January 19, 2024

Complying with the Children's Online Privacy Protection Rule; FTC's Proposed Updates

by Tatum Andres

On December 20, 2023, the Federal Trade Commission (FTC) published a Notice of Proposed Rulemaking (Proposed Rule) seeking to update the Children's Online Privacy Protection Act (COPPA), which would place new restrictions on the use and disclosure of children's personal information. COPPA applies to operators of websites and online services that are "directed" to children under 13 or that have "actual knowledge" that they are collecting personal information from children under 13.[1] COPPA imposes cumbersome notice, parental consent, data security, and data minimization requirements, among other things.

If your company markets to children under 13 years old, or deals with data of children under 13, you are probably aware of COPPA and your current obligations. The FTC's new Proposed Rule significantly increases legal obligations and therefore legal risks, so it is recommended that all companies review their information practices and online privacy policy. In doing so, we recommend that companies scrutinize:

- The details of the information gathered;
- The methods employed for data collection;
- The purposes of usage;
- The necessity of the information for the company's website, mobile app, or online service activities;
- The effectiveness of mechanisms for notifying parents and obtaining verifiable consent; and
- The availability of adequate procedures for parents to review and delete their children's information.

After conducting this review, we recommend that all companies implement robust data security, retention, and deletion practices.

The following is a summary of key updates of the Proposed Rule.

Mixed Audience Sites: The Proposed Rule clarifies the scope of COPPA's application to mixed audience sites, which are sites designed for children but do not have children as their primary audience. These platforms are prohibited from gathering, utilizing, or revealing user information without verified parental consent, unless they employ reasonable means to determine if a user is a child.[2] The Proposed Rule would allow companies to apply COPPA protections exclusively to users under the age of 13. Notably however, for that exception to apply, the

online service cannot set a default age (e.g., pre-populating an age of 18 on a sign-up form) or nudge users to provide an age of 13 or older.

Child Directed Standard Changes: When is an online service "directed to children"? Look at the target audience. To determine the target audience, the Proposed Rule permits the FTC to consider marketing materials, representations to consumers or third parties, reviews by users or third parties, and the age of users on similar websites or services when determining whether a website or online service is directed to children.[3] In practice, the FTC was already using these materials, including the subject matter of a game, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, and presence of child celebrities or celebrities who appeal to children.[4]

If after considering these factors a company determines that their website or service is directed to children, then the company should separately determine whether its website or service falls in the "mixed audience" subcategory i.e., whether children are not your primary audience.

Parental Consent for Disclosure of Children's Personal Information to Third Parties: COPPA already requires verifiable parental consent to ensure that parents are informed about a company's information collection and data sharing practices.[5] Under the Proposed Rule, companies must now obtain separate verifiable parental consent for disclosures of a child's personal information for targeted advertising to third parties.[6] Parents would have the option to refuse disclosure of the child's personal information to a third party but the child's access to the website or online service could not be conditioned on the provision of parental consent.

Newly Available Methods for Obtaining Opt-In Consent: Operators must adopt a method that is reasonably crafted, considering available technology to obtain parental consent.[7] "Knowledge-based authentication" was previously added to the list of methods that qualify as obtaining verifiable parental consent.[8] However, the questions must be of sufficient difficulty that a child aged 12 or younger in the parent's household could not reasonably answer the questions.[9]

Notice to a School for Educational Services: The Proposed Rule expands COPPA's direct notice requirement to the child's school, if applicable (rather than requiring direct notice to a child's parent).[10] Specifically, certain educational technology service providers depend on schools to obtain verifiable consent from parents for the gathering of students' personal information. The Proposed Rule states that under specific circumstances, an operator can obtain consent from a school, rather than a parent, for the collection of child information.

This exception regarding parental consent for education technology was informally adopted by the FTC during the pandemic. The proposal outlines several requirements for relying on the School Authorization exception, including: (1) restricting the use of collected information to school-authorized educational purposes and not for commercial use; (2) establishing a written agreement between the authorizing school and the operator with specific terms; (3) ensuring direct supervision by the school over the operator's use, disclosure, and maintenance of personal information; (4) obligating the operator to publish an online notice with specified

information; and (5) granting the school the right to review and request the deletion of any child personal information. Despite the FTC's clarification that the new School Authorization exception essentially formalizes existing guidance, both schools and operators will need to address unresolved issues, such as determining activities that align with the educational purpose limitation.

In such a case, the operator must ensure that the school receives such notice and must have a written agreement with the school that:[11]

- Indicates the name and title of the person providing authorization and attests that the person has the authority to do so;
- Limits the operator's use and disclosure of the personal information to a school authorized education purpose only and no other purpose;
- Provides that the operator is under the school's direct control with regard to the use, disclosure, and maintenance of the personal information collected from the child pursuant to school authorization; and
- Sets forth the operator's data retention policy with respect to such information.

