ALSTON & BIRD

Consumer Protection/FTC / Privacy, Cyber & Data Strategy ADVISORY

JANUARY 22, 2024

FTC Proposes Significant Amendments to the COPPA Rule

by Kathleen Benway and Hyun Jai Oh

On December 20, 2023, the Federal Trade Commission (FTC) published a notice of proposed rulemaking (NPRM) to seek comment on proposed amendments to the Children's Online Privacy Protection Rule (COPPA Rule), which regulates operators of websites and online services that collect personal information from children under the age of 13. The proposed amendments reflect the FTC's consideration of stakeholder input during the latest review of the COPPA Rule that began in 2019, as well as the FTC's experience in enforcing the Rule. Interested parties will have until March 11, 2024 to submit comments on the proposed amendments. The FTC also held a staff presentation on the proposed changes to the COPPA Rule in its January 18 open meeting, which provided a high-level summary of the NPRM.

The FTC's press release notes that the proposed amendments aim to "place new restrictions on the use and disclosure of children's personal information" and "further limit the ability of companies to condition access to services on monetizing children's data." The proposed revisions, if finalized, would have substantial impact on how businesses may collect, use, and disclose personal information collected from children. Several notable proposals in the NPRM could create significant operational changes for operators within the COPPA Rule's scope.

Separate Verifiable Parental Consent for Disclosures of Personal Information

The NPRM proposes requiring operators to collect separate verifiable parental consent (VPC) before disclosing personal information collected from children, including disclosing persistent identifiers for behavioral advertising. The COPPA Rule currently requires operators to obtain VPC before "any collection, use, or disclosure of personal information from children." The FTC seeks to bolster this requirement by obligating operators to obtain *separate* VPC for disclosures of personal information that is distinct from VPC for collection and use of personal information unless the disclosures "are integral to the nature of the website or online service."

The NPRM does not define what disclosures are "integral," but it explains that a disclosure could be integral, for instance, "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," in which case the operator may rely on VPC for collection and use to make such integral disclosure. The NPRM specifies that this new VPC requirement covers disclosures of persistent identifiers for targeted advertising purposes.

The proposed amendments would also prohibit operators from conditioning access to the website or online service on VPC for personal information disclosure. In other words, if a parent provides VPC for an operator's collection and use of their child's personal information *but does not provide* a separate VPC for disclosure, the operator would be required to provide the website or online service to the child *without* disclosing the child's personal information. Ultimately, operators will need to (1) assess whether their disclosures of personal information collected from children would be considered integral to their websites and online services; and (2) implement a separate VPC procedure for disclosures of personal information collected from children, as necessary.

Narrowing the Scope of the "Support for the Internal Operations" Exception

Under the current COPPA Rule, operators do not need to obtain VPC, provide direct parental notice, or post an online notice if they collect persistent identifiers – and no other personal information – from children and use the persistent identifiers for the sole purpose of providing support for the internal operations of their websites or online services. The NPRM proposes to amend this "support for the internal operations" exception by requiring operators that rely on this exception to provide an online notice. The online notice must specify the internal operations that operators collect persistent identifiers for and how operators will ensure such identifiers are not used or disclosed for any other purposes.

Written Children's Personal Information Security Program

The NPRM proposes to expand the COPPA Rule's general requirement for operators to "maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children." Under the proposed amendments, operators would need to establish, implement, and maintain a written children's personal information security program. To satisfy this requirement, operators must take the following measures, which the FTC explains are modeled after the FTC's Safeguards Rule under the Gramm–Leach–Bliley Act:

- Designate one or more employees that coordinate the program.
- Regularly (and at least annually) conduct risk assessments to (1) "identify internal and external risks to the confidentiality, security, and integrity of personal information collected from children" and; (2) assess the "sufficiency of any safeguards in place to control such risks."
- "Design, implement, and maintain safeguards to control risks identified" through risk assessments.
- "Regularly test and monitor the effectiveness of the safeguards in place."
- Regularly (and at least annually) evaluate and modify the program to reflect "identified risks, results of required testing and monitoring, new or more efficient" methods to control identified risks, and "any other circumstances" that operators know or have reason to know may have a material impact on the program or any safeguards in place.

- Additionally, the proposed amendments would expressly require each operator to conduct reasonable due diligence on other operators, service providers, or third parties that collect personal information from children on behalf of the operator or receive such information from the operator. Operators would also need to have *written* assurances from such entities that they will employ reasonable measures to maintain the confidentiality, security, and integrity of children's personal information.

Written Children's Data Retention Policy

The FTC proposes expanding the COPPA Rule's data retention obligation by requiring operators to establish, implement, and maintain a written children's data retention policy and publish that policy on their online notice. The policy must specify:

- The purposes for which operators collect personal information from children.
- The business needs for retaining personal information collected from children.
- The timeframe for deleting personal information collected from children.

