A Multi-Stakeholder Dialogue on Age Assurance

Working Group on Global & Regional Perspectives

KEY TAKEAWAYS

Working Group Roundtable

22 October 2024

Washington, DC

A Multi-Stakeholder Dialogue on Age Assurance

Working Group on Global & Regional Perspectives

K E Y   T A K E A W A Y S

22 October 2024

Washington, D.C.

On 22 October 2024, the Centre for Information Policy Leadership (CIPL) and the WeProtect Global Alliance continued their multi-stakeholder dialogue on age assurance in Washington, D.C., where the Global and Regional Perspectives Working Group held its inaugural meeting. The in-person, invitation-only roundtable brought together representatives from industry, academia, and civil society to get a better understanding of the state of play of age assurance, with a particular focus on developments in the United States.

The event was held under the Chatham House Rule.

Below is a high-level summary of the key takeaways, followed by suggested actions.

K EY T AKEAWAYS

■ **Age assurance requirements in US state legislation address a diversity of harms.** US state laws requiring the use of age assurance have arisen in response to concerns about harms to minors from their use of the internet. However, there is no consensus among the states on the harms sought to be addressed. Some seek to shield minors from accessing pornographic content, others seek to prevent access to social media platforms, and still others seek to curb so-called "addictive feeds." Indeed, even laws purporting to address the same type of harm present different views of that harm. Nevertheless, all of the laws view age assurance as a means to curb the harm, whatever it may be.

■ **Effectiveness of age assurance measures to mitigate harms is an open question.** Given that US state laws are still in their infancy, assessments on the effectiveness of age assurance measures to accomplish their varied goals do not yet exist. Notwithstanding the challenges raised by these laws—from both a legal (constitutional) perspective and a practical (implementation) perspective—state legislators will likely remain active in this area, continuing to view age assurance as a "silver bullet" to address a host of alleged harms—a view not shared by most of the participants, who recognize the need to use a combination of measures, not age assurance alone, to keep children safe online.

■ **Risks to privacy from the collection of data.** While many state laws prohibit the retention of data collected for age assurance, participants nevertheless expressed concerns about potential risks

materializing prior to the deletion of such data, such as unauthorized data sharing, data harvesting, and potential secondary uses. The potential fallout from unauthorized access and related security incidents is a perennial concern.

■ **Clarity is needed for action thresholds and knowledge standards.** State legislative measures can on occasion be vague on what triggers the obligation to use age assurance. Companies are sometimes unsure if they must independently assess the age of users *before* employing an age assurance method, especially in situations where the obligation arises in the case of a "known child" or a "known minor." For example, New York's Safe for Kids Act prohibits the operator of an "addictive social media platform" from providing an addictive feed to a covered minor unless the operator has obtained verifiable parental consent. Must an operator first determine if a user is a covered minor before deploying a consent feature? Relatedly, companies are sometimes unsure whether age assurance should be deployed to satisfy a "should have known" threshold in laws that do not expressly mandate the use of age assurance measures.

■ **Industry standards and certifications can build trust in age assurance measures.** Participants recognize the benefits of age assurance technologies and appreciate third-party vendors' transparency in sharing data and findings that support their products. Participants noted the need for international industry standards and certifications to establish a baseline for vendor services, to enable benchmarking, and to build confidence in vendor offerings generally. Standards and certifications could also help varied stakeholders (e.g., lawmakers, policymakers, and the general public) to understand the capabilities of different technologies.

■ **A variety of elements factor into an assessment of age assurance measures.** An assessment of the effectiveness of a given age assurance method depends on priorities and perspectives. Each method has different strengths and capabilities, and a measurement of its success will vary depending on the factors deemed most important, e.g., accuracy of the results, minimization of data collection, ease of use, etc. Sometimes these factors can be in tension. For example, an end-user taking a selfie while holding a government ID can provide highly accurate results, but it also collects a great deal of data. The key factors for assessing age assurance methodologies include:
   o **Privacy:** How privacy-protective (or privacy-invasive) is the methodology?
   o **Effectiveness:** How effectively does it assess or estimate age?
   o **Cost:** What is the cost of implementation for platforms?
   o **User experience:** To what degree does the methodology introduce unwanted friction or impose an undue burden on adults accessing legal content?
   o **Interoperability:** Will it work across all user platforms, or will it require frequent re-verification?
   o **Inclusivity:** Will it work appropriately for all users, or will it disproportionately generate erroneous results for some?

