Davis Polk

FTC prioritizes COPPA enforcement as new compliance obligations take effect

April 16, 2026 | Client Update | 9-minute read

The FTC forecasts robust enforcement of new COPPA Rule requirements while encouraging the use of innovative age-verification technology.

Introduction

With amendments to the Federal Trade Commission's (FTC) Children's Online Privacy Protection Act (COPPA) Rule taking effect on April 22, 2026, FTC leadership is underscoring its commitment to robust enforcement. At an International Association of Privacy Professionals (IAPP) summit in late March, FTC Commissioner Mark Meador emphasized that "keeping children safe as they navigate a digital world" is a priority and that the Commission is "willing and eager" to enforce compliance with forthcoming obligations. Previously, Associate Director of the FTC's Division of Privacy and Identity Protection (DPIP) Ben Wiseman similarly forecast: "The commission has been loud and clear for a while that protecting kids is going to be a high priority, and we're going to continue to bring cases on that. And so I think you'll see more of that in the coming months and years."

In parallel, the FTC is seeking to enhance COPPA's efficacy by endorsing the use of innovative age-verification technologies. On February 25, 2026, the FTC issued a Policy Statement limiting enforcement of the COPPA Rule when children's data is collected, used or disclosed for age-verification purposes without first obtaining parental consent. Notably, however, companies must be compliant with the COPPA Rule "in every other respect" to benefit from the discretionary enforcement policy.

Background

The FTC published the final COPPA Rule amendments in the Federal Register on April 22, 2025. Although the amendments became effective on June 23, 2025, operators of websites and online services subject to COPPA have until April 22, 2026 to come into compliance. Entities seeking to take advantage of the COPPA Rule's safe harbor programs had earlier compliance dates.

In the interim, the FTC has continued to pursue companies for alleged COPPA violations. In January 2025, for example, game developer Cognosphere agreed to pay $20 million to settle allegations that, among other things, it collected personal data from children without notifying parents or obtaining parental consent, and failed to take corrective action even after it became aware that specific users were children. In September 2025, Apitor Technology settled allegations that it failed to notify parents and obtain consent before allowing a third-party software development kit embedded in its app to collect personal information from children. Also in September 2025, Disney agreed to pay $10 million to settle allegations that it allowed personal data to be collected from children who viewed child-directed videos on YouTube without notifying parents or obtaining their consent.

New COPPA Rule requirements

Starting on April 22, 2026, operators of websites and online services directed to children (i.e., those under 13) or those with actual knowledge that they are collecting "personal information" from children (collectively, "eligible operators") will face new requirements under the amended COPPA Rule. The Rule—which has long mandated special practices for children's personal information, including providing parental notice and obtaining verifiable parental consent before collecting children's data, minimizing data collection from children and protecting such data when collected—had last been amended in 2013. In addition to modernizing the Rule to keep pace with technological change, the FTC's latest amendment expressly seeks to "strengthen protection of personal information collected from children," including "more focus on operators' data security requirements." The key changes are:

- ***Clarified scope***: While the FTC has stated that it does not expect the amended Rule to bring additional operators under its purview, the amended definitions clarify the Rule's scope and breadth, including additional factors that affect whether an operator is subject to the Rule. The amended Rule:
  - Adds a definition for "Mixed audience website or online service" for operators that direct their services to children but not as the primary audience, which are required to determine whether users are children before collecting their personal information (subject to narrow exceptions). The amended Rule also adds examples of factors to determine whether a service is directed to children, such as an operator's marketing plans and representations to consumers or third parties, reviews by users or third parties and the age of users on similar services; and
  - Adds as examples of "personal information" biometric identifiers (such as retina patterns) and government-issued identifiers beyond Social Security numbers.

