Centre for Information Policy Leadership
HUNTON

Establishing and Implementing Standards for Interoperable Age Assurance Solutions

Key Takeaways from CIPL's Roundtable

September 2026

Takeaways from CIPL Roundtable:

Establishing and Implementing Standards for Interoperable Age Assurance Solutions

HELD 23 JULY 2026
SAN FRANCISO, CALIFORNIA

Age assurance has emerged as a central mechanism in global efforts to protect minors online. Regulatory and legislative efforts worldwide are driving demand for technical standards that are robust, privacy-preserving, and interoperable across jurisdictions.

On July 23, 2026, the Centre for Information Policy Leadership (CIPL) convened a roundtable in San Francisco to assess the landscape of current age assurance standards, to identify gaps, and to explore practical paths toward harmonization and implementation, with a particular focus on the work advanced by the International Organization for Standardization (ISO) and the Institute of Electrical and Electronics Engineers (IEEE).

Participants included senior professionals from CIPL member companies, along with representatives from standards bodies, regulatory agencies, and civil society organizations. The event was conducted under the Chatham House Rule to foster open and candid dialogue.

CIPL is pleased to share the following takeaways.

Standards landscape and terminology

- **A shared vocabulary exists but is not applied consistently.** With "age assurance" generally recognized as the overarching umbrella term, standards make distinctions between age verification (confirming date of birth), age estimation (using biometrics), and age inference (deriving age from other data points). At present, these terms are often applied interchangeably and inconsistently across jurisdictions and organizations.
- **Age inference comprises varied and distinct methodologies.** It can refer to (i) a conclusion from a known fact,[1] (ii) the tracking of behavioral signals,[2] and (iii) an evaluation of transactional factors such as the length of account tenure.[3]
- **Behavioral profiling for age estimation is in an "awkward adolescence phase."** This reflects a tension between its practical value and the ability of services to explain and govern its use. Behavioural profiling is often used to reduce friction, as it can draw on data already held by a service rather than requiring users to complete a separate age check. It can also play an important role in identifying possible circumvention following an initial check. However, the ongoing analysis of behavioural data can make it difficult for users to understand when an age inference is being made, which signals inform it, and how the resulting assessment is used.

- **There's a strong consensus on separating identity verification from age assurance.** Verifying age status ("is this person over 18?") will not require identifying the specific individual.
- **Practical guidance is needed to support consistent use of a common taxonomy.** Technical standards provide an important foundation for a common age assurance taxonomy. Greater coordination among standards bodies could help align terminology and clarify how different standards relate to one another. Building on this alignment, joint awareness-raising and practical guidance by the standard bodies would help regulators and organizations apply consistent terminology in regulation, procurement, and system design.

Alignment between standards and standards bodies

- **Age assurance standards are being developed in parallel across several bodies**, at different speeds and with different degrees of formality. ISO, IEEE, IETF[4] and W3C[5] are all active in this space, with the potential of creating uncertainty for regulators seeking a unified reference point to anchor law.
- **The effectiveness of the standards landscape will depend on the coherence and interoperability** of standards developed by different bodies. Clearly defined scopes and greater clarity on how the standards interact will support their complementary implementation.[6]

Awareness and accessibility of standards

- **Awareness of existing technical standards for age assurance remains uneven across the policy and regulatory landscape.** Some regulators are already using international standards to inform guidance and safe-harbor frameworks, while others may be less familiar with the available instruments.[7] Improving awareness of existing standards could help promote greater consistency and reduce duplication in future policymaking.
- **Public access to standards supports transparency, effective implementation, and meaningful evaluation.** Organizations and other affected stakeholders need to be able to consult relevant standards with ease to understand what is expected of them, assess their practical implications, and contribute informed feedback regarding their effectiveness.[8]

Remaining gaps

- **Common measures of accuracy and effectiveness are needed.** Key parts of standards remain under development, leaving no shared basis by which to measure providers' services. In the absence of agreed metrics, testing conditions, and thresholds, organizations find it difficult to evaluate third-party age assurance providers.
- **The applicability of existing standards to platforms' internal age assurance practices remains unclear.** Current standards have been developed primarily with third-party age assurance providers in mind, and questions remain as to whether, and in what manner, these standards should apply where platforms employ age assessments with their own systems and processes.

