Cooley

Navigating the Age Assurance Maze: FTC Signals Potential Guidance on Harmonizing COPPA With Robust Age Assurance Technologies

February 4, 2026

On January 28, the Federal Trade Commission (FTC) hosted a workshop on age assurance, where FTC leadership signaled new guidance may be forthcoming to clarify potential conflicts between age assurance efforts and federal law. At the workshop, titled, "Protecting American Children: A Workshop to Explore Age Verification Technologies," FTC leadership acknowledged a tension between implementing age assurance technologies, which may be required to comply with state laws, and complying with the Children's Online Privacy Protection Act (COPPA). FTC leadership indicated they are exploring solutions to resolve this tension, while also balancing competing interests of privacy, online safety, free speech and user experience. The workshop panels, which included participants from industry, state governments, the UK data protection regulator's office and other stakeholders, highlighted how companies with an online presence face varying regulatory, privacy and security concerns as they seek to deploy age assurance methods proportional to their business' customer profile and age-related risks.

The FTC perspective: Compatibility of compliance and innovation

In his opening remarks, FTC Chairman Andrew N. Ferguson stated that COPPA remains a top enforcement priority for the agency. He framed the workshop as a critical fact-finding exercise to explore how the FTC can apply COPPA to emerging age verification solutions. Ferguson cited recent COPPA enforcement activity to demonstrate the agency's commitment to online child safety. He argued that innovation and compliance need not be in tension.

Ferguson's view was echoed by FTC Commissioner Mark R. Meador, who argued that age verification is not novel. Instead, he framed age verification as a familiar, protective principle, citing parallels to age gates used for regulated physical goods, such as cigarettes and alcohol. He argued that technological solutions are necessary to support parents and protect youth online. Specifically, Meador commended the development of tools that allow for a one-time, centralized age verification process, which, once complete, can be portable and used across different platforms, thereby avoiding the need to provide raw personal data to every app and website requiring verification. He referred to these emerging technologies as "efficient," "secure" and "the future."

FTC Director of the Bureau of Consumer Protection Christopher Mufarrige reaffirmed the agency's focus on COPPA enforcement, while recognizing that some age verification technologies require the collection of personal information **before** parental consent can be obtained – a direct source of friction with COPPA. Similarly, COPPA may serve as an impediment for companies that wish to create automated methods, including artificial intelligence-based models, to automatically identify and disallow children under 13. COPPA poses challenges for the building of such models, and companies have long hoped the FTC would provide guidance clarifying that the use of personal information of children under 13 for these purposes will not result in liability. Mufarrige clarified that COPPA should not be an impediment to age verification and stated that the agency is exploring solutions to reconcile the chicken-versus-egg dilemma between age verification and privacy.

Age assurance technology and the privacy spectrum

During the daylong workshop, technology experts and members from industry emphasized that age assurance includes a spectrum of technologies. Industry participants largely agreed on the use of a risk-based approach, applying these technologies proportionally to the privacy and safety risks posed by a particular platform. The age assurance technologies fall into three main categories, each with distinct privacy and security implications:

Self-declaration

Self-declaration of age may involve asking a user to either confirm they are above a certain age or provide their date of birth. Where a child misstates their age, this may allow them to potentially avoid triggering additional safeguards. This risk prompted at least one panelist to argue that self-declaration should not be treated as age assurance at all.

Inference/estimation

This includes approaches that infer or estimate age using behavioral signals, AI models, facial age estimation or metadata. These methods offer lower user friction but can raise concerns about accuracy and the collection of potentially linkable identifiers.

Verification

This involves stronger methods that verify age using authoritative data checks, government ID and selfie matching, or reusable digital IDs/tokens. While possibly providing greater assurance, these methods may carry the most substantial privacy risk (at least when deployed by a throng of individual platforms) and could result in significant user drop-off.

For any of these technologies, participants stressed the use of privacy by design. Solutions should aim to prove age without revealing identity or transmitting unnecessary personal details, leveraging techniques like double-blind designs, selective disclosure and zero-knowledge signaling application programming interfaces (APIs) to prevent secondary use, limit data retention and mitigate risk of identity theft.

The fragmented, global regulatory landscape

The need for clear FTC guidance is magnified by the rapidly changing – and increasingly disjointed – regulatory landscape in the United States and around the world.