New Definitions: The FTC has expanded the definition of "personal information" to include geolocation information; photos, videos and audio files containing a child's image or voice as well as biometric identifiers, which are defined as fingerprints or handprints; retina and iris patterns; genetic data, including a DNA sequence; or data derived from voice data, gait data, or facial data.[12]

The Proposed Rule also seeks to define "School" as "a state educational agency or local educational agency, as well as an institutional day or residential school, including a public school, charter school, or private school, that provides elementary or secondary education, as determined under State law."[13]

Finally, the Proposed Rule would add the term "School-Authorized Education Purpose," which it proposes to define as "any school-authorized use related to a child's education."[14] "Uses" under the definition are limited to "operating the specific educational service that the school has authorized, including maintaining, developing, supporting, improving, or diagnosing the service, provided such uses are directly related to the service the school authorized."[15]

Data Security Requirements: In general, the security requirements outlined in the Proposed Rule are reasonable in light of the recent data breaches in all industries, and companies with robust security programs are unlikely to discern a significant difference. These requirements are designed to ensure a high standard of data protection, and organizations already implementing comprehensive security measures will likely find that the stipulated standards align with their existing practices. For companies with well-established security protocols, the prescribed security requirements under the Proposed Rule are consistent with industry best practices, minimizing the need for substantial adjustments.

Under the Proposed Rule, the operator must establish a written children's personal information security program that contains safeguards that are appropriate to the sensitivity of the personal information collected from children and the operator's size, complexity, and nature and scope of activities. In addition to obtaining written assurances that any third parties receiving children's personal information will "employ reasonable measures to maintain the confidentiality, security and integrity of the information" the operator must:[16]

- Designate one or more employees to coordinate the program;
- Perform assessments at least once a year to identify internal and external risks to the confidentiality, security, and integrity of personal information collected from children and the sufficiency of any safeguards in place to control such risks;
- Design, implement, and maintain safeguards to control risks identified through the risk assessments;
- Regularly test and monitor the effectiveness of the safeguards in place to control risks; and
- Evaluate and modify the children's personal information security program at least once a year to address identified risks, results of required testing and monitoring, new or more technological or operational methods to control for identified risks, or any other circumstances that an operator knows or has reason to know may have a material impact on its children's personal information security program or any safeguards in place.

Data Retention and Deletion Requirements: The operator must provide its written children's data retention policy in the notice on the website or online service. In addition to implementing and maintaining a written children's data retention policy that sets forth the purposes for which children's personal information is collected, the business must retain such information, and a timeframe for deletion of such information that precludes indefinite retention because a child's personal information may not be retained indefinitely.[17]

Exceptions

The FTC proposes various changes to the exceptions under COPPA including:

- **Internal Operations Exception:** Under COPPA, parental consent is not required if personal information is used to support internal operations. However, the Proposed Rule narrows the internal operations exception. The Proposed Rule requires operators relying on the internal operations exception to provide public notice online and guarantee the persistent identifiers are used solely to provide "support for the internal operations of the website or online service."[18] Additionally, an operator must explicitly outline the internal operational procedures for which it acquires the persistent identifier and articulate the methods it will employ to guarantee that this identifier is not employed or revealed to reach a particular individual, including through targeted advertising.[19]
- **Multiple Contact Exception:** If operators expect to contact the children more than one time, they must use the "multiple contact" exception, for which operations must also collect a parent's online contact information and provide parents with direct notice of your information practices and an opportunity to opt out. The Proposed Rule requires that operators would be prohibited from using online contact information

and persistent identifiers collected under COPPA's multiple contact and support for the internal operations exceptions to send push notifications to children to prompt or encourage them to use their service more.[20]

The public will have 60 days to submit a comment on the proposed changes to the COPPA Rule after the notice is published in the Federal Register.

We will continue to monitor the landscape and keep you apprised of developments as they occur.

Footnotes

---

[1] *See* Children's Online Privacy Protection Rule, Statement of Basis and Purpose, 78 FR 3972 (Jan. 17, 2013), available at https://www.federalregister.gov/documents/2013/01/17/2012-31341/childrens-onlineprivacy-protection-rule.

[2] 16 CFR 312.2.

[3] *Id.*

[4] *See* COPPA FAQs, FAQ H.5.

[5] § 312.5(a)(1).

[6] § 312.5(a)(2).

[7] 16 CFR 312.5(b)(1).

[8] § 312.5(b).

[9] § 312.5(b)(2)(vi)(2).

[10] § 312.4(b).

[11] § 312.5(c)(5).

[12] § 312.2.

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] § 312.8(b).

[17] § 312.10.

[18] § 312.4(d)(3).

[19] § 312.5(c)(7).

[20] § 312.5(c)(4).