Updates
February 07, 2025
FTC Announces New Children’s Privacy Requirements in Updated COPPA Rule

The Federal Trade Commission (FTC or Commission) announced long-awaited amendments to the Children’s Online Privacy Protection Act Rule (COPPA Rule) on January 16, 2025, marking the first changes to the COPPA Rule since 2013. The amendments are the output of a rule review process that began in 2019 and a notice of proposed rulemaking (NPRM) announced in December 2023. The amendments, which expand the rule’s scope and include new notice and consent requirements, data retention restrictions, and data security requirements, constitute significant but not monumental changes. Indeed, several proposals in the NPRM that would have changed the rule more significantly were ultimately rejected. While the final rule was adopted on a 5-0 vote, Commissioner Andrew Ferguson (now the agency’s chairman) expressed concerns with several provisions in a concurring statement, and it is likely that the rule will be withdrawn and potentially modified before companies are required to comply.

Key Updates

- **“Directed to children” factors.** COPPA applies to operators of websites or other online services that are “directed to children” under age 13 or have actual knowledge that they have collected the personal information of a child under 13. The FTC takes a totality-of- the-circumstances approach to determine whether a website or online service is “directed to children.” Amendments reflected in the final rule expand the factors the FTC may consider include marketing or promotional materials or plans, representations to consumers or other third parties, reviews by users or other third parties, and the age of users on similar websites or services. At the same time, the Commission noted that it was not imposing a burden on businesses to "continuously monitor” reviews of their services or demographic information about users on competitors’ services.
- **Definition of “personal information.”** “Personal information” is a pivotal term in the rule. The amended rule retains the current meaning of this term as “individually identifiable information about an individual collected online” but also expands the express list of examples of personal information to include (1) a

"biometric identifier that can be used for the automated or semi-automated recognition of an individual such as fingerprints; handprints; retina patterns; iris patterns; genetic data, including a DNA sequence; voiceprints; gait patterns; facial templates; or faceprints" and (2) a "government-issued identifier."

- **Notice and separate consent for third-party disclosures.** The current COPPA Rule requires operators to obtain verifiable parental consent to disclose personal information to third parties, including for the purpose of engaging in targeted advertising, but permits operators to bundle this consent with the consent they obtain to collect and process children's information for other purposes. By contrast, under the amended rule, if an operator intends to disclose children's personal information to a third party, the operator will have to obtain a separate consent for that disclosure except to the extent that the third-party disclosure is "integral" to the website or online service. Further, the direct notice and online notice must disclose the identities or specific categories of such third parties (either directly in the notice or via hyperlink) and the purposes for such disclosure and make clear that parents may consent to the collection and use of their child's information without agreeing to the third-party disclosure except to the extent that such disclosure is integral to the website or online service. As to what disclosures are "integral," the FTC generally noted the question is fact-specific and "depends on the type of services offered by the website or online service" but opined that disclosures that are necessary to provide the product or service the consumer is asking for are integral and thus do not require separate consent. By contrast, it opined that "[d]isclosures of a child's personal information to third parties for monetary or other consideration, for advertising purposes, or to train or otherwise develop artificial intelligence technologies" are not integral to the website or online service and thus would require separate consent.
- **"Text plus" verification method.** The amended rule introduces a "text plus" method for obtaining verifiable parental consent. This new mechanism mirrors the longstanding "email plus" method but allows the operator to initiate the consent process by texting the parent and taking additional steps to provide assurance that the person providing the consent is the parent, such as by sending a confirmatory text message to the parent following receipt of consent or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. As with email plus, text plus is available only when the operator will not disclose the child's personal information to third parties.
- **Disclosures for use of persistent identifiers for support for internal operations.** Under the current rule, operators do not need to provide direct parental notice, post an online notice, or obtain verifiable parental consent if they collect only persistent identifiers from children and use them solely to support specified "internal operations" of their website or online service. Under the amended rule, this exemption extends only to the obligation to obtain consent and does not obviate the need to provide notice. Operators must include in their online notice "the specific internal operations for which the operator has collected a persistent identifier pursuant to [the support for the internal operations exception to the rule's verifiable parental consent requirement]" and "the means the operator uses to ensure that such identifier is not 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 (except as specifically permitted to provide support for the internal operations of the website or online service)." As to the details the online notice must provide regarding how an operator uses persistent identifiers, the Commission explained that "general, categorical terms" would suffice. Similarly, to describe the means used to ensure that persistent identifiers are not used or disclosed for prohibited purposes, the Commission stated that operators do not have to "prove a negative" and could "provid[e] a general statement about training, data segregation, and data access and storage."
- **Data security.** Under the current COPPA Rule, operators must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of children's personal information. The modified rule fleshes out this requirement by specifying that the information security program must be in writing and meet the requirements that the FTC elsewhere imposes, such as that the operator designate one or more employees to coordinate the program; conduct at least annual risk assessments to identify risks to the security, confidentiality, and integrity of children's personal information; implement appropriate

