CIPL
Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

WeProtect
GLOBAL ALLIANCE

A Multi-Stakeholder Dialogue on Age Assurance Law and Regulation

CIPL
WeProtect GLOBAL ALLIANCE
Multi-Stakeholder Dialogue on Age Assurance - Brussels Dialogue on Law and Regulation
Thursday, 11 July 2024
Wifi code: Msevent1457re

Key Takeaways

Key Takeaways
A Multi-Stakeholder Dialogue on Age Assurance - Law and Regulation

Brussels, Thursday 11th July 2024

The Centre for Information Policy Leadership (CIPL) and the WeProtect Global Alliance are continuing their efforts to promote a global dialogue involving multiple stakeholders on age assurance. Following a successful two-day meeting in London in March, CIPL and WeProtect continued their efforts in a second of a series of in-person and virtual events on age assurance held in Brussels on July 11th, 2024.

Following the London event, four discrete working groups were formed to enable a more focused discussion and drive the development of consensus-based principles that can ultimately also inform the wider policy discussion.

This second multi-stakeholder dialogue also served as the inaugural meeting of the law and regulation working group. The discussion was grouped around three main topics:

- **The When:** A risk-based approach to age assurance
- **The What**: Defining state of the art and finding a common baseline among differing age assurance mechanisms
- **The Who:** Roles and responsibilities in age assurance

Attendees represented a diverse range of organisations, including child rights organisations, academia, privacy and safety regulators and experts from a number of jurisdictions, lawmakers, government representatives, civil society, age assurance providers, and a wide range of industry representatives including the technology, adult entertainment, social media, telecommunications and financial sectors. The event was held under the Chatham House Rule.

The insights gathered from this session will feed into follow up meetings of the working group. More information on the working groups and how to take part can be found at the end of this summary.

Below is a high-level summary of some key areas of discussion.

The When: A risk-based approach to age assurance

Risk Assessments - Balancing Privacy and Safety

Navigating risk assessments is undeniably complex and made more complex by the increasing number of laws governing various aspects of children's online experiences. Guidance regarding risk assessments under the GDPR is available, and guidance regarding safety laws such as the Digital Services Act or the Online Safety Act is still emerging.

- Some organisations continue to struggle to construct meaningful risk assessments and effective mitigation measures in this cross- sectoral environment. For instance, risk in the context of processing under the GDPR will differ from risk in the context of content as do the corresponding mitigation measures. New risk terminology such as "systemic" risk is not as well defined yet. Understanding the risk and defining appropriate mitigation measures therefore remains an iterative and continuous process.

- At the same time, organisations must carry out risk assessments carefully and honestly. Frequently risks are flagged to be medium or low risk where in reality they present a high risk profile.

- Where assessing risks it is important to avoid conflating different types of risk (such as the 4 Cs), and to ensure that risk is viewed in contexts including where risk may be created by other children.

- Age verification measures may need to be weighed against the potential benefits of access to content like LGBTQ+ resources, in particular as children move through maturity levels.

- The Best Interest of the Child must be considered when determining what makes a service age appropriate. However, more clarity is needed in terms of what constitutes the Best Interest of the Child. The understanding of what constitutes the Best Interest of the Child may differ across jurisdictions and in different cultural contexts and even from one child to another. It is challenging to explain this concept to product teams but standards such as the UN Convention on the Rights of the Child General Comment 25 (relating to rights in the digital world) provide valuable insights.

- Creating appropriate and practicable risk assessments will require a cross functional approach including C-Suite involvement, legal, content specialists, product teams, privacy and safety experts. This has to translate into internal accountability measures such as appropriate policy and procedures and training to support sufficiently holistic risk assessments and the development of effective risk mitigation measures. Having a multi-disciplinary team that has a consistent dialogue to convene on safety decisions, edge cases and product cases is also important.

- Regulatory cooperation, nationally and ultimately internationally, is key to creating a common understanding and a coherent approach to guidance and enforcement as demonstrated in the UK under the DRCF. Similar developments are emerging in other jurisdictions such as the Netherlands, Ireland and Germany.

- The development of standards, nationally and internationally, can further support a balance of innovation and safety across global platforms while creating a level playing field for assessing risk. However, an agreement has to be reached as to how specific standards should be.

The What: Defining state of the art and finding a common baseline among differing age assurance mechanisms

Defining 'State of the Art' and technical solutions

In Europe the discussion around age assurance often centers around Article 8 of the GDPR, and consent. This has commonly led to platforms and services with child users having terms of service which require users to be 13+. Whether motivated by the GDPR, DSA, OSA, AVMD, or existing age appropriate design codes, any age assurance measure must be proportionate to the context in which it is deployed and must be weighed against the best interest of the child including the right to play and for children to express themselves. Other considerations include whether the solution is sufficiently privacy friendly, secure, and designed in a manner that is easy to understand and use.

- While there is generally agreement that age assurance will not have a one-size fits all solution, determining what could be considered a “state of the art” baseline could provide a level of consistency for regulators and organisations alike.

- The GDPR makes reference to “state of the art” throughout but does not define it in order to remain appropriately tech neutral. Frameworks from other sectors working with the concept of “state of the art” such as ENISA’s three step process for IT security can provide helpful learnings, however: State of the art age assurance measures should be commercially available, consider existing scientific knowledge and generally accepted rules or standards, and must move away from deprecated approaches that are known to be less effective or compromised. As an example, self-declaration at least when used without any supplemental measures, is unlikely to be acceptable as state of the art anymore, where age assurance is mandated. Other approaches such as social vouching are still being evaluated.

