Bloomberg BNA

Privacy and Security Law Report®

What You Need to Know About the Revised COPPA Rule

BY D. REED FREEMAN JR., JULIE O'NEILL, AND CINDY P. ABRAMSON

Significant changes to the Federal Trade Commission's rule implementing the Children's Online Privacy Protection Act (the "Rule") will come into force July 1.[1] The quickly approaching effective date should prompt operators of all websites, apps, social plug-ins, advertising networks and other online services (each, a "Service") to take a fresh look at their practices. Some will be newly subject to the Rule's requirements. Others, already covered by the Rule, will have to review their compliance procedures to determine whether any changes are needed. Below we highlight some of the Rule's most noteworthy changes. We also touch on certain frequently asked questions (FAQs) recently issued by commission staff in an effort to help companies come into compliance.[2]

Reed Freeman is a partner, Julie O'Neill is of counsel, and Cindy Abramson is an associate in Morrison & Foerster LLP's Privacy and Data Security Practice Group.

1. The scope of the Rule is now much broader. Consider whether this affects your compliance obligations.

Under the Rule, the online collection of "personal information" from a child under age 13 generally triggers an operator's obligation to provide notice to a parent, obtain the parent's verifiable consent, and comply with other requirements. The commission has revised the Rule to expand the definition of "personal information" to include the following:

- ***A photo, video, or audio file*** that contains a child's image or voice. The current Rule deems a photo to be personal information only if it is combined with other information that permits the contacting of a child. The commission justified doing away with that condition with the reasoning that photos, videos, and audio files are inherently personal and may, on their own, be used to identify individuals if, for instance, they are embedded with geolocation data or analyzed with facial recognition software. It follows that the staff's FAQs explain that an operator will not have triggered the Rule if it prescreens photos prior to posting and either blurs the facial features of any pictured children or deletes any personal information contained in the photos (including images of children and geolocation metadata).[3] In its FAQs, the staff also explains that an operator does not have to obtain parental consent for photos, videos, and audio files it has collected prior to the revised Rule's effective date, but it recommends that, as a best practice,

[1] Children's Online Privacy Protection Rule; Final Rule, 78 Fed. Reg. 3971 (Jan. 17, 2013) (to be codified at 16 C.F.R. pt. 312), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-01-17/pdf/2012-31341.pdf. The commission announced the final revised Rule Dec. 19, 2012 (11 PVLR 1833, 12/24/12).

[2] FTC, *Complying with COPPA: Frequently Asked Questions* (May 2013), http://business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions (12 PVLR 733, 4/29/13). The FAQs represent the views of the FTC staff and are not binding on the commission.

[3] *See* FAQs E2 and E3.

 ISSN 1538-3423

the operator either do so or discontinue its use and disclosure of such materials.[4]

- ***Geolocation information***, if it provides information at least equivalent to street name plus city or town. Interestingly, the staff's FAQs explain that the addition of geolocation information to the definition of ''personal information'' is really just a clarification of—and not a change to—the existing COPPA Rule, which already includes ''a home or other physical address including street name and name of a city or town'' in the definition of ''personal information.'' For this reason, FTC staff says that an operator must obtain parental consent ''immediately'' for already collected geo-location information.[5]

- ***Screen or user name***, when it functions as ''online contact information,'' another type of ''personal information.''[6] In its ''Statement of Basis and Purpose'' accompanying the revised Rule, the commission addressed the concern that the inclusion of screen and user names in the definition of ''personal information'' would limit operators' ability to offer interactive features because they would be constrained by compliance obligations. The commission explained that the definition is intended to cover ''direct, private, user-to-user contact'' and not the use of anonymous screen or user names for purposes of, for example, content personalization, filtered chat, public display, operator-to-user communication, or to allow children to log in across devices. Accordingly, the revision should generally not affect operators' ability to use user or screen names in place of individually identifiable information and thereby avoid triggering the Rule's obligations. In its FAQs, the FTC staff says that an operator is not required to obtain parental consent for already collected screen or user names, but it encourages operators to do so, as a best practice. The FTC staff also explains that a previously collected screen or user name is covered by the Rule if the operator associates new personal information with it after the revised Rule takes effect.[7]

