wiley

ALERT

Key Takeaways from FTC Age Verification Workshop: COPPA Updates May Be on Horizon

January 30, 2026

On January 28, the Federal Trade Commission (FTC) hosted an Age Verification Workshop focused in large part on the interplay between the FTC's enforcement of the Children's Online Privacy Protection Act (COPPA), which requires online services to provide notice and verify parental consent before collecting personal information from children under the age of 13, and developments in age verification technology. The Workshop featured four panels focused on: (1) why age verification matters; (2) age verification and estimation tools; (3) navigating the regulatory contours of age verification; and (4) how to deploy age verification more widely. Panelists included representatives from industry, state legislatures, and civil society think tanks, and panels were moderated by FTC privacy staff. The Workshop highlighted the FTC's continued emphasis on adoption of age verification technology, and previewed potential policy changes or amendments to the COPPA Rule to facilitate wider adoption of age verification.

Below we summarize the panelists' and speakers' comments, outline key themes that cut across several panels, and preview likely next steps from the FTC.

The FTC Commissioners Support Age Verification Technology

Remarks from Chairman Andrew Ferguson and Commissioner Mark Meador expressed their support for the use of age verification technologies to protect kids online. Chairman Ferguson highlighted the recent COPPA enforcement action and settlement with Disney, which allows Disney to phase out mandated reviews for child-directed

Authors

Ian L. Barlow
Of Counsel
202.719.4994
ibarlow@wiley.law

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kimberly S. Alli
Associate
202.719.4730
kalli@wiley.law

Practice Areas

FTC and Consumer Protection

content posted to YouTube if in the future YouTube agrees to use age verification technology to ensure COPPA compliance. Commissioner Meador argued that implementation of age verification technology does not impede free speech and is similar to other age restrictions, such as for tobacco or alcohol, that exist in the physical world. A similar sentiment was echoed by panelists throughout the day.

Panel 1: Need for Age Verification Technology

The opening panel discussed why they believe online age verification is needed, differences between "age verification" and "age assurance," and the status of state laws regulating age verification. To guide the discussion, panelists explained that "age verification" is one method of "age assurance," which is an umbrella term that also includes self-declaration and technology-based age estimation. They defined true "age verification" as involving more rigorous methods such as ID checks or third-party credentialing. Panelists throughout the day agreed that self-declaration alone is not sufficient or reliable to verify age.

When discussing the status of state laws, panelists also noted regulatory fragmentation. State online age verification laws vary in thresholds, terminology, and methodology. Many state laws are also being challenged in court. Across several circuits, many state laws have been enjoined while others remain in effect. In *Free Speech Coalition v. Paxton*, the U.S. Supreme Court upheld a Texas law requiring age verification for websites with pornography as constitutional. However, the Court did not consider the question of age verification in the context of social media and other online spaces.

Panel 2: Age Verification and Estimation Tools

The second panel discussed different age verification and estimation tools. Building on the age assurance vs. age verification discussion above, panelists offered examples of existing age assurance technology including inference systems, facial age estimation, document-based verification, reusable digital IDs or "age tokens," novel biometrics (e.g., hand movement), and interoperability initiatives (e.g., passkeys). Panelists agreed that using layered systems ("waterfall approaches") – starting with low-friction methods and escalating only when needed – is generally a best practice. Panelists also discussed:

- Ways kids circumvent age verification (e.g., parent impersonation or VPN spoofing) and other fraud concerns;
- Legal consideration that age verification is not verifiable parental consent under laws like COPPA;
- Privacy considerations, including the use of data minimization, which limits collection, use, and retention of personal information to certain tailored purposes;
- The need for regulators to clarify how companies may process children's data during age estimation, particularly when a child lies about their age and the system later detects it.

Panel 3: Regulatory Contours

The third panel discussed the regulatory contours of age verification. One panelist raised privacy concerns associated with age verification and noted the risk of cybersecurity incidents involving data collected about children. The discussion also covered First Amendment objections that have been at issue in the cases challenging various state age verification laws.

