wiley

ALERT

FTC Proposes Changes to COPPA Rule and Seeks Comment

December 22, 2023

On December 20, the Federal Trade Commission (FTC) announced a Notice of Proposed Rulemaking (NPRM) proposing revisions to its Children's Online Privacy Protection Rule (COPPA Rule) and requesting comment on a number of open-ended questions regarding its proposals. The FTC's proposed changes to the COPPA Rule range from expanding the definition of "personal information" to include biometric information to requiring separate parental consent for sharing children's data in addition to the consent required for collection. The NPRM will be open for public comment for 60 days after publication in the Federal Register.

Below we highlight some of the FTC's key proposed modifications to the COPPA Rule.

Proposed Changes to Notice Provisions.

For website notices, the NPRM proposes requiring operators to disclose their data retention policies, the type of third parties "to which the operator discloses personal information and the purposes for such disclosures," and where applicable, "the specific internal operations for which the operator has collected a persistent identifier." Additionally, if the operator collects audio files that contain a child's voice, the NPRM proposes that website notice must describe "how the operator uses such audio files and that the operator deletes such audio files immediately after responding to the request for which they were collected. . . ." The NPRM further proposes that, when applicable, an operator will identify that it "has obtained authorization from a school to collect a child's personal information," and will follow the school's policies for protecting that information.

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Stephen J. Conley
Associate
202.719.4572
sconley@wiley.law

Lauren N. Lerman
Associate
202.719.4664
llerman@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

New Methods and Requirements for Obtaining Parental Consent Proposed.

The NPRM proposes three additional methods for operators to obtain parental consent, including two that it has previously allowed. First, the NPRM proposes to amend the current definition of "online contact information" to include "an identifier such as a mobile telephone number provided the operator uses it only to send a text message" to the non-exhaustive list of identifiers constituting "online contact information." As the NPRM explains, this will have the effect of permitting companies to obtain parental consent via a text message to a mobile device, which will be a new method of obtaining parental consent.

Second, the NPRM would permit operators to verify a parent's identity by using a knowledge-based authentication that: (1) "uses dynamic, multiple-choice questions, where there are a reasonable number of questions with an adequate number of possible answers such that the probability of correctly guessing the answers is low;" and (2) uses questions of a "sufficient difficulty that a child age 12 or younger in the parent's household could not reasonably ascertain the answers. . . ."

Third, the NPRM proposes to allow parents to submit "a government-issued photographic identification that is verified to be authentic and is compared against an image of where the parent's face taken with a phone camera or webcam using facial recognition technology and confirmed by personnel trained to confirm that the photos match; provided that the parent's identification and images are deleted by the operator from its records after the match is confirmed. . . ."

Additionally, the NPRM proposes measures that would effectively require operators to obtain separate consent to sharing children's data, including for targeted advertising purposes. In particular, it would require operators to give parents the option to consent to the collection and use of the child's personal information without consenting to the disclose of such information, "unless such disclosure is integral to the nature of the website or online service." The NPRM proposes to require that such an operator obtain "separate verifiable parental consent to such disclosure, and the operator may not condition access to the website or online service on such consent."

Proposed Codification of Strict Data Retention and Deletion Requirements.

The NPRM proposes to clarify that operators may only retain personal information as long as it is "reasonably necessary for the specific purpose for which it was collected, and not for any secondary purpose." Moreover, the NPRM proposes to require operators to "delete the information when such information is no longer reasonably necessary for the purpose for which it was collected," and personal information collected from a child "may not be retained indefinitely." The NPRM also proposes requiring operators to establish and maintain a written data retention policy that specifies "its business need for retaining children's personal information and its timeframe for deleting it, precluding indefinite retention."

Proposed Provisions Related to Schools.

The NPRM proposes codifying the FTC's guidance that schools, state educational agencies, and local educational agencies may authorize the collection of personal information from students younger than 13 in limited circumstances, where the data is used for a school-authorized education purpose and no other commercial purpose. The NPRM proposes to define "School" as "a state educational agency or local educational agency . . . as well as an institutional day or residential school, including a public school, charter school, or private school, that provides elementary or secondary education, as determined under State law." The NPRM would also add the term "School-Authorized Education Purpose," which it proposes to define as "any school-authorized use related to a child's education." "Uses" under the definition are limited to "operating the specific educational service that the school has authorized, including maintaining, developing, supporting, improving, or diagnosing the service, provided such uses are directly related to the service the school authorized."

The NPRM also proposes to clarify that the definition does not include "commercial purposes unrelated to a child's education, such as advertising."

Proposed Changes to the Definition and Management of Personal Information.

First, the NPRM proposes to amend the definition of "personal information" to include "[a] biometric identifier that can be used for the automated or semi-automated recognition of an individual, including fingerprints or handprints; retina and iris patterns; genetic data, including a DNA sequence; or data derived from voice data, gait data, or facial data." Separately, the NPRM concludes that the definition should *not* be amended to include "inferred" data about a child.

The NPRM requests additional comment on whether the FTC should retain its position that an operator will not be deemed to have "collected" personal information if it employs automated means to delete all, or virtually all, personal information from one-to-one communications. The NPRM also asks whether avatars generated from a child's image should constitute personal information, and whether the definition of personal information should be expanded to include other government-issued identifiers.

Second, the NPRM would require operators to establish and maintain a written comprehensive security program that includes specific safeguards for children's personal information. The security program proposed in the NPRM must include certain elements, such as: (1) designating an employee to coordinate the information security program; (2) identifying and, at least annually, performing additional assessments to identify risks to the confidentiality, security, and integrity of personal information collected from children; (3) designing, implementing, and maintaining safeguards to control any identified risks, as well as testing and monitoring the effectiveness of such safeguards; and (4) at least annually, evaluating and modifying the information security program.

Third, the NPRM would prohibit operators from conditioning a child's participation in a game, the offering of a prize, or another activity "on the child's disclosing more personal information than is reasonably necessary to participate in such activity."

Safe Harbor Programs Subject to Additional Requirements.

The NPRM would require COPPA Safe Harbor programs to demonstrate that they meet certain performance standards, including:

- Requirements to ensure operators subject to the self-regulatory program guidelines provide substantially the same or greater protections for children as those contained in COPPA;
- An effective, mandatory mechanism for the independent assessment of subject operators' compliance with the FTC-approved COPPA Safe Harbor program's guidelines; and
- Disciplinary actions for subject operators' non-compliance with self-regulatory program guidelines.

Additionally, the NPRM proposes to require FTC-approved COPPA Safe Harbor programs to "identify each subject operator and all approved websites or online services in the program, as well as all subject operators that have left the program."

Once the NPRM is published in the Federal Register, interested parties will have 60 days to file comments. Considering the substantive changes being proposed, companies that may collect children's information should consider weighing on the NPRM's proposals.

***

Wiley's Privacy, Cyber & Data Governance team has helped companies of all sizes comply with their state and federal privacy and cyber obligations. Please reach out to the authors with any additional questions.