Bloomberg BNA

Privacy and Security Law Report®

No More Kidding Around: How the Amendments to the Children's Online Privacy Protection Rule Affect Websites and Other Online Service Providers

BY MATTHEW SAVARE

The regulations implementing the Children's Online Privacy Protection Act (COPPA) got a sweeping overhaul Jan. 17, when the Federal Trade Commission (FTC) published its final rule amendments (the Rule).[1] The Rule, which the FTC issued to clarify the scope of its regulations and strengthen the protection for children's personal information, is the first amendment since the original regulations became effective in April 2000.

Since 2000, there has been an explosion in online and digital technologies, including the advent of mobile applications, online gaming, social media, geolocational data, and behavioral advertising. The Rule seeks to address these developments along with a host of other issues. Aside from altering the landscape regarding the collection, usage, and disclosure of children's personal information, the Rule may provide insight into how the FTC may regulate privacy more generally in the future. The Rule will go into effect July 1.

Here is a brief overview of COPPA and an analysis of the new Rule.

What Is COPPA and Who Must Comply?

COPPA regulates the collection, use, and disclosure of ''personal information'' from and about children,[2] whom the Rule defines as any individuals under the age of 13.[3] The statute applies to ''any operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child.''[4] Although the regulations do not define ''online service,'' the FTC's Sept. 27, 2011, notice of proposed rulemaking made clear that the term ''broadly covers any service available over the Internet, or that connects to the Internet or a wide-area network,'' including ''mobile applications that allow 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[, and] . . . Internet-enabled gaming platforms, voice-over-Internet protocol services, and Internet-enabled location based services.''[5]

One significant change ushered in by the Rule is the new standard for first-party operator liability. Under the Rule, websites and online services are now responsible for any children's personal information collected on the site or service by: (1) their agents or service providers or (2) third-party services, such as ad networks, plug-ins, and software downloads, when the operators benefit from such collection.[6] Under the prior regulations, liability attached only if the operator owned or controlled the third party or had access to the data. The FTC states that this new standard is necessary to close

[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 (11 PVLR 1833, 12/24/12).

Matthew Savare is a partner at Lowenstein Sandler LLP. He practices intellectual property, media, entertainment, technology, and privacy law with a particular focus on new media. His email is msavare@lowenstein.com.

[2] *See* Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506.

[3] 16 C.F.R. § 312.2.

[4] 16 C.F.R. § 312.3; *see also* 15 U.S.C. § 6502(a)(1).

[5] *See* Section IV of Children's Online Privacy Protection Rule; Proposed Rule, 76 Fed. Reg. 59803 (Sept. 27, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-09-27/pdf/2011-24314.pdf (10 PVLR 1327, 9/19/11).

[6] *See* definition of ''Operator'' at 16 C.F.R. § 312.2.

 ISSN 1538-3423

the perceived ''loophole'' where personal data were being collected, but no party was responsible under COPPA.[7]

Under the Rule, third parties will be subject to COPPA only if they have ''actual knowledge'' that they are collecting personal information directly from users of another website or online service that is ''directed to children.''[8] Although urged to so from many industry commenters, the FTC provided little guidance as to when a plug-in or advertising network would be deemed to have ''actual knowledge'' that it is collecting information through a child-directed site or service, stating instead in commentary to the Rule that:

> Knowledge, by its very nature, is a highly fact-specific inquiry. The Commission believes that the actual knowledge standard it is adopting will likely be met in most cases when: (1) A child-directed content provider (who will be strictly liable for any collection) directly communicates the child-directed nature of its content to the other online service; or (2) a representative of the online service recognizes the child-directed nature of the content. The Commission does not rule out that an accumulation of other facts would be sufficient to establish actual knowledge, but those facts would need to be analyzed carefully on a case-by-case basis.[9]

This standard is problematic for third parties for several reasons. First, it appears to create an imputed knowledge standard where a company could be held liable by the knowledge of one of its employees. Second, given the complex, multifactor analysis discussed below to determine if a website or online service is indeed ''directed to children,'' how are such employees expected to ''know'' the ''child-directed'' nature of a site or service? Finally, the catchall phrase at the end of the quote above indicates that liability is not limited to the two examples set forth by the FTC, thus creating uncertainty and ambiguity for third parties.

Despite requests from consumer groups and an earlier proposed rule to expand broadly the definition of the phrase ''directed to children,'' the Rule maintains the FTC's multifactor test, but adds two elements to be considered in the analysis. Specifically, as it had done under its initial regulations, the FTC will continue to evaluate the website's or online service's:

> subject matter, visual content, use of animated characters or child-oriented activities and incentives, . . . age of models, . . . language or other characteristics, . . . whether advertising promoting or appearing on the Web site or online service is directed to children[,] and empirical evidence regarding audience composition and evidence regarding the intended audience.[10]

The Rule now permits the FTC to consider the ''music or other audio content'' and the ''presence of child celebrities or celebrities who appeal to children.''[11] In addition, a website or online service shall be deemed ''directed to children'' when it has actual knowledge that it is collecting personal information directly from users of another website or online service directed to children.

