March 18, 2026

Andrew Ferguson, Chair
Federal Trade Commission
600 Pennsylvania Ave NW
Washington, DC 20580

Re: Call for the FTC to Revise Its COPPA Age Verification Enforcement Policy Statement and Initiate COPPA Rulemaking on Age Assurance Standards

Dear Chair Ferguson and Commissioner Meador:

We, the undersigned organizations dedicated to privacy, children's rights, and consumer protection, write to urge the Federal Trade Commission (FTC) to take immediate action to revise its Enforcement Policy Statement Promoting the Adoption of Age-Verification Technology ("Enforcement Statement")[1] and to develop stronger, privacy-protective standards that can serve as national guidance for age assurance as it relates to the Children's Online Privacy Protection Act (COPPA).

We welcome the FTC's efforts to advance children's safety online. We understand the purpose of the Enforcement Statement to provide guidance and regulatory clarity for entities collecting personal data for age verification to determine whether a user is a child for COPPA compliance. Because the Enforcement Statement signals the FTC's intention not to "bring an enforcement action under the COPPA Rule against a Relevant Operator[2] that collects, uses or discloses personal information for the purpose of determining a user's age," it is important this regulatory incentive include strong privacy and security protections for data used in an age verification process. The standards the FTC sets now will shape how age verification is implemented nationwide for years to come, whether to comply with COPPA or other frameworks. It is therefore essential that the Commission get this right.

The current Enforcement Statement falls short and should be revised. It effectively sets a weak federal floor for age verification data practices. It falls below the FTC's own established standards for children's data, biometric data, and sensitive data more broadly. If this framework becomes the de facto national baseline, it risks undercutting the more protective approaches emerging at the state level.

Beyond revising the Enforcement Statement, we urge the Commission to initiate a COPPA rulemaking on age assurance. Congress and state legislatures are actively advancing age

[1]FTC, Enforcement Policy Statement Promoting the Adoption of Age-Verification Technology (Feb. 2026).

[2]The Enforcement Statement defines "Relevant Operators" as "operators of websites or online services directed to children that do not target children as their primary audience (known as "mixed audience" websites or online services), as well as operators of general audience sites or Services." *Id*.

verification and age assurance requirements across multiple contexts, making coherent federal guidance both timely and urgent.[3] The Enforcement Statement itself illustrates the need: it is titled as guidance on "age verification," but defines the term to include age estimation and age inference — methods that are fundamentally different in the data they collect, the certainty they produce, and the privacy risks they create. By collapsing this distinction, the statement applies a single weak framework to technologies with very different risk profiles.

The FTC should revise the Enforcement Statement immediately, clarify that its prior policy guidance and rules are not undercut by this statement, and pursue COPPA rulemaking to provide guidance on recommended approaches to age assurance that are grounded in a risk-based framework, protective of privacy, and consistent with the First Amendment.

1. The Enforcement Statement Inverts COPPA's Core Protection

COPPA requires parental consent before collecting children's data.[4] The Enforcement Statement creates an exception allowing Relevant Operators to collect personal information from every user, including children, without parental consent in order to determine who is a child. The FTC's own 2025 COPPA Rule amendments strengthened both consent and notice requirements, including by mandating separate parental consent specifically for third-party data disclosures and requiring expanded disclosures about how children's personal information will be used.[5] The Enforcement Statement exempts age verification data from these requirements entirely, creating a collect-first, protect-later model that contradicts both the statute's foundational logic and the FTC's own recent rulemaking. In choosing to create these broad exemptions, the FTC's Enforcement Statement should be at least as protective as the FTC's own guidance and similar enforcement practices.

2. The Enforcement Statement Applies Weaker Security Standards Than the FTC's Own Rules and Guidance

The Enforcement Statement requires "reasonable security safeguards" and leaves the term undefined. The FTC has consistently specified what reasonable means when applied to sensitive data. Its 2023 Biometric Policy Statement, which remains in effect, identifies the failure to assess foreseeable harms before collection, failure to address known risks, and failure to train employees as potentially unfair practices.[6] The Rite Aid consent decree requires a comprehensive information security program with safeguards calibrated to the volume and

[3] See, e.g., New York Stop Addictive Feeds Exploitation (SAFE) for Kids Act, N.Y. Gen. Bus. Law Art. 45 (2024); Utah Minor Protection in Social Media Act, Utah Code § 13-71 (2024).