■ **It's not too late to develop industry-led solutions.** Participants representing the alcohol and tobacco industries recounted how they were intentionally proactive upon entering the online marketplace by coalescing around a voluntary, industry-led standard, which curbed the need for regulatory action. While industries from other sectors are already facing age assurance laws and regulations, they can nevertheless be proactive in developing industry-led solutions to share with regulators. Still, industry players recognize that the formulation of such solutions will be challenging to build and adopt, given the different roles and responsibilities of stakeholders across

the online ecosystem. Stakeholders are not likely to align on a single approach. Flexibility will be key to advancing a range of solutions moving forward.

- **A risk-based approach may be in tension with political realities**. Participants generally agreed that age assurance measures should be appropriate and proportionate to the level of risk and not be overly prescriptive. Most would therefore support legislation that requires a risk assessment with a proportionate response (without overly prescribing what that response would be). That said, laws are being enacted without requiring risk assessments, as lawmakers have already deemed certain content or certain platforms as high risk. While some participants felt the need to push back against laws lacking an assessment of risks, others thought that support for particularly effective, privacy-protective forms of age assurance—rather than advocating for risk assessments—would be an easier lift, given the political pressure.

- **Special considerations around age assurance legislation.** Participants raised concerns about age assurance measures potentially leading to the suppression of certain types of speech or the chilling of anonymous speech. Although many state laws are currently being challenged in US courts, some feared that such laws could nevertheless be copied in countries that lack robust free speech protections. Moreover, to the extent certain laws include parental consent and/or parental control provisions, some cautioned that such features could inhibit minors' access to information and/or fora they deem valuable.

SUGGESTED ACTIONS

➔ **Articulate age assurance capabilities clearly and transparently.** Stakeholders should develop a framework that articulates and clarifies different approaches to age assurance so that policymakers, legislators, industry, and others can understand the strengths and weaknesses of different methods and choose the method(s) best suited for a given purpose.

➔ **Evaluate whether and how age assurance effectively mitigates identified harms.** Evidence is needed to assess the effectiveness of age assurance in mitigating the harms sought to be addressed by legislation, since minors are quite savvy in fashioning technical workarounds. Relatedly, evidence is needed to measure the impact of various methodologies on minors' (and adults') access to certain content. Stakeholders should work together to devise a means to collect such evidence and share it with policymakers and legislators.

➔ **Develop industry standards and certifications.** International industry standards would help establish a baseline for vendor services, enable benchmarking, and build trust in the use of age assurance technologies. The draft international ISO Age Assurance standard would be a good starting point. Certifications by independent third parties should be explored in tandem.

➔ **Promote privacy-protecting and privacy-preserving solutions.** Limitations on the collection, use, sharing, and retention of data related to age assurance should be established and implemented in laws and regulations.

➔ **Endorse a proportionate, risk-based approach to using age assurance.** Future laws and regulations should adopt a risk-based approach, and current regimes should consider amendments supporting an approach that enables the use of age assurance measures appropriate to the risks that arise in a given context.

➔ **Evaluate the impact of age assurance provisions on marginalized communities.** Lawmakers and policymakers should be made aware of the potential impact of age assurance methodologies on marginalized or disadvantaged communities, such as those who may lack government-issued IDs.

WHO WE ARE

The Centre for Information Policy Leadership (CIPL) is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices to ensure 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 https://www.informationpolicycentre.com/. Nothing in this document should be construed as representing the views of any individual CIPL member company or of the law firm Hunton Andrews Kurth LLP. This document is not designed to be and should not be taken as legal advice.

WeProtect Global Alliance brings together over 300 members from governments, the private sector, civil society, and intergovernmental organisations to develop policies and solutions to protect children from sexual exploitation and abuse online. WeProtect Global Alliance is registered as a Stichting (foundation) in the Netherlands, with a subsidiary company registered in the UK. A Global Policy Board provides expertise and advice to monitor and guide the activities of the organisation.

Secretariat support: Praesidio Safeguarding

Praesidio is a specialist child online safety consultancy that believes that every child has a right to be safe and to thrive in the digital environment. Praesidio is committed to delivering high quality projects which help to create a better and safer online experience for children and young people.