14 Feb. 2025

ANALYSIS

Advertising & Marketing | North America | Children's Privacy | Law & Regulation | Third Party Management | Data Security

Top 5 impacts of the new COPPA Rule

Stacy Feuer
Contributor
CIPP/E, CIPP/US

Maria Nava
Contributor
CIPP/US

Courtney Cox
Contributor
CIPP/US, CIPT

12 Minute Read

The Children's Online Privacy Protection Rule received a long-awaited update from the U.S. Federal Trade Commission in mid-January, days before the end of the Biden administration. The FTC announced the final rule revising COPPA's implementing regulations on approximately the 12th anniversary of the last update in 2013.

The amended COPPA Rule takes effect 60 days after publication in the Federal Register.

Though the timing of the final rule is uncertain following the Trump administration's stay of new regulations, the FTC adopted the final rule on a bipartisan, unanimous basis, with new Chair Andrew Ferguson supporting the improved "data privacy and security protections for children" and reminding the public that the "amendments to the old COPPA Rule are the culmination of a bipartisan effort initiated when President Trump was last in office."

Although the final rule's publication may be delayed and deadlines may shift, companies should plan compliance strategies now. There are five key areas to focus on.

1. Separate consent for third-party "non-integral" disclosures

COPPA has long required companies to obtain verifiable parental consent from parents before they can collect, use, and disclose children's personal information. The final rule requires companies to "give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of ... personal information to third parties, unless such disclosure is integral to the website or online service." Verifiable parental consent for such disclosure must be obtained separately.

The FTC explained "a separate consent requirement for non-integral disclosures to third parties, such as for third-party advertising, enhances transparency and enables parents to make more deliberate and meaningful choices." But questions remain; what is an integral disclosure? Who is a third party? How does this disclosure interplay with existing COPPA exceptions?

What is an integral disclosure? Per the FTC, information sharing with third parties as necessary to provide the product or service requested by the consumer is integral to the website or online service and falls outside the scope of these amendments. By contrast, providing a child's personal information for monetary or other consideration, for advertising purposes, or to train or otherwise develop artificial intelligence technologies is not considered integral.

Who is a third party? A third party is "'any person' who is neither an operator ... nor 'a person who provides support for the internal operations' of the subject website or online service." The final rule mandates companies obtain consent before disclosing children's personal information to "any entity other than the one providing the subject website or online service (or providing support for the internal operations of the subject website or online service)."

How does the historically available "support for internal operations" COPPA exception relate to website functionality? Support for internal operations is a carve-out of the verifiable parental consent requirement.

In the past, the FTC has defined internal operations as those activities necessary to maintain or analyze the function of the website or online service; perform network communications; authenticate users of, or personalize content on, the website or online service; serve contextual advertising on the website or online service or cap the frequency of advertising; protect the security or integrity of the user, website or online service; ensure legal or regulatory compliance; or fulfill a request of a child as permitted by the one-time or multitime basis exception outlined under COPPA.

Companies have historically relied on this exception to collect and use persistent identifiers like IP addresses or device IDs — but no other personal information — without verifiable parental consent for these activities.

However, the final rule does not address whether activities falling within the internal operations exception would also be viewed as integral to the website or online service for the purpose of determining if the separate verifiable parental consent requirement applies. For example, maintaining the functioning of a website would appear necessary to provide a consumer with a requested product or service. But is ensuring legal compliance or serving contextual advertising necessary to providing the service?

Takeaway

Compliance with this amendment requires a multistep analysis to determine whether companies must obtain verifiable parental consent before sharing a child's information with a third party.

First, companies must determine whether a specific disclosure would fall within the existing COPPA exception for consent for internal operations or another exception.

If a company's planned third-party disclosure of a child's personal information does not fit a previously existing exception, it must determine whether the integral purpose concept applies. As noted, integral disclosures are those necessary to provide the requested product or service, and not disclosures for targeted advertising or AI training or development.

Companies must gauge the necessity of a specific disclosure with the functioning of their service, accounting for the FTC's statement that "the separate consent requirement for non-

integral disclosures to third parties, such as for third-party advertising, enhances transparency and enables parents to make more deliberate and meaningful choices." Note that, even if a company is subject to this consent exception, such disclosures still require parental notice.

If a company's planned disclosure does not fit the support for internal operations exception or meet the standard of an integral disclosure, it must obtain verifiable parental consent.

The FTC declined to specify methods or timing of consent, prioritizing operator flexibility. But consent must be meaningful — that is, "freely given, informed, specific, and unambiguously expressed through an affirmative action distinct from the parent's consent to the operator's collection and use of children's personal information." The FTC cautioned "consent flows that mislead, manipulate, or coerce parents — including choice architectures that deceive parents about the effect of a consent, or trick parents into providing their consent — will not suffice."