- **National approaches may address immediate policy needs but could risk creating additional fragmentation.** Differences in regulatory requirements across jurisdictions, combined with the continued lack of interoperability between systems, contribute to the challenge. Global standards are seen as a more sustainable long-term solution, provided they are flexible enough to accommodate legitimate jurisdiction-specific requirements.
- **Accuracy claims cannot readily be verified by those relying on them.** Providers often report high levels of accuracy, but organizations procuring their solutions may lack access to the testing data and methodologies needed to assess these claims independently. The absence of agreed performance benchmarks also makes it difficult to determine what level of accuracy is sufficient for a particular use case. For age-estimation methods, this challenge is even greater because their outputs carry an inherent margin of error.
- **The evolving standards landscape requires greater coordination and clarity.** As different bodies develop technical standards, protocols, certification schemes, and regulatory guidance, greater clarity is needed on their respective roles and scopes, how these initiatives relate to one another, and how they can work together as part of a coherent and complementary framework.

Adoption and implementation of standards

- **Nascent/developing standards still provide little incentive for adoption.** With standards still in their infancy, certification to standards often remains voluntary, used by individual providers to distinguish themselves. Greater recognition of relevant standards in regulatory frameworks could encourage wider adoption.
- **Effective age assurance depends not only on the method used, but on how it is implemented.** Even recognized or certified methods may perform differently depending on system design, deployment context, and ongoing monitoring. Assessments should therefore consider how a method performs in the specific use case, rather than relying on recognition or certification alone.
- **Industry-led standards from other age-restricted sectors.** In the alcohol and tobacco sectors, voluntary, sector-led standards have been used to establish common expectations for online age checks. Although these sectors are not directly comparable to many online services, their experience illustrates how early industry coordination can complement and inform regulation.

Regulatory approaches: risk, harmonization, and fragmentation

- **There is no shared legal starting point for age assurance obligations.** In the EU and UK, age assurance requirements are anchored in data protection law and online safety rules.[9] In the United States, they arise from a patchwork of state legislation with no federal privacy framework to underpin them.[10] These differences affect the scope of the obligations, the relevant age thresholds, and the safeguards governing the associated processing.
- **Compliance with a technical standard does not, by itself, establish that the associated processing is lawful.** Where legally required, organizations must still identify an appropriate legal basis and comply

with requirements relating to necessity, proportionality, transparency, and data minimization. Regulatory guidance should distinguish between a minimum age for accessing a service and the age at which a child may consent independently to the processing of personal data.

- **The available legal bases for safety-related processing remain narrow in the EU and UK.** Consent, vital interests, and substantial public interest each face structural limits when applied to safety processing, and other measures — including the Digital Omnibus proposal[11] and the UK Data (Use and Access) Act 2025[12] — remain limited in scope. The practical effect is that some services may decide to withhold certain safety features in these markets.
- **Prescriptive versus outcomes-based regulations.** Some regulations identify methods considered sufficiently effective for particular contexts, while others allow services to determine how best to meet expectations for accuracy and effectiveness. Standards should ultimately be capable of supporting both approaches.
- **Risk-based regulation is widely endorsed in principle, but its application remains inconsistent.** Regulatory expectations should reflect the nature and severity of the risk, the characteristics and features of the service, existing safeguards, and the relevant age threshold. In the absence of a shared risk taxonomy, standards can help define levels of assurance and expected outcomes without prescribing a single technology.
- **Balancing flexible approaches with baseline requirements.** Age assurance should be adaptable to the circumstances and risks of a particular use case, enabling proportionate approaches. At the same time, common baseline requirements can provide greater certainty and consistency across the market. The challenge is to determine which elements require a consistent baseline and which should remain responsive to context.
- **Accuracy expectations should account for the degree of deviation from the relevant age threshold.** Misclassifying a user who is close to the threshold (for example, age 16 or 17) may pose a risk different from misclassifying a materially younger user (for example, age 12 to 13). Standards and safe-harbor frameworks should reflect these distinctions.
- **Technical standards should inform regulatory frameworks.** Similar products may be subject to different regulatory requirements depending on where they operate. While standards cannot resolve differences in policy objectives, they can support greater consistency in how age assurance is implemented.
- **Greater cross-regulatory cooperation is needed to address regulatory fragmentation.** Bringing privacy and online safety regulators together, establishing formal coordination fora, and developing regional accreditation schemes can help reduce duplication and minimize conflicting obligations.

