

FTC Finalizes Amendments to Rule Protecting Children's Data: Regulatory Freeze Likely Signals Further Revisions

Author: Jana Slavina Farmer, AIGP, CIPP/US, FIP

On January 16, 2025, the Federal Trade Commission (FTC) **announced** that it finalized changes to the **COPPA Rule**, which protects information collected online from children under the age of 13. The COPPA Rule imposes obligations on the operators of commercial websites and online services (including mobile apps and online games) that are directed to children under the age of 13 and that collect, use, or disclose children's personal information. The COPPA Rule was last amended in 2013. For the purposes of this discussion, we will refer to the Rule, as amended, as the "new COPPA Rule" (although further changes are anticipated) in contrast to the "current COPPA Rule."

Notably, the new COPPA Rule is pending further review following the January 20, 2025, **Presidential Action** instituting a Regulatory Freeze Pending Review.

The FTC's new chair and then-commissioner, Andrew N. Ferguson, had previously issued a concurring statement on the new COPPA Rule. While he supported the enhanced measures improving children's data privacy, Ferguson criticized the new COPPA Rule as being highly problematic in three major areas, adding unnecessary burdens to businesses. The Regulatory Freeze procedure means that Chair Ferguson or his designee will again review the new COPPA Rule.

Considering Ferguson's prior criticism, businesses can expect that the new COPPA Rule will undergo further revisions before it is finalized. That said, businesses should be aware that measures such as requiring a separate and specific verifiable parental consent (VPC) for disclosure of children's data to third parties, and identification of specific third-party recipients of such data, were noted with approval by Ferguson and are likely to ultimately pass. These measures encourage businesses to carefully select vendors with whom data may be shared, and to examine such vendors' track record on privacy and security. The enhanced requirements to the information security program are likely here to stay. The pending review of the new COPPA Rule as a result of the Regulatory Freeze means businesses have a little more time to prepare to address additional compliance requirements.

Key Changes Introduced in the New COPPA Rule

Expanded Definitions

The definition of "personal information" was expanded to include biometric identifiers that can be used for the automated or semi-automated recognition of an individual, with the definition listing examples of such identifiers. This amendment reflects the evolving concerns over more-recent data collection practices: biometric identifiers such as fingerprints or facial scans may be combined with persistent identifiers (such as IP addresses) that may uniquely and persistently identify a child.

The new COPPA Rule also contains a stand-alone definition of a "mixed audience" website or service, which means platforms that do not target children as their primary audience. The current COPPA Rule uses the term "mixed audience," but does not expressly define it. A mixed-audience website or online service is a sub-category of child-directed websites and online services subject to the COPPA Rule. The new COPPA Rule clarifies that operators of mixed-audience websites and

online services may use the exceptions to the VPC requirement set forth in §312.5(c) of the COPPA Rule, as is true for operators of online services targeting children as their primary audience. The definition of “online contact information” also was amended to include mobile telephone numbers, provided the operator uses them only to send text messages to a parent in connection with obtaining VPC.

New Examples of “Child-Directedness” Factors

The determination of whether a website or a service is “child-directed” is based on factual analysis under both the current and the new COPPA Rule. The current COPPA Rule already requires that businesses pay attention to known indicators that children may be using their platform. See, for example, [Yelp settlement](#) and [NGL Labs settlement](#). The current COPPA Rule features a non-exhaustive list of evidence that the FTC may consider in determining “child-directedness.” See COPPA Rule §312.2 (definition of “Web site or online service directed to children”).

The new COPPA Rule provides additional examples: (1) marketing or promotional materials or plans, (2) representations to consumers or third parties, (3) reviews by users or third parties, and (4) age of users on similar websites or services. Commenters on proposed amendments previously expressed concerns about the latter two factors, noting, for example, that this amendment would incentivize competitors or others to file false reviews, potentially trying to influence how a website or online service is categorized. In response to these comments, the FTC reiterated that child-directedness is determined on a totality of the circumstances, and that evidence such as reviews may receive little weight given that reviews may not always be representative, accurate, or genuine.

Separate Consent for Targeted Advertising

The new COPPA Rule will require a separate and specific VPC before any non-integral disclosure of children’s personal information to third parties, such as for third-party advertising. The amendment is meant to reduce the flow of children’s information to data brokers and discourage targeting children with personalized advertising, because the process of obtaining consent is an expensive and cumbersome process for businesses. This is one of the areas that Ferguson previously flagged as highly problematic.