- Age assurance technology must take the different age bands of children and teens into consideration and the challenges that this may bring. For example, some technologies while generally commercially available, such as using payment information or digital ID solutions, may not be available for the 13+ age band for instance.

- New methods, such as voice age estimation, are a developing area and have the potential to become ‘state of the art’. This requires room for innovation and a continuous evaluation process by organisations and regulators alike.

- Organisations operating globally face the challenge that not all age assurance measures will be accepted in every jurisdiction; as an example age verification solutions based on biometrics are approached differently across EU member states, or in the US.

- Cultural differences and different national cultural contexts (e.g., varying parenting approaches and different perceptions of harmful content) have an impact on the uptake of age assurance technology. This may require to make allowances for local specificity, but should not lead to drastic divergence across jurisdictions either. Technical solutions must be tested in the real world and testing must involve children and parents in the design.

- Additionally, good practices can be drawn from experience in other sectors with access limitations such as in the insurance or banking sector, alcohol or gambling industry and successful cross-sector collaboration such as between tech platforms and the alcohol industry.

- Privacy remains a major concern for the implementation of effective age assurance mechanisms and finding the right balance between the various trade-offs can be a challenge. Privacy-enhancing technologies (PETs) including AI-based technologies can provide mitigation measures.

The Who: Roles and responsibilities in age assurance

Device, service, platform and parental responsibility

Parents, caregivers, and also children have agency and an important role to play in the context of effective age assurance. Parents can play a key role in protecting their children. In reality families and caregivers are often overwhelmed by the volume of interactions with different individual services and the technical knowledge this involves. To be effective, age assurance measures (and parental control tools) should strive to be user-friendly and easy to understand, including by children.

- Solutions for age assurance involve different actors in the online ecosystem from the telecommunications providers, to the online platforms, device manufacturers, app stores, and individual apps. Proposals to streamline the process for the benefit of users include browsers, app stores or device OS as opportunities to establish age at a central point of contact, which has the advantage of building on some already existing infrastructures. However, such an approach would need to carefully balance a number of challenging issues including privacy, security, competition concerns, costs and liability. Experiences in the US also raised questions around sufficient granularity of such an approach given the exclusionary nature of age assurance. Workable solutions will have to carefully address all these concerns.

- Overall, all efforts should be made to align policy and legislative approaches wherever possible and diverge only when necessary. With principle-based laws and a risk-based approach, there will always be a degree of ambiguity which is to be embraced to remain tech neutral. It relies on organisational accountability and an iterative process of developing appropriate policies and tools to respond to developing risks. It is also an opportunity to align through multi-stakeholder initiatives such as this on some of these issues and inform future approaches.

Recommendations and Next Steps

Proposed Recommendations

1. Develop a framework: Establish an inclusive framework for the when, what and who of age assurance. This should be developed involving multiple stakeholders and follow a principle- and risk-based approach, taking account of key global laws and regulations.

2. Promote collaboration: Encourage ongoing collaboration between organisations, regulators, industry, and international bodies.

3. Enhance guidance: Develop guidance for product and design teams on child privacy, safety and security and associated risk assessments, which could be reinforced by training programmes. A culture of compliance and training should also be built for parents, guardians and children.

4. Innovate safely: Leverage new technologies for effective age assurance while protecting privacy by undergoing a continuous evaluation process and define clear standards.

5. Engage stakeholders: Involve parents, educators, and children in developing and implementing an age assurance framework, with a key focus on child participation.

Next Steps

Working Group Membership

To continue the exchange and work through the complexities of these issues, a series of working groups are being established to further this initiative. The aim of the working groups is to facilitate discussion and progress on each of the below work streams, providing the opportunity to gather further insights from a variety of experts and perspectives.

The three working groups are:

Law and Regulation

Terms of reference - *To consider potential framework(s) for the implementation of age assurance under European relevant laws and regulations, with a view to this knowledge being applicable to other global regions. This will take account of potential challenges (e.g., overlapping laws, conflicting viewpoints and regulator perspectives, different roles of companies in the age assurance ecosystem) and opportunities to advance interoperable age assurance.*

Risk assessments

Terms of reference - *To explore the role of risk assessments in supporting a balanced and rights-based age assurance and the opportunities to develop a more holistic approach to assessing both safety and data protection risks to young people.*

Regional and global perspectives

Terms of reference - *To gather international insights on age assurance, including regional, cultural and socioeconomic factors, and assess lessons learned for a global approach.*

Each working group will meet virtually for 90 minutes on up to two occasions before the end of 2024 and will produce a short summary paper of key discussions and learning. All groups will receive secretariat support from Praesidio Safeguarding, who will coordinate the logistics of meetings, compile minutes and produce a draft summary position paper for each working group, which will be reviewed by working group members. Participation in the working groups is voluntary and not an endorsement of the paper or the wider project.

If you would like to be involved in this work and in shaping the outputs and recommendations for one or more of these groups, please contact Natascha Gerlach (ngerlach@huntonak.com), Iain Drennan (iain@weprotectga.org), Eden Tayyip (etayyip@huntonak.com), and the secretariat support for the working groups (AgeAssurance@praesidiosafeguarding.co.uk).

All expressions of interest should be received by **30th August 2024**

Who We Are

CIPL is a global privacy and data policy think and do tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90+ 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 that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world.

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.

Additional support provided by Microsoft, Snap and TikTok.