[4] Children's Online Privacy Protection Act, 15 U.S.C. § 6501 *et seq.* (1998).

[5] 90 FR 16918 (Apr. 22, 2025) (requiring separate verifiable parental consent for third-party disclosures and expanded direct notice content requirements).

[6] FTC, Policy Statement on Biometric Information and Section 5 of the FTC Act (May 18, 2023).

sensitivity of the data.[7] The 2025 COPPA Rule requires a written security program with designated coordinators, annual risk assessments, and tested safeguards.[8] The Safeguards Rule specifies that financial institutions must utilize encryption and multi-factor authentication to protect customer data.[9] In every other context involving sensitive data, the FTC has given the reasonableness standard specific, enforceable content. In the Enforcement Statement, the FTC should also specify the reasonableness standard for security safeguards for data collected from children during age verification.

3. Third-Party Oversight Falls Below the FTC's Own Established Standards

The Enforcement Statement requires only "written assurances" from third-party age verification vendors that they will employ "reasonable measures" to protect information gathered for age verification. The 2025 COPPA Rule requires operators to conduct reasonable due diligence on third parties, obtain written assurances, and maintain a written information security program covering shared data.[10] The FTC's Biometric Policy Statement advises businesses to go beyond contracts and "supervise, monitor or audit" third parties' compliance.[11] The Enforcement Statement drops all of these layered requirements to a paper compliance exercise with no audit mechanism, no independent verification, and no public disclosure for data that may include children's facial scans, voice recordings, and behavioral profiles processed through third-party vendor APIs. The FTC should amend the Enforcement Statement to include third-party oversight requirements beyond "written assurances" that are in line with similar requirements in the 2025 COPPA Rule and the FTC's Biometric Policy Statement.

4. The Expansive Definition of "Age Verification" Undermines Meaningful Limits on Data Collection

The Enforcement Statement prohibits using age verification data for other purposes, but defines "age verification" to encompass age estimation, age verification, and age inference based on "various signals."[12] This category is essentially unbounded. Behavioral data, browsing patterns, device characteristics, and content engagement could all be characterized as inputs to age

---

[7] In re Rite Aid Corp., FTC File No. 2023190 (Dec. 19, 2023) (consent decree requiring comprehensive information security program with safeguards based on the "volume and sensitivity" of the information at risk and written retention schedule with deletion timeframes no greater than five years).

[8] 90 FR 16918, at 16972–73 (requiring written information security program with designated coordinators, annual risk assessments, tested safeguards, and annual program evaluations).

[9] FTC Safeguards Rule, 16 C.F.R. Part 314 (as amended 2021) (requiring encryption, multi-factor authentication, and a designated Qualified Individual).

[10] 90 FR 16918, at 16973 (requiring operators to conduct reasonable due diligence on third parties and obtain written assurances).

[11] FTC Biometric Policy Statement, *supra* note 6, at 11 (advising businesses to "supervise, monitor or audit" third parties' compliance).

[12] Enforcement Statement, at n.7 ("For the purposes of this enforcement policy statement, 'age verification' refers to a variety of tools used to obtain information about a user's age, including: (1) age estimation tools that estimate a user's age or age range; (2) age-verification tools that verify a user's age; and (3) age inference tools that infer a user's likely age or age range based on various signals.").

inference. The constraint operates on purpose labeling, not on the scope or volume of what is collected. A Relevant Operator deploying a behavioral profiling system that ingests extensive user data could characterize the entire collection as serving "Age Verification Purposes" so long as the stated goal is inferring age. Notably, the Enforcement Statement contains no data minimization requirement. It does not require Relevant Operators to limit collection to what is strictly necessary to determine a user's age, leaving the door open to expansive data gathering under the age verification label. The FTC should include a robust data minimization requirement for any data used in the age verification process and further define "age verification" to limit the scope of data collected for that purpose.