- ***A persistent identifier***, such as a customer number held in a cookie, an internet protocol (IP) address, a processor or device serial number, or a unique device identifier, where it can be used to recognize a user over time *and* across different sites or online services.[8] This is a significant expansion of the Rule's coverage. *The current version of the Rule (effective only until June 30) provides that persistent identifiers constitute ''personal information''—and thus trigger the Rule—only when they are associated with individually identifiable information, such as name or email address*. This change to the Rule codifies the commission's position that information associated with a device is ''personal,'' and it dramatically affects compliance obligations: *Effective July 1, the collection of persistent identifiers, as defined above, on their own, will trigger the Rule's obligations*. The commission did, however, provide businesses with some relief by exempting from the Rule's parental notice and consent obligations the use of persistent identifiers *solely to support the Service's internal operations*. As a practical matter, this means that:

  o *An operator does not have to comply with the Rule's notice and consent obligations if it uses persistent identifiers solely to support its internal operations*. The Rule defines such ''support'' as *only* those activities necessary to do any of the following, provided that the information collected is not used to contact a user (including through behavioral advertising), to amass a profile on a user, or for any other purpose: (1) maintain or analyze the functioning of the Service; (2) perform network communications; (3) authenticate users; (4) personalize the content on the Service;[9] (5) serve contextual advertising on the Service;[10] (6) cap the frequency of advertising; (7) protect the security or integrity of the user or Service; (8) ensure legal or regulatory compliance; or (9) fulfill a permitted request of a child.[11] The revised Rule permits a party to seek commission approval of additional activities to be included within the ''internal support'' definition.

  o *An operator must comply with the Rule's notice and consent requirements if it uses persistent identifiers for any other purpose, including to contact a user or for retargeting or other behavioral advertising*. The commission intends the activities enumerated within the ''internal support'' definition to be narrowly construed. If a persistent identifier is used for any nonenumerated purpose, it is ''personal information'' and triggers the Rule's requirements.

  The FTC staff explains in its FAQs that an operator does not have to obtain parental consent for an already collected persistent identifier, but if it associates new personal information with it after July 1, then it must do so (unless the collection is solely for the support of the Service's internal operations).

2. Third parties that collect personal information through a COPPA-regulated Service are now expressly covered by the Rule. Even more importantly, operators of COPPA-regulated Services are now strictly liable for their compliance.

The commission has set forth new standards for which party (or parties) is liable for COPPA compliance when a third-party service—such as an ad network or a

[4] *See* FAQ A4.

[5] *Id.*

[6] Under the current Rule, a screen or user name does not fall within the definition of ''personal information'' unless it contains an individual's email address. 16 C.F.R. § 312.2 (2005) (definition of personal information); *see also* 78 Fed. Reg. at 3971, 3978.

[7] *See* FAQ A4.

[8] The term ''different'' means either Services that are unrelated to each other or Services where the affiliate relationship is not clear to the user. 78 Fed. Reg. at 3971, 3980.

[9] According to the commission, ''personalizing content'' would permit operators to, for example, maintain user-driven preferences, such as game scores or character choices in a virtual world. 78 Fed. Reg. at 3971, 3979.

[10] Contextual advertising is ''the delivery of advertisements based upon a consumer's current visit to a web page or a single search query, without the collection and retention of data about the consumer's online activities over time.'' FTC, Preliminary Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, 55 n. 134 (Dec. 2010), *available at* http://ftc.gov/os/2010/12/101201privacyreport.pdf (9 PVLR 1642, 12/6/10).

[11] The commission's ''Statement of Basis and Purpose'' for the revised Rule notes that the following activities are included within the definition's categories: intellectual property protection, payment and delivery functions, spam protection, optimization, statistical reporting, and de-bugging. 78 Fed. Reg. at 3971, 3981.

