) the operator collected the parent's contact information for the purpose of providing notice to the parent; (2) the parent's consent is required for the collection, use, or disclosure of such information, and the operator will not collect, use, or disclose such information without the parent's consent; (3) all items of personal information the operator intends to collect if and when the parent provides consent; (4) the means by which the parent can provide verifiable consent; and (5) that the parent's contact information will be deleted from the operator's records if the parent does not provide consent within a reasonable time from the date of notice. In addition, the FTC will now require that all forms of direct notice include a hyperlink to the operator's online notice of its information practices.

FTC Retains the "Single Operator Designee" Requirement

The 2011 NRPM proposed to 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 existing Rule – provide contact information that includes the operator's name, physical address, telephone number and email address. The proposed revision was intended to address the mobile app environment in which multiple parties, including app developers, advertising networks, and service providers are responsible for different functions in delivering the app to the consumer. In response to industry concerns that this proposal, if implemented, would have confused parents due to the potentially large volume of information that they would receive from disparate operators, the Commission elected to retain the Rule's single operator designee proviso. Under this approach, the primary operator must list all other operators that collect or maintain personal information from children through its website or online service. The operator also must list contact information for an operator designated to respond to parents' inquiries.

No Lengthy Policies for Parental Notice

The FTC's final revision to the Notice section eliminates the use of lengthy privacy policies to provide online notice and, instead, requires a simple statement that describes: (1) the information that the operator collects from children, and whether the child can make information publicly available on the operator's site; (2) how the operator uses the child's information; and (3) the operator's disclosure practices for such information. The change is intended to provide consumers with more readily available and easy-to-understand information, given that an increasing amount of online content is provided over mobile devices with smaller screen sizes.

Parental Consent Mechanisms

Expanded Types of Parental Consent

The Commission adopted several substantial changes to the mechanisms that an operator can use to obtain verifiable parental consent before it can collect, use or disclose information obtained from children. For example, the proposed revisions 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. Operators could use such information for verification purposes only.

Payment System and Credit Card Consent only for Transactions

The Rule also would clarify that credit card information can be used for verification purposes only in instances where the parental consent is needed to facilitate an actual monetary transaction. In addition, the Commission will now allow the use of alternative payment systems (such as an iTunes username and password) to verify parental consent in connection with a monetary transaction, provided that the alternative system can meet the same stringent criteria as a credit card (for example, the payment system operator must provide notification of each discrete monetary transaction to the primary account holder).

Preserving Email Plus Verification

In the 2011 NPRM, the FTC proposed eliminating the "email plus" method of verification currently used by operators that collect children's personal information for internal use only. The method requires operators to obtain consent through an email to the parent, in concert with a separate verification step such as confirming the parent's consent by letter or telephone. In response to public comments on the Commission's proposal, the Commission has decided to retain email plus as an acceptable method for opera-

tors that collect personal information for internal use only.

In addition, the Commission is implementing a new process through which operators may voluntarily seek Commission approval of potential consent mechanisms. Applicants seeking approval must submit to the FTC a description of the mechanism, along with an analysis of how it complies with COPPA. The mechanism then will be subject to public comment before the Commission grants approval.

Safe Harbor Parental Consent Okay

The FTC also added a provision to the Rule stating that operators participating in an FTC-approved safe harbor program may use any parental consent mechanisms deemed by the safe harbor program to meet COPPA requirements.

Confidentiality And Security Of Children's Personal Information

Security Safeguards Required with Third Parties

COPPA requires operators to establish reasonable procedures to protect the confidentiality, integrity and security of children's personal information; however, the existing rule is silent on the data security obligations of third parties. The revised Rule includes a requirement that operators take "reasonable steps" to release children's personal information only to third parties that provide assurances to the operator that they can and will maintain the confidentiality, security and integrity of such personal information.

Data Minimization Requirements

The revised Rule also imposes a new data retention and deletion requirement, whereby operators can retain children's personal information only for so long as is reasonably necessary to fulfill the purpose for which the information was collected. The operator also is required to take reasonable measures to protect against unauthorized access to the information during the data deletion or disposal process.

The Role of Self-Regulation Programs

COPPA permits operators to participate in safe harbor programs that have created guidelines that protect children's online privacy to the same or greater extent as COPPA, and include processes to ensure that member participants comply with the program's provisions. Operators that fully comply with an approved safe harbor program are deemed to be in compliance with the Rule for purposes of enforcement. The FTC has made several modifications to the manner in which it will oversee safe harbor programs:

- Annual Audits of Program Members. Under the existing rule, safe harbor programs are required only to conduct "periodic reviews" that may be conducted "on a random basis" to assess an operator's compliance with the program. Under the amended Rule, the safe harbor programs must conduct annual, comprehensive reviews of each of their members' information practices as a way to improve accountability and transparency of such programs.
- Report Periodically to the Commission. The Commission has modified the existing requirement that safe harbor programs maintain records of consumer complaints, disciplinary actions and the results of independent assessments for three years, which must be made available to the Commission upon request. Under the revised Rule, each safe harbor program is required to submit an annual report to the Commission that includes an aggregated summary of the results of the annual independent audits conducted on program members. Notably, this change to the Rule is less stringent than the 2011 NPRM proposal, which would have required the safe harbor programs to expressly name each member operator that is subject to disciplinary action based upon the safe harbor program's annual comprehensive review.
- Provide FTC with Detailed Capabilities Overview. The Commission has added a new requirement that program applicants include with their safe harbor application a detailed explanation of their business model and the technological capabilities and mechanisms they will use to assess an operator's fitness for membership in the safe harbor program.

Conclusion

The FTC's amendments to COPPA impose significant new requirements on operators relating to who is subject to the Rule, parental notice and consent, the types of information that an operator can collect from children, and how such information must be protected. Because the FTC is able to levy fines of up to $16,000 per violation for non-compliance with the COPPA Rule, all companies that either collect information from children or operate a website or online service that may be attractive to children should carefully assess their legal obligations under the revised Rule.

In his remarks announcing the amended COPPA Rule, Chairman Leibowitz noted that the FTC takes "special care discharging [its] duty to safeguard the privacy of the most vulnerable members of our society – first and foremost among them, our nation's children." During the past two years, the FTC has repeatedly demonstrated this point by pursuing enforcement actions against a number of online entities for violations of the Rule, and the Commission has given every indication that it will continue to aggressively enforce the revised Rule in 2013. In December 2012, the FTC released the report "Mobile Apps for Kids: Disclosures Still Not Making the Grade," which described how very few mobile app developers or app stores provide privacy policies, disclosures or other information that enable parents to determine what data is collected from their children and how that information is used or shared with third parties. The report noted that FTC staff has already launched multiple non-public investigations to determine whether certain entities in the mobile app ecosystem are violating COPPA.

---

1 16 C.F.R. Part 312.

2 The Commission considers "different" websites or online services as those that are unrelated to each other, or sites or services where the affiliate relationship is not clear to the user.

3 Under the revised Rule, the Commission also created a new voluntary process whereby parties can request Commission approval for additional activities to be included within the definition of "support for internal operations." These requests will be placed on the public record for notice and comment, and the Commission will act on the request within 120 days. *See new* Section 312.12(b).