FTC Final Rule – Amendments to COPPA

On January 11, 2025, the U.S. Federal Trade Commission ("FTC") updated the Children's Online Privacy Protection Rule (COPPA) to expand protections for children's data (the "Final Rules"). This marks the first changes to COPPA since 2013, reflecting the evolving digital landscape and the increasing risks to children's privacy in an era of rising smartphone usage, social media, and data monetization.

The Final Rules introduces several key changes aimed at enhancing transparency, strengthening parental control, and ensuring robust data security for children under the age of 13. The Final Rule will come into effect 60 days after publication in the Federal Register. However, on January 20, 2025, President Trump issued an executive order requiring all executive departments (which includes FTC) to withdraw any rules that have been sent to the Office of Federal Register but not published in the Federal Register. As a result, the effective date of the Final Rules is still uncertain.

Below, we outline the most notable updates and their implications for website and online service operators subject to COPPA.

1. Website or Online Services Directed to Children

The COPPA statute and rule regulate how operators of online services, such as e-commerce websites, online games, and social media sites, collect, use, and share personal information of users who are children under the age of 13. Operators of "website or online services that are directed to children" as their primary audience must get verifiable parental consent before they may collect any personal information from users.

The Final Rules clarify the application of COPPA by updating the key definition of "website or online services directed to children", which includes:

(i) adding a non-exhaustive list of information the FTC may consider when determining whether a website or online service is "directed to children", and the Final Rules now list the following elements
- s*ubject matter,*
- *visual content,*
- *use of animated characters or child-oriented activities and incentives,*
- *music or other audio content,*
- *age of models,*
- *presence of child celebrities or celebrities who appeal to children, language or other characteristics of the website or online service,*
- *whether advertising promoting or appearing on the website or online service is directed to children,*
- *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*.

(ii) excluding a mixed audience website or online service with respect to any visitor not identified as under 13. The Final Rules defines a "mixed audience website or online service" as a website or online service that is directed to children under the criteria listed above, but that (a) does not target children as its primary audience, and (b) does not collect personal information from any visitor, other than to determine whether the user is a child.

The site may only collect age information in a neutral way, without defaulting to a set age or encouraging users to falsify their ages. If a mixed audience platform determines a user is over the age of 13, the platform may collect personal information without requiring verified parental consent. For users under 13, a mixed audience platform may require verified parental consent or may provide an experience that does not collect personal information.

2. Direct Parental Notice Requirements.

Operators of websites and online services must now identify the following information in the direct notice to parents:

- how the operator intends to use information collected from children;
- the "identities and specific categories" of the third parties may receive personal information; and
- the purposes for such disclosures.

These notices must be written in plain language to ensure parents can easily understand how their children's data is being used and shared.

3. Disclosure to Third Parties.

Prior to disclosing children's personal information to third parties (including targeted advertising), operators must directly notify parents.

Unless disclosures to third parties are "integral to the nature" of the website or online services, operators must obtain separate verifiable parental consent. The rule did not explain the term "integral", but the FTC explained a disclosure could be integral "*if the website or online service is an online messaging forum through which children necessarily have to disclose their personal information ... to other users on that forum*". However, a video game with in-app advertisement cannot share children's data with advertisers for personalized ads unless the operator has obtained parental verifiable consent.

It is unclear if this restriction would require additional separate consent every time a new third party non-integral to services is added or changed.

4. Parental Verifiable Consent.

The FTC adopted three additional methods of verifying parental consent:

- knowledge-based authentication using dynamic multiple-choice questions that children under the age of 12 or younger cannot reasonably answer;
- facial recognition using the parent's government-issued ID by matching a selfie photo with that a verified photo ID, provided that the ID and images are deleted after the match is confirmed; and
- a text message method allows operators to collect, but not disclose to third parties, personal information from a child by sending a text message to the parent and taking additional steps to verify the parent's relationship with the child. The additional steps include: (1) sending a confirmatory text to the parent following consent; or (2) obtaining the parent's postal address or phone number and confirming consent through a letter or phone call.

5. Data Retention Policy

Children's personal information may not be retained indefinitely and must be deleted when no longer reasonably necessary for the purposes for which it was collected. In addition, operators must establish and maintain a written data retention policy specifying the purposes for which children's personal information is collected, the business need for retaining such information, and a time frame for deleting it, which may not be longer than the time needed to fulfill the purpose for which it was collected.

6. Minimum Security Requirements.

The FTC set forth minimum security expectations for children's data, requiring that operators create or implement a written information security program appropriate to the operator's size, complexity, and nature and scope of activities and the sensitivity of the personal information the operator collects. To comply, information security programs must include safeguards such as designated qualified employees, routine risk assessments, ongoing monitoring and annual updates.

7. Implications for Businesses

Companies operating websites and online services that collect children's data should take the following steps to ensure compliance:

- Review and update online privacy notices to include detailed disclosures about third-party data sharing, data retention policies, and security measures.
- Review and update parent direct notice to meet the new requirements.
- Implement new parental consent methods, such as knowledge-based authentication or facial recognition, to streamline the consent process.
- Ensure their security programs cover personal information of children and compliance with the FTC's minimum-security requirements.

By Chao Yu

February 8, 2025