Basically, the new COPPA Rule seems to suggest that every time a business decides to share children’s data with a third party, it is a material change requiring a separate consent. If so, given the operational costs of obtaining VPC, this requirement will greatly discourage businesses from switching from their existing third-party vendors. Ferguson noted that not every change to the identities of third parties should require a new consent, but only changes that would make a reasonable parent believe that the privacy and security of their child’s data is being placed at materially greater risk. Further clarifications from the FTC in this area are expected.

Additional Options to Collect VPC

The new COPPA Rule added three new methods for obtaining VPC, including via “text plus” (with requirements similar to the current “email plus” method), facial recognition, or by using knowledge-based authentication (using multiple-choice questions that are hard to guess and that children under 13 will have difficulty answering). Additionally, the payment transaction method for obtaining VPC was revised to remove the “monetary” requirement, meaning that consent may be obtained without receiving and then refunding a payment. Notably, the list of methods to obtain VPC is not exhaustive under either the current or the new COPPA Rule.

Collection Solely for Age Verification Purposes

Ferguson also criticized the new COPPA Rule for its failure to add an exception to the general prohibition on the unconsented collection of children’s data for the sole purpose of age verification, along with a requirement that such information be promptly deleted once that purpose is fulfilled. Currently, collection of age verification–related information, such as photographs or government-issued ID images, require VPC and discourage the use of age verification techniques that are more

accurate than a self-declaration. Businesses can expect further changes to the Rule on this issue as well.

Data Retention and Deletion Requirements

The current COPPA Rule provides that an operator may retain children's data only as long as is reasonably necessary to fulfill the purpose for which the information was collected. The new COPPA Rule provides that operators are expressly prohibited from indefinitely retaining children's data. This is one of the areas that Ferguson flagged as seriously problematic, as it is likely to generate outcomes not favorable to users. For example, data such as digital diary entries, childhood photos, or emails may be erased, blindsiding a user who cherished such records and relied on the platform to preserve them. Ferguson further noted that the "indefinitely" requirement is meaningless given that a company may get around it by stating that data will be kept for "two hundred years." Again, we expect to see further revisions on this topic.

WISP and Data Retention Policy Requirements

The new COPPA Rule modifies operators' obligations with respect to direct and online notices, information security, and deletion and retention protocols. Regarding information security, the current COPPA Rule states only that the operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

The new COPPA rule adds more prescriptive requirements to:

- Designate at least one employee to coordinate the information security program
- Conduct risk assessments at least annually
- Design, implement, and maintain safeguards to control the risks identified through risk assessments
- Regularly test and monitor the effectiveness of such safeguards
- Evaluate and modify the operator's information security program (WISP) at least annually to address identified risks.

Operators also must determine that their service providers and third parties are capable of maintaining the confidentiality, security, and integrity of the information and must obtain written assurances that such entities will employ reasonable measures to maintain the confidentiality, security, and integrity. With respect to data retention, the new COPPA Rule provides that at a minimum, the operator must establish, implement, and maintain a written data retention policy that sets forth the purposes for which children's personal information is collected, the business need for retaining such information, and a timeframe for deletion of such information. This policy must be provided in the notice of information practices posted on the website or online service in accordance with § 312.4(d) of the COPPA Rule.

These requirements are broadly aligned with some of the requirements of the FTC Safeguards Rule and the FTC's guidance to businesses on what constitutes a reasonable information security program. Commentary to the new COPPA Rule clarifies that a separate information security program and data retention policy is not needed for children's data, but rather general programs and policies that encompass children's data and otherwise meet the requirements of the COPPA Rule will be sufficient.

Enhanced Transparency for Safe Harbor Programs

COPPA Safe Harbor programs – self-regulatory initiatives approved by the FTC to implement COPPA protections – will now be required to publicly disclose membership lists and provide additional reports to the FTC. These changes aim to increase accountability and transparency within these programs.

Summary

Originally, the new COPPA Rule was to take effect 60 days after its publication in the *Federal Register*, and covered businesses were to have one (1) year from the publication date to achieve full compliance with most amendments unless earlier compliance dates are specified. As discussed, however, the new COPPA Rule was not yet published and is considered withdrawn pursuant to the January 20, 2025, Regulatory Freeze Pending Review, until they can be reviewed by the FTC Chair or his delegates for this task. While further changes are anticipated, businesses that have knowledge of children using their online platforms should review the new COPPA Rule and be aware of its current compliance impacts. Now is the time to review and update information security practices and take a careful look at each vendor's compliance.