The Rule also adopted an exception to the ''directed to children'' definition. Specifically, if a website or online service that would otherwise be considered ''directed to children'' under the above criteria does not target children as its **primary audience**, it will not be deemed ''directed to children'' if it age screens users prior to collecting any personal information and then complies with the notice and parental consent requirements (as discussed below) before collecting, using, or disclosing the personal information of any users identifying themselves as under 13.[12]

The Rule broadens the definition of ''collection'' to include not only the collection of personal information that an operator **mandates** a child input, but also the collection of any personal information that an operator: (1) ''prompts'' or ''encourages'' a child to submit or (2) obtains by passively tracking a child online.[13] The FTC justified this addition to clarify that operators cannot shield themselves from COPPA compliance by simply not requiring a child to provide personal information. The Rule does, however, broaden the exception to the definition of ''collection'' to exclude any activities if the operator ''takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete such information from its records.''[14] This is a relaxation of the former standard, which imposed a 100 percent deletion standard, as opposed to ''reasonable measures.''

What's Considered Personal Information?

The definition of ''personal information'' is often a vexing question, as states, nations, statutes, and regulations define the term differently. As discussed in greater detail below, the Rule has expanded the definition of ''personal information,'' which now includes any ''individually identifiable information about an individual collected online,'' including:

- a first and last name;
- a home or other physical address, including street name and name of a city or town;
- ''online contact information,'' which is an email address or any other identifier that permits direct contact with a person online;
- a screen or user name where it functions in the same manner as ''online contact information;''
- a telephone number;
- a Social Security number;
- a ''persistent identifier'' that can be ''used to recognize a user over time and across different Web sites or online services,'' 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;
- a photograph, video, or audio file where such file contains a child's image or voice;
- geolocational information sufficient to identify street name and name of a city or town; or

[7] *See* commentary to the Rule at Children's Online Privacy Protection Rule; Final Rule, 78 Fed. Reg. at 3976.

[8] *See* definition of ''Website or online service directed to children'' at 16 C.F.R. § 312.2.

[9] *See* commentary to the Rule at Children's Online Privacy Protection Rule; Final Rule, 78 Fed. Reg. at 3978.

[10] *See* definition of ''Web site or online service directed to children'' at 16 C.F.R. § 312.2.

[11] *Id.*

[12] *Id.*

[13] *See* definition of ''Collects or collection'' at 16 C.F.R. § 312.2.

[14] *Id.*

  PVLR ISSN 1538-3423

- information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.[15]

The Rule's expansion of the definition of ''personal information'' is among its most significant changes. For example, under the former regulations, screen and user names were deemed ''personal information'' only when combined with a child's email address. Under the Rule, however, screen and user names are considered ''personal information'' when they function in the same manner as online contact information.

The Rule also adds to the list of ''personal information'' any information that identifies a specific computer or mobile device, certain geolocational information, and photo, audio, and video files containing a child's image or voice.[16] This is an extremely broad addition to the definition, especially in light of how prevalent social media sites and mobile devices have become and how they have facilitated the sharing of pictures, videos, and audio files.

Similarly, whereas the prior regulations considered ''persistent identifiers'' such as cookies ''personal information'' only when grouped with individually identifiable information, the Rule regards customer numbers held in cookies, IP addresses, processor or device serial numbers, and unique device identifiers as ''personal information.''[17]

Importantly, the Rule mandates that operators are not required to comply with COPPA's notice and consent requirements (discussed below) if such ''persistent identifiers'' are used to support the website's or online service's ''internal operations,'' which the Rule defines as those activities ''necessary'' to:

- maintain or analyze the functioning of the website or online service;
- perform network communications;
- authenticate users;
- personalize the content;
- serve contextual advertising or cap the frequency of advertising;
- protect the security or integrity of the user, website, or online service;
- ensure legal or regulatory compliance; or
- respond to a child's specific request as permitted by Section 312.5(c)(3) and (4) of the Rule.[18]

The Rule makes clear that this exception for the ''support of internal operations'' does not apply if such ''persistent identifiers'' are ''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.''[19]

What Is Required Under COPPA?

Some of the important elements of COPPA include: (1) a requirement that websites and online services: (a) provide notice describing, among other things, what information they collect from children, how they use such information, and their disclosure practices for such information; (b) obtain ''verifiable parental consent'' prior to any collection, use, and/or disclosure of children's personal information; (c) provide a reasonable mechanism for parents to review the personal information collected from their children and to refuse to permit its further use or maintenance; and (d) establish and maintain ''reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children;'' and (2) a prohibition on websites and online services conditioning a child's participation in a game or receipt of a prize on the disclosure of more personal information than is necessary to participate in that activity.[20]

Here are more details regarding the above requirements.

