CLIENT ALERTS & INSIGHTS

The FTC Finalizes Changes to the COPPA Rule: Updated Guidance for Businesses in the New Era of Children's Privacy

JANUARY 24, 2025

Authors: Alison K. Evans, Sydney E. Allen

The Children's Online Privacy Protection Act ("COPPA") Rule, which became effective in 2000 and was amended only once in 2013, aims to protect children's privacy by establishing requirements for websites and online services that collect, use or disclose personal information from children under 13.

On January 16, 2025, the Federal Trade Commission ("FTC") finalized amendments to the COPPA Rule to address evolving technology and further protect the online privacy of children.

"These amendments are much needed," said FTC Chair Lina M. Kahn. "Much has changed [ ], with a dramatic rise in kids' smartphone usage, screentime, and consumption of social media. Meanwhile, firms' financial incentive to harvest kids' personal data only continues to grow: not only is behavioral advertising now a multi-billion dollar business, but-as FTC's enforcement experience has shown-expanded deployment of AI models can further incentivize businesses to harvest and retain kids' personal data."

The revised rule introduces several key changes to enhance privacy protections that website and online service operators covered by COPPA must keep in mind, including:

- **Parental opt-in consent is required for targeted advertising and other disclosures to third parties:** The updated COPPA Rule states that operators will be required to obtain separate verifiable parental consent before disclosing children's personal information to third-party companies for targeted advertising or other purposes. Importantly, parents' refusal to provide consent cannot result in the operator cutting off access to the website or service.
- **Limits on data retention:** Operators will only be permitted to retain children's personal information for as long as reasonably necessary to fulfill the specific purpose for which it was collected. Such information cannot be retained indefinitely. Operators will also be required to maintain a written data retention policy that details the specific business need for holding on to children's personal data and includes a timeline for deleting such data.

- **Expanding transparency in Safe Harbor programs:** The updated COPPA Rule also includes increased transparency requirements for Safe Harbor programs, which are self-regulatory programs approved by the FTC that allow companies to demonstrate compliance with COPPA by adhering to specific guidelines set by FTC-approved industry groups. The required assessment of a member's compliance with the Safe Harbor program's guidelines will now include a comprehensive review of the member's information security and privacy policies, practices, and representations.

In addition, Safe Harbor programs will be required as part of their mandatory annual reports to the FTC to disclose their membership lists, identify all approved websites or online services, and provide the names of any subject operators that have left the safe harbor program during the applicable year.

- **Identification of third party data recipients:** Operators will now be required to provide parents with direct notice that identifies the specific third parties or categories of third parties to whom the operator discloses personal information and the purposes of such disclosure. Additionally, operators will be required to inform parents that they can consent to the collection and use of their child's personal information without consenting to the disclosure of such information to third parties (except to the extent such disclosure is integral to the website or online service).
- **Clarification of data security requirements:** Operators will be required to establish, implement, and maintain a written information security program that contains safeguards that are appropriate to the sensitivity of personal information collected from children and the operator's size, complexity, and nature and scope of activities. To satisfy this requirement, an operator will be required to (i) designate one or more employees to coordinate the program, (ii) conduct assessments 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, (iii) design, implement, and maintain safeguards to control risks identified through the assessments, (iv) regularly test and monitor the effectiveness of the safeguards in place; and (v) evaluate and modify the program at least annually. An operator does not need to maintain a separate children's personal information security program if it maintains an information security program that applies to both children's personal information and other information and meets the above requirements.

Additionally, before an operator can release children's personal information to other operators, service providers, or third parties, the operator will be required take reasonable steps to determine that such data recipients are capable of maintaining the confidentiality, security, and integrity of the information and obtain written assurances that the recipients will do so.

- **Expanded definition of "personal information":** The revised rule also expanded the definition of "personal information" to include government-issued identifiers (e.g., Social Security, state identification card, birth certificate, or passport number) and biometric identifiers that can be used for the automated or semi-automated recognition of an individual (e.g., fingerprints, handprints, retina patterns, iris patterns, genetic data including DNA sequence, voice prints, gait patterns, facial templates, or faceprints).

One noteworthy omission from the final rule is the lack of and new provisions addressing the collection of children's personal information by education technology ("EdTech") companies. Several proposed rules included modifications addressing EdTech; however, the Commission decided against making any changes to the rule to avoid potential conflicts with the Family Education Rights and Privacy Act ("FERPA"). Despite this omission, the Commission reaffirmed its commitment to enforcing COPPA in the EdTech sector in accordance with its existing guidance.

The Commission unanimously approved the publication of the final rule in the Federal Register with a 5-0 vote. The final rule will go into effect 60 days after its publication. Operators subject to the final rule will have one year from the publication date to come into full compliance, unless otherwise specified.

As technology continues to rapidly evolve, bringing with it new privacy and security challenges, it remains critical for operators to continuously evaluate their data processing practices for compliance with updated regulations.

Alison Evans is a Partner of Benesch's Intellectual Property Practice Group. She can be reached at 216.363.4168 or aevans@beneschlaw.com.

Sydney Allen is a Senior Managing Associate in the Intellectual Property Practice Group. She can be reached at 628.600.2229 or seallen@beneschlaw.com.