This panel also addressed COPPA and how states look to its parental-consent methods as a foundation for broader age-verification regimes. The panelists noted a tension between COPPA's neutral age gate requirement – which permits certain websites to rely on a neutral age gate in which a user inputs their age – and states' desire for stronger age-assurance obligations. They argued that states need COPPA to remain flexible enough to allow for innovative verification technologies (e.g., age keys, digital identity systems).

Panel 4: Deploying Age Verification Widely

The last panel discussed what companies are already doing, risk-based approaches to determine when and how age verification should be used, and other parental controls that are part of the larger effort to protect kids online. In terms of current approaches, industry representatives focused on parental controls, including tiered teen social media accounts that require parental approval and parental controls for downloading apps. All of the panelists agreed on using a risk-based approach under which high-risk contexts (like pornography and age-restricted goods) may merit verification, while other contexts might employ lighter assurance or none. One panelist noted that apps designed for business-to-business services likely do not require any age verification. The panelists also agreed that age verification is just one tool among many to protect kids that should also be combined with parental controls, screen-time limits, web filters, safety-by-design defaults, and family conversations about online use.

Four Key Themes and Assumptions Cut Across Panels:

1. *Age verification implementation is here to stay and on the rise.* Even with legal challenges pending to state-mandated age verification, industry is starting to make changes to implement this technology and has recognized that age restrictions are appropriate in many circumstances. The FTC, legislators, and many civil society groups appear to be in agreement to continue pushing for broader implementation.
2. *There is regulatory uncertainty around age verification requirements and how online age verification fits with current privacy laws.* Throughout the day, panelists discussed fragmented laws with different terminology and requirements, litigation challenging current state laws, and the tension between state laws and COPPA requirements, which create a difficult compliance landscape.
3. *The future of age verification technology likely won't be a one-size-fits-all approach.* Legislators at the workshop recognized that different age assurance and verification processes may be appropriate for different situations, and industry representatives favored a risk-based approach. Several speakers also discussed that laws must have sufficient flexibility to allow for innovation.
4. *Legislators and industry have data minimization concerns.* Across every panel, speakers noted that age verification technology requires collecting and storing certain personal data, but that this is an

area where data minimization is appropriate.

What's Next for the FTC on Age Verification and COPPA

Chairman Ferguson said he "expect[s] the fruits of this workshop will inform future FTC policy statements on age verification technology, as well as a possible amendment of our own COPPA rule that will promote the age verification technologies in compliance with COPPA." A policy statement or rule amendment may address COPPA's current requirement that certain websites and online services obtain verifiable parental consent to collect the data that may be necessary to verify whether a new user is a child protected by COPPA. In January 2025, then-Commissioner Ferguson wrote that the Commission "missed an opportunity" to change COPPA's current requirement of parental consent to create an exception for the collection and use of information solely for age verification, "along with a requirement that such information be promptly deleted once that purpose is fulfilled." In his closing remarks at the workshop, FTC Consumer Protection Bureau Director Christopher Mufarrige said that a "statute designed to empower parents to protect children online should not be an impediment to the most child-protective technology to emerge in decades."

Although issuing a policy statement and updating the COPPA Rule might seem duplicative, a policy statement would be faster for the FTC to approve than a rulemaking, which must follow statutory requirements for public notice and comment. Thus, a policy statement could provide companies with guidance about what types of age verification practices the FTC would decline to enforce against while the rulemaking proceeds. However, while a policy statement would provide companies with clarity about FTC enforcement, it would not bind states, which can also enforce COPPA. An amendment to the COPPA Rule, on the other hand, would be binding on states as well as the FTC.

For more information, please contact one of the authors listed on this alert. Wiley's FTC and Consumer Protection and Privacy, Cyber & Data Governance practices have a deep bench of attorneys with experience serving a wide array of companies and business groups that deal with FTC, privacy, and consumer regulatory issues across industries.