Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

WeProtect GLOBAL ALLIANCE

# A Multi-Stakeholder Dialogue on Age Assurance

## Working Group on Risk Assessments

## Key Takeaways and Next Steps

Working Group Meeting, 19 September 2024

# A Multi-Stakeholder Dialogue on Age Assurance

## Working Group on Risk Assessments

KEY TAKEAWAYS & NEXT STEPS

19 September 2024

Brussels and Online

As part of the ongoing multi-stakeholder dialogue on age assurance led by the Centre for Information Policy Leadership (CIPL) and the WeProtect Global Alliance, the Working Group on Risk Assessments held a hybrid meeting on 19 September 2024 under the Chatham House Rule.

The aim of the meeting was to further the understanding of the complexities and challenges of assessing risk—specifically in the context of whether and how to deploy age assurance methodologies—and to outline a framework for a robust risk assessment that takes privacy and safety considerations into account.

Below is a high-level summary of the key takeaways, along with suggested next steps.

## Key Takeaways

### Identifying Current Challenges

- The risk assessment landscape remains challenging due to varied and yet undefined terminology (e.g., "systemic risk") across different regulatory regimes. Moreover, similar terminology can mean different things in different cultural contexts, adding to the complexity. Stakeholders need a clear baseline for risk assessments, with a focus on the risk of *what*, to *whom*, and *when*, and the best interests of the child as the guiding North Star.

- Risk assessments in the context of the GDPR differ from risk assessments in the context of children's safety. Risks also vary in the context of different online services and their offerings.

- Regulators and regulated entities may understand and categorize risks differently, with regulators often attaching a higher risk score.

- Companies continue to struggle when addressing pertinent risks comprehensively. Holistic risk assessments require consideration of a number of issues, including human rights, children's rights, data protection, and safety. A holistic approach requires engagement with all relevant stakeholders early in the risk assessment process.

## Overarching Considerations

- A one-size-fits-all approach is insufficient; a contextual assessment of risks and opportunities is essential.

- Risk assessments should be forward-thinking to account for emerging risks, such as those presented by AI.

- In light of rapid product development and continual upgrades of product features, risk assessments should be iterative and flexible, incorporating specific mitigation strategies to unique risk profiles and tailoring age assurance solutions to specific services and offerings. The best solution may sometimes comprise a combination of different approaches.

- Meaningful assessments start with a clear understanding of the severity, likelihood, and type of risks for a given product or service.

- Assessments should evaluate specific objectives, such as safeguarding children from inappropriate content and preserving the right to freedom of expression.

- Establishing a baseline for risk assessments can help industry identify shared risks and ensure consistency when deploying age assurance methodologies. Sharing proposed best practices based on multistakeholder engagement will advance the discussion.

## Balancing Safety and Privacy

- Some companies segregate privacy issues from safety issues, but in the context of deploying age assurance technologies, privacy and safety teams should cooperate to ensure a holistic risk profile.

- Privacy risks and safety risks should be addressed holistically to ensure the protection of children’s data and accessibility of age-appropriate content in an accountable manner.

## Implementing Accountability and Governance Measures

- Robust accountability measures—with a clear understanding of the decision-making process and internal responsibilities—will ensure that risks are appropriately addressed and mitigated.

## Embedding Risk Assessments into Product Design

- Risk assessments should not be a one-time exercise, but an iterative, flexible process. Ideally, risk assessments should already be embedded at the product design, user experience design, and product testing stages to ensure full consideration of safety and privacy issues as early as possible. This should include ethical considerations—such as “*Should we do this?”* and *“What happens if we don’t?”*.

- Risk assessments should consider the impact of emerging technologies and potential enhancements to product features, ensuring that age assurance tools remain applicable and appropriate to evolving digital ecosystems. Those responsible for assessing risk should collaborate with product teams and technology developers to understand what innovations (and potential new risks) are on the horizon and to ensure that new factors are considered.

- An organization's approach to defining risks should also adapt as technologies evolve. Organizations will need to determine how to assess potential risks posed by technological enhancements and how to amend the organization's risk framework accordingly.

- Organizations should consider providing guidance for engineers and technologists to help prioritize the safety, privacy, and developmental needs of children through a structured approach to designing age-appropriate online environments (e.g. the CEN-CENELEC Workshop Agreement on an Age-Appropriate Digital Services Framework).

### Balancing Age Assurance with Children's Rights and Participation

- Organizations should factor in potential privacy risks associated not only with the collection and processing of children's data when using age assurance measures, but also the data of adults who may be required to provide proof-of-age to access material deemed inappropriate for children. Recent accounts of the hacking or sharing of users' data have brought to light some of these potential concerns.

- Organizations should take into account the possibility that certain age assurance measures may exclude some adult users from services or platforms that they otherwise have the right to access and, in certain cases, may impair the ability of minors and children to access and participate in age-appropriate services and platforms.

- Organizations should reassess the effectiveness and appropriateness of age assurance measures over time, taking into account the developmental and maturity level of children as they grow older.

- As with any risk assessment, organizations should factor in the benefits and opportunities related to age assurance measures, along with the risks. Age assurance has the potential to enable the creation of specialized services for specific age groups that only members of that age group can access. The potential benefits of such a service should not be lost in the conversation about risks.

### Incorporating Children's Perspectives

- Children's input should not be overlooked when designing and implementing appropriate age assurance measures. Young people of different ages can offer unique perspectives and valuable feedback on the ease, effectiveness, and utility of a given methodology—all of which should be considered for a truly holistic risk assessment. Equally, children's increasing autonomy and maturity levels should be taken into consideration, and risk assessments should consider cultural, familial, or even government contexts that could touch upon privacy or safety concerns (e.g. in an LGBTQ+ context).

- Finally, parental/care-taker involvement is equally crucial. Educators also play a role and their perspectives should be reflected. Designing appropriate age assurance measures should take these considerations and relationships into account, with an understanding of regional and culturable differences and sensibilities.

## AVAILABLE RISK ASSESSMENT GUIDANCE

- U.K. Information Commissioner's Office: Children's Code Self-Assessment Risk Tool
- U.K. Office of Communications (Ofcom): Quick guide to children's risk assessments: protecting children online
- U.K. Digital Regulation Cooperation Forum (DRCF): A Joint Statement by Ofcom and the Information Commissioner's Office on Collaboration on the Regulation of Online Services
- European Union: BIK [Better Internet for Kids] age assurance self-assessment tool for digital service providers
- Ireland Data Protection Commission: Fundamentals for a Child-Oriented Approach to Data Processing

## Suggested Next Steps

- **Develop an overview of risks and guidance.** Create a mapping of existing regulatory frameworks and risk assessment tools to include specific features and types of risk to be assessed across different services.

- **Define tangible mitigation measures.** Propose practical examples of risk assessments and real-world application case studies to help smaller organizations navigate compliance.

## 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.