  PVLR ISSN 1538-3423

social plug-in—is integrated into a child-directed site or service. Specifically:

- ***The host operator is responsible for the activities of a third party that collects personal information on the host's Service if: (1) the third party is an agent or service provider of the host, or (2) the host benefits by allowing the third party to collect personal information directly from users.***[12] This revision reflects a shift from prior commission statements indicating that an entity had to have ownership, control, or access to the personal information at issue in order to be liable as an operator with respect to it. The commission has now taken the position that a strict liability standard is appropriate because the host is in the best position to know and control which plug-ins, software downloads, and other services it integrates into its Service and is also in the best position to give notice to and obtain consent from parents. In fact, in its FAQs, the staff says that an operator must inquire into the information collection practices of every third party that can collect information via the operator's Service.[13] The operator can assess its compliance obligations only if it has this information.[14]

- ***A third party that collects personal information through another operator's Service—such as an ad network or a social plug-in—will be considered ''directed to children'' and therefore itself subject to the Rule if it has actual knowledge that it is collecting personal information from users of a Service directed to children.*** The commission declined to impose a strict liability standard on such third parties, recognizing the logistical difficulties that they face in controlling and monitoring the sites that incorporate their services. That said, the commission suggests that the ''actual knowledge'' standard may not be difficult to meet, as it will generally be met when: (1) the host Service communicates to the third party about its child-directed nature, or (2) a representative of the third party recognizes the child-directed nature of the host's content.[15] This test could raise compliance issues, since whether or not a particular Service is ''directed to children'' under the Rule is a question that involves multiple factors and may not be readily ascertainable by employees of the third party. Moreover, given that the third party could be held liable for the knowledge of any one of its employees, it must train them to take appropriate action in the event that they believe that the host Service could be child-directed.

  In its FAQs, the staff explains that the operator of a child-directed Service is not required to inform third parties of the child-directed nature of the Service, but the staff recommends that it signal this to the third party because the host operator is strictly liable for the collection of personal information from its users, including by a third party. The operator may then arrange with the third party to provide adequate COPPA protections.[16]

3. The revised Rule streamlines the parental notice requirements. Consider whether changes to your direct notice and privacy policy are required.

An operator subject to the Rule must provide parents with notice of its information practices in two ways: in a notice delivered directly to the parent and on the Service itself (typically through the posting of a privacy policy). The commission has revised the Rule to rely less on the posted privacy policy and more on the direct notice.

- ***Direct notice to parents:*** Under the revised Rule, the direct notice is intended to work as an effective ''just-in-time'' communication to a parent about the operator's information practices. The commission has revised the Rule to prescribe the disclosures that must be made in each type of direct notice,[17] to ensure that a parent receives key information up front and is directed, via link, to the full privacy policy for additional information.

- ***Online notice (the privacy policy):*** The revised Rule streamlines the content of the COPPA privacy policy by requiring that it include only: (1) the operator's contact information; (2) the information that the operator collects from children, including whether the site or service permits a child to make personal information publicly available, such as through a message board or chat room; (3) how the operator uses such information; and (4) its disclosure practices.

4. If you are an app developer, review the staff's guidance on providing notice and obtaining consent.

With respect to mobile apps, the staff explains that the privacy policy must be placed on the app's home or landing screen; it does not require that the policy appear at the point of purchase or download, such as in the app store, though the commission encourages that as a best practice.[18]

If an app will collect personal information as soon as it is downloaded, the operator should provide direct no-

[12] The ''benefit'' to the host Service could be, for example, through the addition of content, functionality, or advertising revenue. The commission explains in its ''Statement of Basis and Purpose'' for the revised Rule that platforms—such as those that offer mobile apps—are not liable if they merely offer access to content provided by others. 78 Fed. Reg. at 3971, 3977.

[13] *See* FAQ D8.

[14] Importantly, the commission notes in its ''Statement of Basis and Purpose'' for the revised Rule that, ''[a]lthough this issue is framed in terms of child-directed content providers integrating plug-ins or other online services into their sites because that is by far the most likely scenario, the same strict liability standard would apply to a general audience content provider that allows a plug-in to collect personal information from a specific user when the provider has actual knowledge the user is a child.'' 78 Fed. Reg. at 3971, 3976.

[15] The commission explains that these two examples are not exhaustive, and ''an accumulation of other facts'' could also establish actual knowledge. 78 Fed. Reg. at 3971, 3978.

[16] *See* FAQ D6.