Interoperability and privacy-enhancing technologies

- **Interoperability does not rest solely on technical compatibility.** While technical advances may permit age checks to move beyond a single transaction, jurisdictions accept different methods and apply different age thresholds or assurance requirements. As a result, a check that is sufficient in one context may not always be accepted in another, requiring users to repeat the process. This means that the current ecosystem remains fragmented across providers, platforms and jurisdictions. Effective

interoperability will require common technical frameworks as well as agreement on assurance levels, trust, and accreditation.

- **Effective interoperability requires common terminology**, clearly defined levels of assurance, criteria for recognizing trusted signals, and a clear allocation of responsibilities across the ecosystem. Standards can provide common reference points for these elements while remaining sufficiently flexible to accommodate different technologies, use cases, and regulatory requirements.
- **Credential management APIs are a pivotal recent development**, allowing users to share an age signal from a stored credential. Their use across services and jurisdictions, however, depends on common technical protocols and trust frameworks.
- **Privacy-enhancing technologies can support age assurance.** For instance, zero-knowledge proofs can verify that a person meets a required age threshold without disclosing any additional personal information. Selective-disclosure credentials can reveal only the specific attribute needed. Cryptographic attestations can also allow a trusted issuer to verify an age-related fact without requiring direct interaction between the issuer and the relying service. Their acceptance across services and jurisdictions, however, depends upon relying parties being satisfied that a privacy-preserving signal meets their needs.
- **The main barrier to full interoperability is the accreditation of "trusted signals."** Greater clarity is needed from standards bodies and regulators on what constitutes a trusted age signal. Related questions include the criteria for evaluating reliability and the designation of entities to be responsible for accreditation or recognition.

Parents, children, and the wider ecosystem

- **Regulatory frameworks should distinguish between baseline safeguards and areas of parental discretion.** Privacy and safety protections should be embedded in services by design, while parents and caregivers should be able, where appropriate and proportionate, to make choices in light of a child's needs, maturity, and evolving capacities.
- **Meaningful parental involvement depends on transparency and usable controls.** Parents and caregivers need clear information about risks, safeguards, and available choices. Existing parental controls may not always provide the level of granularity needed to reflect different family circumstances and preferences. Greater consistency across services would support greater ease of use for parents and caregivers.
- **Parents and children should be recognized as stakeholders in standards development**, rather than considered only at the point of implementation. Their perspectives can help ensure that standards reflect children's evolving capacities and different family circumstances. Greater clarity is needed by standard bodies on when and how these perspectives should be incorporated in the design.

Global applicability and inclusion

- **Global standards should not assume universal access to identity documents or personal devices.** In some jurisdictions, official identification may not be available to children, devices may be shared,

connectivity may be limited, and regulatory capacity may vary. These conditions affect which methods are practical and inclusive.

- **A choice of methods can reduce exclusion.** Age assurance should accommodate users who cannot or do not wish to use a particular credential or technology. Alternatives should be assessed for accessibility, security, accuracy, and privacy rather than treated as interchangeable.
- **Standards should consider children's benefits and access alongside protections from harm.** Age assurance should support age-appropriate participation in the digital environment and should not become an exclusionary tool where less restrictive safeguards can address the relevant risk.