- ***Expanded notice requirements***: The amended Rule expands requirements both for direct notice to parents (before obtaining their consent, as well in other targeted scenarios) and for the notice to be displayed on the relevant service. For direct parental notice—which already needed to include, among other things, the personal information to be collected—the amended Rule adds several requirements, including most notably how the operator intends to use the child's information, the identities or categories of third parties to which the child's information will be disclosed and the purposes for such disclosure. Eligible operators must also include much of this information on their services, as well as certain other added requirements, such as a written data retention policy (discussed further below).
- ***Expanded consent requirements and options***: Beyond the existing requirement to allow parents to consent to collection of their child's data without consenting to disclosing that data to third parties, the amended Rule (i) adds an exception to the consent requirement for disclosure that is "integral" to the service and (ii) newly requires eligible operators to obtain separate parental consent for third-party disclosure. The FTC has not defined what "integral" means, but has noted that disclosure "necessary to provide the product or service the consumer is asking for" would qualify while "for monetary or other consideration, for advertising purposes, or to train or otherwise develop artificial intelligence technologies" would not be "integral." More broadly, the amended Rule adds more options for obtaining parental consent, including a facial-recognition comparison and "text plus," permitting parental consent by text message when combined with additional steps to confirm it is actually the parent.
- ***Stricter information security and third-party oversight***: Building on the preexisting requirement for "reasonable procedures to protect the confidentiality, security, and integrity" of children's data, the amended Rule defines a "minimum" baseline for these procedures, requiring eligible operators to "establish, implement, and maintain a written information security program" appropriate for the operator and the sensitivity of the data. The written program must encompass certain elements, including annual risk assessments, safeguards to control identified risks, safeguard testing and annual evaluations and adjustments to the program. Notably, the FTC has said that operators can leverage broader information security programs that meet the stated requirements, which align at a high level with the FTC's Safeguard Rule for financial institutions, standard requirements in various FTC consent orders and compliance best practices. For third parties that collect or maintain children's data on the operator's behalf, the amended Rule also requires eligible operators to take reasonable steps to determine that those third parties are capable of protecting the relevant data and obtain written assurances that third parties will take reasonable measures to do so.
- ***More limited data retention***: The amended Rule strengthens the existing requirement to retain children's data only as long as reasonably necessary to fulfill the purposes for which it was collected, stating explicitly that children's data must then be deleted and adding a prohibition on indefinite retention. The amended Rule also bolsters these requirements by mandating a written data retention policy—to be posted on the operator's service, as noted above—that lists the purposes for which children's data is collected, the business need for its retention and a timeframe for its deletion.
- ***Expanded safe harbor reporting***: The amended Rule places greater reporting obligations on safe harbor programs approved to evaluate eligible operators' compliance with the COPPA Rule, requiring such programs to submit to the FTC—among other things—lists of operators who passed the evaluation or, conversely, have left the program.

Discretionary enforcement policy

To facilitate the COPPA Rule's efficacy, the FTC is simultaneously encouraging the use of innovative technologies to verify users' ages via a discretionary enforcement policy that permits the use of children's data for age-verification purposes without parental consent in specific circumstances. The policy follows an FTC-hosted public age-verification workshop held on January 28, 2026, where FTC Chair Andrew Ferguson expressed an eagerness "to explore what steps the FTC can take to ensure that the COPPA rule does not unduly inhibit the implementation and innovation of effective age verification technology." Among other things, the workshop recognized the tension between, on the one hand, restrictions on collecting children's data under the COPPA Rule and other legal regimes and, on the other hand, the development of technology to more accurately determine a user's age.

On February 25, 2026, the Commission issued a Policy Statement exempting operators of mixed audience services and general audience services with actual knowledge of under-13 users (collectively, "Relevant Operators" under the Policy Statement) from obtaining parental consent if they collect, use or disclose children's data solely to employ age-verification technologies and meet certain other requirements. The Policy Statement does not apply to services primarily directed to children, which are required to treat all users as children. Described as a "very narrow carveout" by Chair Ferguson's attorney adviser at the IAPP summit, the Policy Statement is intended "[t]o promote innovation in, and the responsible use of, age-verification mechanisms," so that operators "can utilize age-verification mechanisms without subjecting themselves to the risk of enforcement under the COPPA Rule."

Relevant Operators who wish to benefit from the Policy Statement must meet certain conditions, several of which conceptually align with the COPPA Rule or the amendments shortly coming into effect—these include employing reasonable security safeguards, deleting the information collected for age-verification purposes once no longer needed to fulfill that purpose and providing clear notice to parents and children of the information collected in the Relevant Operator's privacy policy. In addition, Relevant Operators must:

- Refrain from using or disclosing information collected for age verification for any other purpose;
- Take reasonable steps to determine that any method or third party utilized for age verification is likely to provide reasonably accurate results as to the user's age; and
- Obtain additional written assurances from third parties to which the Relevant Operator will disclose data collected for age-verification purposes. In addition to measures consistent with the COPPA Rule amendments—limiting sharing only to third parties capable of protecting the data and where the operator obtains written assurances that the third party will employ reasonable measures to do so—Relevant Operators must also obtain written assurances that such third parties will not use or share the data for any purpose other than age verification and will delete the data afterwards.

Key takeaways

As the deadline approaches to comply with the new COPPA Rule amendments, operators should keep in mind:

- It is not too late for operators to review their practices to ensure they align to the stricter, more granular requirements of the amended COPPA Rule given the FTC's plans for robust enforcement.
- Operators implementing age-verification technologies should consider reviewing data flows and security protocols; reviewing and updating vendor agreements to account for more stringent third-party sharing requirements; and documenting the testing and results of age-verification systems. Operators should also ensure they are fully compliant with the COPPA Rule, including the April 22 requirements, to maintain eligibility for the discretionary enforcement policy.
- Operators should continue to monitor the area for further COPPA Rule amendments and enforcement actions. The FTC intends to initiate a review of the COPPA Rule to address age-verification mechanisms via further amendment, which would require a standard notice and comment process before adoption. At the IAPP summit, an attorney advisor to Chair Ferguson noted that companies should "stay tuned … we might have more on [the COPPA Rule] very soon."

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

James W. Haldin
+1 212 450 4059
james.haldin@davispolk.com

David I. Feinstein
+1 212 450 3293
david.feinstein@davispolk.com

Tyson Dean Kennedy
+1 650 752 2016
tyson.kennedy@davispolk.com

Maude Paquin
+1 212 450 3205
maude.paquin@davispolk.com