safeguards to address identified risks; regularly test and monitor the efficacy of those safeguards; and at least annually evaluate the program. In addition, the amended rule adds a requirement for obtaining written assurances that third parties, service providers, and other entities to which an operator releases children's personal information will maintain its confidentiality, security, and integrity. At the same time, the Commission clarified that operators need not have a separate data security program for children's data.

- **Data retention.** The current COPPA Rule requires operators to retain personal information collected from a child for only as long as reasonably necessary to fulfill the purpose for which the information was collected. The amended rule specifies that operators must delete such information when it is no longer reasonably necessary for such purposes and that it may not be retained indefinitely. It also requires operators to publish a data retention policy for children's data in their online privacy policy.
- **Safe harbor self-regulatory programs.** The amended rule imposes new reporting requirements by "safe harbor" organizations, which are FTC-approved self-regulatory entities. These requirements include public posting of all the operators certified by the safe-harbor organization, annual reporting to the FTC on the consumer complaints that the safe harbor has received related to the operators subject to its guidelines, and reporting to the FTC every three years on the safe harbor organization's technological capabilities and mechanisms for assessing operators' fitness for membership in its safe harbor program.

Rejected Proposals

The Commission rejected several proposed modifications or concepts in questions it had advanced in the NPRM, including the following:

- **"Nudging" to prolong engagement.** The FTC did not adopt any restrictions on the use of children's personal information to prompt or extend online engagement as it had proposed in the NPRM, agreeing with some commenters that its proposal was overly broad and could limit beneficial prompts. At the same time, the Commission emphasized that it may pursue enforcement under Section 5 of the FTC Act in appropriate cases to address unfair or deceptive acts or practices encouraging prolonged use of websites and online services that increase risks of harm to children.
- **Edtech.** The FTC declined to codify its longstanding guidance that permits schools to consent to the processing of students' personal information if specific conditions are met, despite a proposal to do so in the NPRM. At the same time, the Commission said it would continue to enforce COPPA consistent with its prior guidance. This modification may have resulted from concerns previously expressed by Chairman Ferguson that the COPPA statute does not authorize schools to stand in the shoes of parents for purposes of COPPA's notice and consent requirements.
- **Contextual advertising.** While the NPRM asked if the FTC should reconsider its treatment of contextual advertising, which is deemed a type of "support for internal operations" under the current rule, the Commission decided to continue this approach.

Next Steps

The amended rule is slated to become effective 60 days after publication in the *Federal Register*, and the compliance date for the rule, except certain safe harbor program requirements, is 365 days after publication. However, the rule is subject to an executive order issued on January 20, 2025, that orders all executive departments and agencies to withdraw any rules that, like the amended rule, have already been adopted and sent to the *Federal Register* but have not been published so that they can be reviewed and approved by an agency head appointed by President Donald Trump.

While Chairman Ferguson, President Trump's appointee heading the FTC, voted in favor of the final COPPA rule, he issued a concurring statement expressing concerns about three issues:

1. A lack of clarity regarding whether a change in the identities of the specific third parties to whom an operator discloses children's data is a material change requiring new parental consent.
2. The prohibition on "indefinite" retention of personal information, which in some cases may yield outcomes adverse to consumers and, because "indefinite" is undefined, may be evaded by businesses who could declare they will retain data for 200 years.
3. The lack of an exception to allow operators to use children's personal information solely for the purpose of age verification.

Once the Republicans hold the majority at the FTC, Chairman Ferguson may withdraw the final COPPA rule in order to address whether these modifications should be made. Whatever ultimate course this rulemaking takes, children's privacy is likely to remain an FTC priority under the current COPPA rule (which carries maximum penalties of $53,088 per violation for 2025) and Section 5.

Authors

Explore more in

Privacy & Security Technology Transactions & Privacy Law Digital Media & Entertainment, Gaming & Sports

Related insights

Update

Securities Enforcement Forum New York 2025: A New Era Looms

Update

Trends in the Growth of Investment in US Data Centers Under the Trump Administration