[17] The type of notice depends on the type of consent sought: ''Notice to Obtain Parent's Affirmative Consent to the Collection, Use, or Disclosure of a Child's Personal Information''; ''Notice to a Parent of Operator's Intent to Communicate With the Child Multiple Times'' (such as via a newsletter); ''Notice to a Parent in Order to Protect a Child's Safety''; and ''Voluntary Notice to a Parent of a Child's Online Activities Not Involving the Collection, Use, or Disclosure of Personal Information.'' The last type of notice is new. It corresponds to a new exception to parental consent, which gives an operator the option to collect a parent's online contact information for the purpose of providing notice of a child's participation in a Service that does not otherwise collect, use, or disclose children's personal information. The parent's online contact information may not be used for any other purpose, disclosed, or combined with any other information collected from the child. 78 Fed. Reg. at 3971, 4010–12.

[18] *See* FAQ C9.

tice and obtain parental consent at the point of purchase, or it should insert a landing page to do so before the download is complete.[19] The staff explains in its FAQs that an operator may not rely on a parent's app store account number or password, without some other indicia of reliability, to meet the Rule's consent requirements. The staff explains that this information, alone, does not provide sufficient assurance that the person entering the information is the parent and not the child.[20]

5. Evaluate whether your practices comply with the revised Rule's new data security and retention obligations.

- ***The revised Rule imposes pass-through data security obligations.*** The existing Rule requires an operator to maintain procedures to protect the confidentiality, security, and integrity of children's personal information. The revised Rule strengthens that obligation by requiring an operator to take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining its confidentiality, security, and integrity and who provide assurances that they will do so.[21] The FTC staff believes that this requires an operator to: (1) determine what the service provider or third party's practices are for maintaining security and confidentiality and preventing unauthorized access or use; (2) expressly address expectations for treatment of children's personal information in its contract with the service provider or third party; and (3) use reasonable means, such as periodic monitoring, to confirm that the service provider or third party is maintaining the security and confidentiality of the information.[22]

- ***The revised Rule imposes limits on data retention.*** Because the commission views the deletion of unneeded personal information as an integral component of a reasonable data security program, it has added the requirement that an operator retain personal information ''for only as long as is reasonably necessary to fulfill the purpose for which the information was collected.'' Thereafter, the information must be deleted in a manner that safeguards against a breach.

[19] *See id.*

[20] *See* FAQ H10.

[21] This obligation covers only business-to-business disclosures and not, for example, the disclosure of a child's personal information through a site's social networking-type features. 78 Fed. Reg. at 3971, 3994.

[22] *See* FAQ K1.

6. The revised Rule gives certain child-directed Services some compliance flexibility. At the same time, the staff seeks to impose new requirements on them. Determine whether these changes affect you.

- ***The revised Rule permits certain Services that are ''directed to children'' to comply only with respect to those users who self-identify as under 13.*** A Service that fits within the Rule's definition of ''directed to children'' but that does not target children under 13 as its primary audience can be deemed not ''directed to children'' if it age-screens all users and then provides notice and obtains parental consent (and otherwise complies with the Rule) only with respect to those who indicate that they are under 13.

  On the other hand, a Service that targets a primary audience of children under 13 must continue to presume that all users are children, subject to the requirements of the Rule. The commission provides little guidance on what it means to target a ''primary audience'' of children. In its ''Statement of Basis and Purpose,'' it explains that the determination must be based on the totality of the circumstances and not on some precise threshold cut-off.

- ***The staff takes the position that a Service that is directed to children but does not target children under 13 as its primary audience may not, after age-screening, completely block children from the Service.*** Instead, it is the staff's view that the Service must offer some content to children who self-identify as under 13.[23] Although neither the COPPA statute itself nor the revised Rule imposes an affirmative obligation to provide content, the staff's apparent theory for this requirement is that such a Service may not completely block children because it knows that it will attract them, including those who return after having been age-blocked.[24] It is not clear from the FAQs what the staff believes that such a Service *must do*—perhaps offering a minimum of content would suffice—only what such an operator apparently *cannot do*, which is to block age-screened children under 13 altogether.

* * *

The revised Rule's effective date is not far off. Both those companies that are already subject to the Rule, as well as those that will be newly subject to it, are advised to take a careful look at the revisions, along with the commission's ''Statement of Basis and Purpose'' and the staff's FAQs, to help ensure compliance as of July 1.

[23] *See* FAQs D2, D4, and G2.

[24] The staff does not extend this obligation to general audience Services that age-screen.

  PVLR ISSN 1538-3423