Notice

Operators must make ''reasonable efforts'' to provide parents a direct notice of the operator's privacy practices regarding children's personal information. Although providing parents a link to the operator's privacy policy was sufficient under the former regulations, the Rule now mandates not only a link to the full online policy, but also additional information, as set out in detail in Section 312.4(c) of the Rule.[21]

In addition to this direct notice, an operator must post a ''prominent and clearly labeled link'' to its privacy policy on the home or landing page or screen **and** at each area of the website or online service where personal information is collected from children.[22] For mobile applications, the Rule's commentary notes that although recommended, operators are not required to post such information in every location where the mobile app can be purchased or downloaded.[23] Section 312.4(d) of the Rule specifies the information that must be included in the online privacy policy.

Consent

Section 312.5(b) of the Rule provides the following nonexhaustive list of approved methods for obtaining parental consent, which includes several new ones from the prior rules:

- obtaining from the parent a signed consent form, which is returned to operator by postal mail, fax, or electronic scan;
- requiring a parent to use a credit card, debit card, or other online payment system in connection with a monetary transaction that provides notification of each discrete transaction to the primary account holder;
- having a parent call a toll-free telephone number staffed by trained personnel;
- allowing a parent to connect to trained personnel via video-conference; or
- verifying a parent's identity by checking a form of government-issued identification against databases of such information, where the parent's identifica-

[15] *See* definition of ''Personal information'' at 16 C.F.R. § 312.2.
[16] *Id.*
[17] *Id.*
[18] *See* definition of ''Support for the internal operations of the website or online service'' at 16 C.F.R. § 312.2.
[19] *Id.*
[20] 16 C.F.R. § 312.3.
[21] 16 C.F.R. § 312.4.
[22] *Id.*
[23] *See* commentary to the Rule at Children's Online Privacy Protection Rule; Final Rule, 78 Fed. Reg. at 3986.

> tion is deleted by the operator from its records promptly after such verification is complete.

In addition, when an operator collects and uses children's personal information for internal purposes only, it may obtain parental consent by the so-called ''email plus'' method, which allows the parent to send the operator an email coupled with an additional step to demonstrate that the person is, in fact, the parent. Such an additional step has included the operator sending a confirmatory email to the parent after receiving consent or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. Any operator that employs the ''email plus'' method must provide the parent notice that he or she can revoke any consent given in response to the earlier email.[24]

Security

As noted above, the regulations require operators to establish and maintain ''reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.'' The Rule extends this requirement and now mandates that operators employ ''reasonable steps'' to release children's personal information only to third parties and service providers that are capable of providing similar safeguards and that provide assurances that they will do so, either by contract or otherwise.[25] This extension to third parties mirrors the requirements set forth in other privacy regulations with respect to personal and sensitive information, such as the Safeguards Rule of the Gramm-Leach-Bliley Act and Massachusetts' comprehensive data privacy regulations.

In addition, the Rule also introduces into COPPA the best practices principle of ''retention limitation.'' Simply, operators may now maintain children's personal information for ''only as long as is reasonably necessary to fulfill the purpose for which the information was collected.'' After such time, the operator must delete the information.[26]

[24] 16 C.F.R. § 312.5.
[25] 16 C.F.R. § 312.8.
[26] 16 C.F.R. § 312.10.

Safe Harbor

The original regulations created a safe harbor framework whereby operators could self-certify to certain FTC-approved programs, such as TRUSTe, and be deemed in compliance with COPPA. The Rule creates three additional requirements for these safe harbor programs. First, safe harbor programs must conduct at least one comprehensive annual review of each operator's information policies, practices, and representations to verify that the operator is in compliance with the regulations. Second, safe harbor programs must submit reports to the FTC outlining their reviews of participating operators, detailing any disciplinary actions, and documenting any approvals of member operators' use of a parental consent mechanism. Finally, new safe harbor program applicants must provide the FTC with descriptions of their business models and technological capabilities to assess operators' eligibility to self-certify.[27]

Closing Thoughts

Although the new COPPA regulations do not go as far as some privacy advocates would like, the Rule does impose many new obligations on websites, online service providers, and the companies that support and do business with them, such as ad networks and service providers. Care must be taken when navigating this new regulatory regime. In addition, the Rule should serve as an indication as to how the FTC may implement new privacy regulations in the future with respect to other industries and other types of data. For example, the greatly expanded definition of ''personal information'' indicates the FTC's willingness to expand the scope of privacy regulation, at least with respect to data relating to children. Broadening the definition in connection with data not relating to children, such as an adult's IP address or photograph, would have profound implications on many other industries, including internet, mobile, and online advertising, as much more data would be subject to privacy regulation. In light of the new COPPA regulations and the FTC's increased emphasis on information privacy, such a scenario seems likely and imminent.

[27] 16 C.F.R. § 312.11.

  PVLR ISSN 1538-3423