The proposed amendments would also expressly prohibit operators from retaining children's personal information indefinitely or for any purpose other than the specific purposes operators collected the information for.

Education Technology Providers

The NPRM seeks to bring education technology providers squarely into the scope of the COPPA Rule by codifying the FTC's May 19, 2022 Policy Statement on Education Technology and the Children's Online Privacy Protection Act. The proposed amendments would allow schools and school districts to provide authorization for operators of education technology services to collect, use, and disclose students' personal information without obtaining individual VPC, as long as the operators collect, use, and disclose such information for a "school-authorized education purpose" only. "School-authorized education purpose" means providing specific educational services that schools authorize.

Under the proposed amendments, operators would bear the primary burden of providing adequate protections for personal information collected from children for the school-authorized education purpose by complying with the following requirements:

- **Direct school notice**: Operators must provide a direct notice to the school providing authorization, describing the operators' planned collection, use, and disclosure of personal information collected from children for the school-authorized education purpose.
- **Online notice**: Operators must make additional disclosures in their online notice, specifying that: (1) they received authorization from a school to collect personal information from children; (2) they will use and disclose personal information collected from children for a school-authorized education purpose only; (3) the school may review the personal information that operators collect from children; and (4) the school may request deletion of personal information that operators have collected from children, as well as the procedures for making such request.

- **Written agreement**: Operators must enter into a written agreement with the school providing authorization that: (1) lists the name and title of the school personnel providing authorization, as well as the personnel's attestation that they have the authority to provide the authorization; (2) limits operators' use and disclosure of personal information to a school-authorized education purpose only; (3) provides that operators are under "the school's direct control with regard to the use, disclosure, and maintenance of the personal information"; and (4) sets forth operators' data retention policy.

Other Notable Changes

Expansion of "personal information"

The FTC proposes to expand the definition of "personal information" by expressly incorporating a "biometric identifier that can be used for the automated or semi-automated recognition of an individual" into the nonexhaustive list of personal information. The biometric identifier would include fingerprints or handprints, retina and iris patterns, genetic data, or "data derived from voice data, gait data, or facial data."

Additional contents for direct and online notice

The proposed amendments would require operators to specify, in both direct and online notices, the identities or specific categories of third parties to whom operators disclose personal information collected from children, as well as the purposes for the disclosure. The direct parental notice would also need to state that parents may consent to the collection and use of personal information without consenting to the disclosure, except to the extent the disclosure is integral to the nature of the website or online service.

Safe harbor

The FTC seeks to implement additional oversight for Children's Online Privacy Protection Act (COPPA) safe harbor programs through the proposed amendments. First, the safe harbor programs would need to provide additional information in their annual reports submitted to the FTC, including a narrative description of the program's business model and copies of consumer complaints related to operators' violation of the program guidelines. Second, the proposed amendments would require the safe harbor programs to publicly post and regularly (at least once every six months) update a list of participating operators. Third, the safe harbor programs would be required to submit to the FTC a report detailing their technological capabilities and mechanisms for assessing operators' fitness for membership, once every three years.

Takeaways

Children's privacy remains a focus for the FTC

The FTC continues to emphasize its regulatory focus on children's privacy, from a record-breaking half-a-billion-dollar settlement for an alleged COPPA violation to initiating the rulemaking process for the COPPA Rule amendments. The FTC appears particularly concerned about businesses' disclosures of personal information from children, including monetization of children's personal information, which the FTC calls "pervasive" in the NPRM. Businesses that collect children's personal information online should confirm they collect, use, and

disclose children's personal information in a COPPA-compliant manner and conduct adequate due diligence for service providers or third parties that have access to such information.

The FTC expects operators to maintain written policies and procedures to protect children's personal information

The NPRM places a heightened focus on maintaining written policies and procedures to ensure adequate protections for children's personal information are in place, such as written security programs, written retention policies, and written assurances from service providers or third parties that have access to personal information operators collect from children. Businesses should closely monitor the development of the proposed amendments to the Rule and ensure they have adequate written policies and procedures in place to demonstrate compliance.

The FTC plans to enhance oversight of the safe harbor programs

In the NPRM, the FTC reaffirms its position that "FTC-approved COPPA Safe Harbor programs serve an important function in helping companies comply with COPPA." But businesses should note the FTC's position that enhanced oversight and transparency are necessary to ensure the effectiveness of the safe harbor programs.

You can subscribe to future Practice Group Name advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions, or would like additional information, please contact one of the attorneys with our Consumer Protection/FTC team or one of the attorneys with our Privacy, Cyber & Data Strategy team.

.