2. Notice of third-party disclosures

Relatedly, the amended Section 312.4 requires enhanced parental notice — in both the direct notice to parents and website or online service notice — when an "operator discloses personal information to one or more third parties."

Direct notice. The direct notice to parents for purposes of obtaining consent now requires listing the "identities or specific categories of such third parties," the purposes for disclosure, and that the parent can consent to the collection and use of the child's personal information without consenting to the disclosure of such personal information to third parties," except to the extent it is integral to the website or online service.

Website or online service notice. The website or online service notice now must include both the identities and specific categories of any third parties to which an operator discloses personal information, the purposes for such disclosures, and the operator's data retention policy.

This notice must also list the specific internal operations for which an operator has collected a persistent identifier pursuant to the internal operations exception and the means the operator uses to ensure such an identifier is not used or disclosed improperly.

Takeaway

Companies should ensure notices provide detailed third-party disclosures. For the direct notice, companies can choose to disclose either categories or specific identities of third parties but should consider the final rule's preference for consumer-friendly information. The FTC stated, in some cases "categories may help parents understand the implications of the parent’s decision in a way names may not," while in others "identifying third parties by name may be more informative and more efficient."

Many companies have historically only listed categories, rather than specific identities, in direct notices to parents for child-directed services and through privacy disclosures for services that are not child-directed. This may change as several state laws now require party identification. However, companies should aim for clear, informed notice when structuring their privacy policies and direct notices.

For the website or online service notice, companies must include both categories and specific identities to "improve parents' ability to make informed decisions about the websites or online services their children use and facilitate enhanced accountability for operators."

Looking forward

Notice requirements may be an area of focus and contention in the new FTC. Commissioner Ferguson expressed concern regarding the interplay with existing requirements of parental notice upon a "material change" to a privacy policy. He stated, since materiality is not defined, the requirement to disclose specific third parties may result in constant parental notification whenever a third-party vendor is added or changed.

This friction could lead to loss of consumers or a reluctance to change vendors, impairing competition. Former Commissioner Lina Khan's contrasting statement emphasized the increased parental control over whether a child's data is disclosed, including for targeted advertising.

3. Enhanced data security obligations

The FTC has long been concerned about heightened risks caused by lax data security practices. Accordingly, the final rule significantly changed Section 312.8 to better align with the FTC's Safeguards Rule for financial institutions.

The 2013 COPPA Rule only required companies to "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."

Amended rule. Now, companies must "establish, implement, and maintain a written information security program" with safeguards appropriate to the sensitivity of the personal information collected and "the operator's size, complexity, and nature and scope of activities."

Cementing the FTC's shift toward specific security obligations rather than broad "reasonable" standards, the final rule sets out explicit obligations requiring companies to:

• Designate at least one employee to coordinate the information security program.

• Identify and perform annual assessments to identify risks to the confidentiality, security and integrity of personal information and the sufficiency of any safeguards to control such risks.

• Design, implement and maintain safeguards to control risks identified through required risk assessments.

• Test and monitor the effectiveness of the safeguards in place to control risks identified through the risk assessments.

• Evaluate and modify the program, at least annually, to circumstances the operator knows or has reason to know may materially impact its program or safeguards.

Takeaway

The final rule clarified the information security program need not be in addition to any existing program that applies to both children's and nonchildren's personal information. So, companies with established security programs should ensure they comply with Section 312.8's obligations. Companies undertaking the exercise for the first time should carefully review internal practices and document their programs.

4. Increased retention and deletion obligations

The final rule also updates COPPA's data retention and deletion requirements. The 2013 COPPA Rule required operators to retain personal information "only for as long as is reasonably necessary to fulfill the purpose for which the information was collected." By now prohibiting indefinite retention, the final rule goes beyond data retention concerns voiced in the FTC's Amazon and Microsoft settlements.

The inclusion of the ambiguous term indefinite set off an intra-FTC firestorm. Chair Ferguson criticized the prohibition as well-intended but "poorly conceived." He explained a categorical prohibition on indefinite retention could provide "outcomes hostile to users," risking, for example, upsetting adults if their "digital diary entries, photographs, and emails from their childhood (were) erased from existence due to the operation of the Final Rule."

He argued the original language — still retained in the final rule — prohibiting data retention for no longer than necessary to fulfill the purpose for which it was collected was sufficient to protect children. The Democratic commissioners contested Ferguson's statement, explaining the prohibition would protect data from use in developing and refining large language models and other AI and machine learning tools.