Many **US states** have age-gating laws that require platforms to restrict minors' access to and/or require parental consent for certain online content. States have turned to age assurance to tackle different problems, further complicating the regulatory landscape and inviting constitutional challenges.

Some states have passed laws specifically requiring age gates for websites where a certain portion of content (often one-third) is "harmful to minors," while other states have targeted social media platforms. Some states – California, Louisiana, Texas and Utah – also passed laws placing the burden on app stores to verify a user's age and implement certain age safeguards. A federal court preliminarily enjoined the Texas law (SB 2420) in December 2025, and the case is now on appeal before the US Court of Appeals for the Fifth Circuit.

At the federal level, the FTC's recent amendments to the **COPPA Rule** are enforceable starting April 22, 2026. As amended, parents will need to opt in via a verifiable parental consent mechanism for companies to disclose children's personal data to third parties for targeted advertising purposes. Companies must only retain children's personal data for the purpose it was collected, with indefinite retention prohibited, and approved safe harbor organizations will need to disclose membership lists and report additional information to the FTC for increased accountability and transparency. Additionally, the definition of "covered data" will expand to expressly include government-issued identifiers and biometric identifiers.

In **Europe**, the Audio-Visual Media Services Directive, the EU Digital Services Act and the UK Online Safety Act impose age assurance requirements on certain online services. Most European Union member states are also actively debating social media bans – with a French bill banning social media for users under 15 likely to become law. Additionally, the EU Digital Identity Regulation requires each EU member state to implement an interoperable digital wallet that will allow individuals in the EU to prove their age (or age range) without revealing additional personal information. This regulation also requires providers of certain large services to accept the wallet for user authentication, where authentication is already required. An interoperable token-based wallet was one of the age assurance methods heavily discussed during the FTC workshop as a reliable age assurance method that is also privacy-protective and efficient.

As of December 2025, **Australia's** ban on major social media platforms for Australians under the age of 16 came into effect – with providers required to take "reasonable steps" to enforce the ban. The Australian government published a detailed report in August 2025 with technical findings about various age assurance technologies. US legislators have proposed similar legislation and debated social media age restrictions as recently as January 2026.

Issues we are tracking

In preparation for potential guidance from the FTC, there are several key issues companies may consider as they assess whether age assurance is appropriate for their platform and what age assurance methods best address their risks:

1. **A heightened standard to trigger age assurance obligations:** US state and foreign laws increasingly use standards other than COPPA's "actual knowledge" standard. Even if COPPA does not apply, companies should consider whether their online content could trigger age assurance obligations under other standards (such as the "one-third" standard used by some US states).
2. **Risk-based approach:** Different platforms have different purposes and risk profiles. An age assurance framework that is appropriate to implement in one context may not be appropriate in another. When determining how to balance safety and privacy trade-offs, it is important to calibrate the approach to the specific platform and its risk profile.
3. **Privacy by design:** Privacy is critically intertwined with age assurance. Data minimization and other privacy-preserving efforts are important foundations for deploying age checks – collecting only what is necessary, using privacy preserving techniques to process data, and deleting data quickly after use to avoid legal exposure and security risks.
4. **Post-verification protections:** Government and industry participants suggested that age assurance should be a continual process, rather than a one-time event, to address risks of circumvention later in time. Meador referred to behavioral age assurance – based on how a user interacts with a platform over time – as "one of the best uses for artificial intelligence" and an opportunity for US companies to lead the world in inferred age assurance efforts.
5. **Scalable solutions:** Interoperable solutions, such as standardized "age keys," reusable credentials or API signaling, may provide useful means for scaling age assurance across the online ecosystem. However, these efforts may also raise privacy and security risks that require contractual and technical safeguards.

Key Contacts

Scott Dailard San Diego	sdailard@cooley.com +1 858 550 6062
Brett R. Weinstein New York	bweinstein@cooley.com +1 212 479 6306

Sean Quinn New York	squinn@cooley.com +1 202 728 7075
Tristan Lockwood London	tlockwood@cooley.com +44 20 7556 4115
Morgan Perna Washington, DC	mperna@cooley.com +1 202 776 2402
Nathaniel L. Kim Boston	nkim@cooley.com +1 617 937 2302
Adam Silow New York	asilow@cooley.com +1 212 479 6163