RECOMMENDATIONS

- Harmonize terminology across standards bodies and regulators.
- Make standards publicly accessible. Public access supports transparency, accountability, and effective implementation by organizations and affected stakeholders.
- Clarify the respective roles of standards bodies and how their outputs relate to one another. Define the scope of each standard and explain how relevant standards should be used together, giving regulators and organizations a coherent reference framework and avoiding conflicting or duplicative requirements.
- Strengthen the role of standards and certification in procurement. Issue practical guidance on how organizations can assess alignment with standards, interpret certifications, and incorporate appropriate requirements into due diligence, contractual terms, and ongoing oversight.
- Develop a common approach to recognizing and accrediting trusted age signals. Establish criteria for issuers, providers, and assurance levels that can support reuse across services and, where possible, jurisdictions.
- Develop a shared taxonomy of risks and methodologies. Map service- and feature-level risks to proportionate assurance levels and expected outcomes, without mandating a specific technology.
- Embed transparency, data minimization, purpose limitation, accessibility, and user choice into standards and certification frameworks.

REFERENCES

1 International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 27566-1:2025, Information Security, Cybersecurity and Privacy Protection — Age Assurance Systems — Part 1: Framework, 1st ed. (Geneva: ISO, 2025), available at https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27566:-1:ed-1:v1:en.

2 Behavioral monitoring may operate as a secondary safeguard to identify users who have misrepresented their age or circumvented an earlier check, rather than as a method for establishing age at the point of entry. Conflating these functions can obscure the purpose of the processing and the level of assurance provided. See also, Ofcom, *Use of Age Assurance Report 2026* (London: Ofcom, 2026), available at https://www.ofcom.org.uk/online-safety/protecting-children/use-of-age-assurance-report-2026.

3 Australian Government, Department of Infrastructure, Transport, Regional Development, Communications and the Arts, *Age Assurance Technology Trial: Final Report* (Canberra: Department of Infrastructure, Transport, Regional Development, Communications and the Arts, 2025), available at https://www.infrastructure.gov.au/department/media/publications/age-assurance-technology-trial-final-report.

4 Internet Engineering Task Force, available at https://www.ietf.org/.

5 World Wide Web Consortium, home page, available at https://www.w3.org/.

6 The processes used by IEEE and ISO differ in their participation models, pace and routes. IEEE develops standards through internationally open working groups, allowing emerging concepts and operational approaches to be developed and tested relatively quickly. ISO follows a consensus-based process involving national delegations, which generally takes longer but can support broader international recognition and alignment. IEEE work may therefore provide an experimental foundation from which concepts can mature and potentially inform later ISO standardization, although there is no formal or automatic progression between the two bodies, which retain independent processes and mandates.

7 See, for example, Ofcom, *Guidance on Highly Effective Age Assurance* (London: Ofcom), https://www.ofcom.org.uk/; or Utah Department of Commerce, Division of Consumer Protection, https://commerce.utah.gov/dcp/.

8 The decision to make ISO/IEC 27566 available free of charge illustrates one approach to improving access to technical standards. Please see: International Age Assurance Standard to Be Open, Free of Charge," *Biometric Update*, January 2026, available at https://www.biometricupdate.com/202601/international-age-assurance-standard-to-be-open-free-of-charge.

9 See Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119/1 (4 May 2016), https://eur-lex.europa.eu/eli/reg/2016/679/oj; Regulation (EU) 2022/2065 (Digital Services Act), OJ L 277/1 (27 October 2022), https://eur-lex.europa.eu/eli/reg/2022/2065/oj; and, in the United Kingdom, the Data Protection Act 2018, c. 12, https://www.legislation.gov.uk/ukpga/2018/12, and the Online Safety Act 2023, https://www.legislation.gov.uk/ukpga/2023/50.

10 See, for example, Utah Code Ann. § 13-63 (Utah Social Media Regulation Act); N.Y. Gen. Bus. Law § 1500 et seq. (Stop Addictive Feeds Exploitation for Kids Act); and Tex. Bus. & Com. Code Ann. § 509 (App Store Accountability Act). At the federal level, the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506, applies to children under 13, but no general federal privacy statute governs age assurance.

11 European Commission, "Digital Omnibus Regulation Proposal," *Shaping Europe's Digital Future*, November 19, 2025, available at https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal?ref=eutechloop.com.

12 Data (Use and Access) Act 2025, c. 18, available at https://www.legislation.gov.uk/ukpga/2025/18/contents.

Who We Are

The **Centre for Information Policy Leadership (CIPL)** is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.