5. Deletion and Retention Requirements Are Weaker Than the FTC's Own Rules

The Enforcement Statement requires Relevant Operators to delete age verification data "promptly" with no maximum retention period and no specification of what must be deleted. The FTC's Biometric Policy Statement warns that retaining biometric information without a legitimate business need or indefinitely "creates an increased risk of harm to consumers."[13] The Rite Aid consent decree requires a written retention schedule with deletion timeframes no greater than five years.[14] The 2025 COPPA Rule requires operators to publish a written data retention policy and prohibits indefinite retention.[15] The Enforcement Statement requires no published policy, no defined timeline, and no specification of whether "deletion" covers the raw image, derived faceprint, metadata, or model training inputs. There is no mechanism for verifying deletion occurred. The Enforcement Statement should be amended to include stricter guidance about data deletion in line with similar FTC policies.

6. The Accuracy Standard Tolerates Demographic Bias

The Enforcement Statement requires only "reasonable steps" to determine a tool is "likely" to provide "reasonably accurate" results, with no quantitative floor and no obligation to assess differential performance across demographic groups. The FTC's own Biometric Policy Statement warns that biometric technologies can perform differently across demographic groups, leading to higher false positives for women, elderly people, and children, and that such errors are particularly harmful when used to determine access to "important benefits and opportunities."[16] Access to COPPA protections is precisely such a benefit. The Rite Aid consent decree was built on the FTC's finding that the company failed to test accuracy and to assess or address risks of

[13]FTC Biometric Policy Statement, *supra* note 6, at 9 n.45 ("Collecting or retaining biometric information without any legitimate business need or keeping that information indefinitely creates an increased risk of harm to consumers.").

[14]In re Rite Aid Corp., *supra* note 7 (requiring written retention schedule with deletion timeframes no greater than five years for biometric information).

[15]90 FR 16918, at 16974 (requiring published written data retention policy and prohibiting indefinite retention).

[16]FTC Biometric Policy Statement, *supra* note 6, at 4–5 (discussing NIST research finding higher false positive rates for women, elderly people, children, and certain racial groups).

disproportionate harm based on race, gender, or other demographic characteristics.[17] Yet the Enforcement Statement imposes none of those obligations. States are already moving further. Utah requires a 95% accuracy threshold.[18] New York's proposed rules require specific accuracy minimums, 98% circumvention detection, and annual third-party certification under international standards.[19] A facial age estimation system that systematically misidentifies Black children as older should not be able to meet the FTC's standard here while functionally denying those children COPPA protections. The Enforcement Statement should require accuracy standards for age verification that address risks of demographic bias to ensure that minors of all backgrounds benefit from COPPA protections.

Conclusion

For age assurance to succeed, families must be able to trust it. If the federal government's own standards fail to protect the data collected from children during the verification process, the result will not be greater safety. It will be unforeseen harms and public backlash that sets back the cause of child protection online. We are concerned the Enforcement Statement as written risks doing exactly that.

The FTC has the expertise and the authority to do better. We urge the Commission to pursue COPPA rulemaking on age assurance and revise the Enforcement Statement to align it with the FTC's own established standards for sensitive data, and seize this moment to provide the national leadership on age assurance that children and families deserve.

We welcome the opportunity to discuss these concerns further with your offices and other Commission staff.

Sincerely,

Center for Digital Democracy (CDD)

Electronic Privacy Information Center (EPIC)

Fairplay

[17]In re Rite Aid Corp., *supra* note 7 (alleging failure to test accuracy and to assess or address risks of disproportionate harm based on race, gender, or other demographic characteristics).

[18]Utah Minor Protection in Social Media Act, Utah Code § 13-71-101(2) (defining "age assurance system" as measures with "an accuracy rate of at least 95%").

[19]N.Y. Office of the Attorney General, Proposed Rules for the SAFE for Kids Act (Sept. 2025) (requiring specific accuracy minimums, 98% circumvention detection rates, and annual third-party certification under ISO/IEC 27566 or IEEE 2089.1).