KIRKLAND & ELLIS

Kirkland Alert

FTC Publishes COPPA Rule Amendments to Strengthen Protections for Children's Data

24 April 2025

Earlier this week, the Federal Trade Commission ("FTC") published its final amendments to the Children's Online Privacy Protection Act ("COPPA") Rule. The rule is intended to provide parents of children under 13 with heightened control over what data is provided to third parties, strengthen requirements for companies that use, collect and/or disclose children's data, and increase transparency regarding FTC-approved COPPA Safe Harbor programs. The new amendments will become effective on June 21, 2025. Relevant online operators will have until April 22, 2026, to comply with the changes, and Safe Harbor programs will have until October 22, 2025, to comply with relevant provisions.

Background

The FTC adopted the COPPA Rule in 2000, pursuant to rulemaking authority under the Children's Online Privacy Protection Act of 1998. The rule requires websites and apps that are directed to children under 13 and/or have actual knowledge that they collect personal information from children under 13 to provide direct notice to parents of their information practices and obtain verifiable parental consent before collecting, using, or disclosing such information from children, among other things. The rule was last updated in 2013.

In January of this year — prior to the transition to the Trump Administration — the FTC announced that it agreed unanimously to amend the COPPA Rule. However, because the incoming Trump Administration did not immediately publish the rule amendments in the Federal Register, the announcement itself had no legal effect. The FTC subsequently published the amendments in the Federal Register earlier this week, on April 22, 2025; as a result, the below changes will take effect on June 21, 2025.

Key Changes to the Rule

- **Opt-In Parental Consent Required for Third-Party Advertising**. Operators must now obtain separate verifiable parental consent prior to disclosing children's personal information to third parties for the purpose of targeted advertising (in addition to the initial verifiable parental consent obtained for the collection, use and/or disclosure of children's personal information more broadly).
- **Heightened Requirements for Direct Notice to Parents**. The "direct notice" that companies must send to parents before collecting personal information from children must now include how the collected personal information will be used, and if applicable, which third parties will receive such information.
- **New Data Security and Retention Requirements**. Website operators must now "establish, implement, and maintain a written information security program that contains safeguards that are appropriate to the sensitivity of the personal information collected from children . . . and scope of activities" and provide written notice on their sites of their policies regarding their retention of children's data. They must also ensure that any third party receiving such data is able to maintain the confidentiality, security and integrity of the information. Lastly, operators are explicitly prohibited from retaining personal information indefinitely and must instead keep it for as long as reasonably necessary to fulfill a specific purpose for which it was collected.
- **Three New Methods Available for Verifying Parental Identity**. In addition to previously approved methods for verifying parental identity, like telephone or video calling, written consent forms and credit card verification, operators may also use (1) knowledge-based multiple-choice questions that are of sufficient difficulty that a child "could not reasonably ascertain the answers," (2) facial recognition technology that uses an authorized "government-issued photographic identification," or (3) the "text plus" method, whereby the operator sends a text message to the parent followed by an additional step to ensure the recipient is in fact the parent (e.g., a confirmatory text message, letter or telephone call).
- **Increased Transparency for FTC-Approved COPPA Safe Harbor Programs**. FTC-approved COPPA Safe Harbor programs must now provide records of disciplinary actions taken and publicly disclose their membership lists.

The commission also announced updates to the following defined terms:

- **"Personal Information" Includes Biometric Data and Government-Issued Identifiers**. The definition of "Personal Information" under the COPPA Rule will now include "biometric identifier[s] that can be used for the automated or semi-

automated recognition of an individual" (e.g., fingerprints, handprints, retina and iris patterns, genetic data), as well as government-issued identifiers beyond Social Security numbers (e.g., state identification card, birth certificate, passport number).

- **Additional Factors Included in Considering a Website's "Purpose."** When considering whether a website is "directed to children," the commission will now also consider a website's "marketing or promotional materials or plans, representations to consumers or to third parties, reviews by users or third parties, and the age of users on similar websites or services."

Missing from the amendments are a number of proposed provisions that the FTC considered but ultimately rejected, including provisions clarifying how the rule applies to education technologies in school settings and limiting the use of push notifications to keep children engaged in online services.

Authors

Lucie H. Duvall

Partner / Washington, D.C.

Christopher B. Leach

Partner / Washington, D.C.

Richard H. Cunningham, P.C.

Partner / Washington, D.C.

Olivia Adendorff, P.C.

Partner / Dallas / Washington, D.C.

Celanire A. Flagg

Associate / Washington, D.C.

Related Services

Practices

- Cybersecurity & Data Privacy
- Litigation
- Antitrust & Competition

Suggested Reading

- 24 April 2025 - 25 April 2025 Sponsored Event 11th National Conference on CFIUS
- 23 April 2025 Press Release Kirkland Advises FP-Backed VitalSource on Acquisition of RedShelf
- 23 April 2025 Award Partner Sunil Shenoi Named to Cybersecurity Docket's Incident Response 50 for Second Straight Year