Although the new commission may tweak this provision during the regulatory pause or provide additional guidance after the publication of the final rule, companies should review their retention and deletion practices now. This will not only facilitate compliance but also help reduce exposure to a data breach or theft.

5. Enhanced safe harbor oversight and transparency

FTC-authorized COPPA safe harbor programs like the Entertainment Software Rating Board's Privacy Certified provide a self-regulatory complement to FTC oversight. The final rule significantly expands the obligation of safe harbors to enhance oversight and transparency.

What's new? Section 312.11(b)(2) includes the most momentous change, requiring safe harbor programs to conduct a comprehensive review of members' "information privacy and security policies, practices, and representations." This enhanced duty to assess members' data security beyond the previous rule aligns with the FTC's broader data security amendments for all COPPA-covered entities summarized above.

ESRB Privacy Certified has long supported strong safeguards for children's data and routinely reviews members' security practices, flagging outdated security protocols and vulnerabilities. Nevertheless, ESRB and other safe harbors raised concerns that the new rule would deputize them as full-scale data security systems auditors.

In response, the FTC explained safe harbors should rely on guidance accompanying Section 312.8 to evaluate companies' compliance, recognizing the cost and resources required to assess different operators' programs also may vary.

Together, the expanded data security requirements and safe harbor responsibilities show the FTC is serious about stronger standards for children's data security. As it emphasized in announcing the change to safe harbor programs' responsibilities, "The Rule has always included both privacy- and security-related requirements, and the Commission in this rulemaking is putting more focus on operators' data security requirements."

What's new-ish? Many other changes to the rule simply formalize the information the FTC has long required safe harbor programs to submit as part of its provided template safe harbors must use in preparing their confidential annual reports. The new rule also adds a triennial reporting requirement requiring safe harbors to submit copies of complaints received about violations of the program's requirements to the FTC along with the confidential annual report.

Regarding disciplinary actions, ESRB Privacy Certified sought clarification that the FTC's changes would not require safe harbor programs to report "technical and inadvertent and promptly and easily remediated" issues and instead only require disclosing the disciplinary measures formalized in the COPPA Rule.

Recognizing that requiring safe harbor programs to disclose every remedial action would be "self-defeating and dissuade companies from joining Safe Harbor programs," the FTC stated it would not require reporting situations when "some corrective action is warranted but (the program) does not discipline the operator due to prompt responsiveness or other similar reasons."

A final change requires safe harbor programs to publish a list of all program members and their certified products on the safe harbor's website and other online communications channels. The FTC clarified its "intent for this provision is to require FTC-approved COPPA Safe

Harbor programs to publicly share a list of the particular websites and online services certified by their respective programs."

It also explained the requirement to identify certified products or services applies only to those approved products and not those under review for certification.

What isn't changing with COPPA?

While the final rule kept many initially proposed changes, it notably removed proposed changes for educational technology providers. Citing the Department of Education's expressed intent to amend the Family Educational Rights and Privacy Act, the FTC did not include amendments related to edtech and schools, but clarified it will still regulate edtech "consistent with its existing guidance."

What's next?

After a lengthy process, the final rule's future may hinge on the new administration's priorities — namely, whether Chair Ferguson will revisit amendments he took issue with now that the administration paused the rule's publication.

Notwithstanding further amendments, this is a fast-moving area, and companies should expect further action soon.

Stacy Feuer, CIPP/E, CIPP/US, is senior vice president and Courtney Cox, CIPP/US, CIPT, is senior director of the Entertainment Software Rating Board Privacy Certified.

Maria Nava, CIPP/US, is an associate at Frankfurt Kurnit Klein & Selz.

This article is eligible for Continuing Professional Education credits. Please self-submit according to CPE policy guidelines.

Submit for CPEs

Related stories

FTC finalizes COPPA Rule amendments

A view from DC: Unpacking FTC's COPPA Rule update

The increasing need to address digital governance

Notes from the IAPP Canada: Consultation period on CBPR implementation ends 30 June

CPPA Board tees up new consultation on draft ADMT, cybersecurity audit, risk assessment regulations

About

The IAPP is a policy neutral, not-for-profit association founded in 2000 with a mission to define, promote and improve the professions of privacy, AI governance and digital responsibility globally.




Contact us

Press

Advertise

Become a member

The IAPP is the only place you'll find a comprehensive body of resources, knowledge and experts to help you navigate the complex landscape of today's data-driven world. We offer individual, corporate and group memberships, and all members have access to an extensive array of benefits.

Sign up today

Privacy Notice

IAPP Cookie Notice