Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

WeProtect GLOBAL ALLIANCE

A Multi-Stakeholder Dialogue on Age Assurance

Key Takeaways

Key Takeaways
A Multi-Stakeholder Dialogue on Age Assurance

Day 1 | Tuesday, 26 March 2024 - Day 2 | Wednesday, 27 March 2024

Evidence Based - Child Informed - Risk Based

Digital age assurance is a complex and sensitive issue, requiring a careful balancing of rights and risks. We sought to bring together experts from across a range of sectors to understand the current state of play - challenges and opportunities - and to advance a holistic and principles-based approach. Attendees represented a diverse range of organisations, including child rights, privacy, safety, academia, regulators, civil society and industry representatives from technology, entertainment, telecommunications and financial sectors.

The event was held under the Chatham House Rule. Below is a summary of the key points of discussion, as well as a call for expressions of interest in participation in ongoing working groups.

Age Assurance

- Age assurance is an umbrella term which includes age verification (identity documents, parental consent etc.) and age estimation (age inference, based on behaviour on a platform, social vouching, AI-based facial age estimation).
- It is widely recognised that self-declaration alone is generally inadequate as a means to help higher-risk services identify the user's age (apart from when used in addition to other methodologies).
- It is key to realise that services have very different challenges that manifest at different stages of their users' journey.
- Age assurance should be seen as a process, not a one-off check.
- Getting age assurance right is important. However, it is not a panacea and must not distract from other legal compliance and accountability activities that organisations need to put in place to ensure online safety and privacy in the delivery of their products and services to children.

Striking a Balance between Safety and Privacy

- When implementing age assurance solutions, organisations must consider the appropriate balance between safety and privacy. Age assurance is part of digital safety by design, but solutions must also come from a privacy by design approach.
- Data minimisation, storage limitation, and data security must be balanced against the necessity to process data in line with the perceived risk. It is imperative that those responsible for safety, security and privacy within organisations cooperate to determine the appropriate balance.
- Any approach must be mindful of the difference between privacy and safety and the need to address both privacy and safety interests and rights: there may be one privacy concern versus many safety ones we are trying to solve when we contemplate age assurance solutions.
- Red teaming and starting with a "what could go wrong" approach to designing age assurance solutions is critical.

The Regulatory Landscape

- Legal and regulatory fragmentation remains a major concern for many organisations.
- Broad global landscape of diverging child privacy and safety legislation, including age assurance and verification requirements, is creating challenges for international organisations.
- Regulatory guidance is available and being developed especially by European regulators (including the UK) for both privacy and safety, which should help to establish more legal clarity.
- More institutionalised cooperation between different regulators in Europe (including from different disciplines) and internationally is imperative to reach a level of convergence that ensures consistency in the protection of children online.
- Models such as the Digital Regulation Cooperation Forum in the UK and other nascent fora are extremely important to support a consistent approach, including by supporting the development of joint privacy and safety guidance and shared regulatory expectations.

In turn, regulators expect better assessments of risks and harms from organisations. When it comes to age assurance solutions in particular, companies must be able to demonstrate the effectiveness of age assurance solutions in the context of their service. Organisations must be ready to provide evidence of how solutions mitigate the assessed risk and the efficacy of the measure.

Importance of a Context-and-Risk-Based Approach

- There is no “silver bullet” or proportionate “one size fits all” solution that could be deployed for age assurance that could satisfy all privacy and safety needs. The deployment of age assurance should follow a risk-based approach and solutions must be based on the issue we are trying to solve and the context and the type of services and products offered to children.

- There is no consensus on the risk taxonomy in general when it comes to digital policy and compliance. However, when it comes to assessing risk in the deployment of age assurance solutions, it is important to consider the benefits, in the context of the best interest of the child.

- Any risk assessment must be context specific and consider both the likelihood and severity of a risk of harm.

- High risk lists, which set out instances where a greater risk to children is likely, should be rebuttable and we should consider integrating risk assessments across the various legislations to facilitate operationalising them.

- Age assurance measures must be proportionate to the level of risk on a particular service and not collect more data than is necessary. Furthermore, as services develop and the environment changes over time, risks will change. This means risk assessments must be systematic and repeatable.

- Different stakeholders must work together to create holistic and contextual risk assessment frameworks that incorporate human rights, child rights, data protection and safety that translates into demonstrable measures.

- Adherence to existing and developing codes and standards can lower the overall risk for children on a platform or service and minimise the necessity for age assurance measures.

Technical Challenges and Opportunities

- The question of 'reuse'/'interoperability' is a continuing point of discussion. Sharing signals and information is one approach to age assurance. If users can successfully verify themselves in one digital place can trusted providers hold the verification keys? This exists in other areas (telecoms, ID providers) – can this be extended to age assurance solutions?

- Such an approach may require further guidance also from regulators on data sharing and liability questions.

- Privacy-enhancing technologies, in particular zero knowledge proofs as suggested by the CNIL in France, may play a future role. Regulators should incentivise development and adoption of PETs.

- There is space for age assurance providers, but also a space for more development by platforms. Stakeholders should develop a roadmap for technological advances (AI for age assurance).

- There has to be an understanding, especially from privacy regulators, that the more granular and specific the age verification, the more (personal) information may have to be processed (children often lack ID for instance).

- There is further need to reconcile a layered approach to age assurance with the views expressed by some parents, children, and young people that there are "too many hoops to jump through" and experiences across different apps to verify age.

User Experience and Education

- Age assurance and parental control tools must be accessible to children, young people and parents. Bringing them along the privacy, security and online safety journey, and ensuring user-centred and participatory co-design is part of accountable and responsible technology behaviour.

- While the responsibility lies with the organisations, there is a role for parents – and children and youth in peer-to-peer support – and we need to build their capacity and understanding. Making available controls, assurance and guidance in a single place via tools which parents and children already access and are familiar with, would help with this.

- All children and parents' perspectives or means are not the same however and the challenge lies in differing attitudes to parental controls and age assurance that can vary across age, culture and socio-economic status.
- There is a need to continuously ensure that product developers are up to date on child rights frameworks, legal requirements and child friendly design. Diverse teams that include children can ensure that teachable moments (such as when somebody gets rejected by age assurance) come with the right message to further the understanding of why certain measures are in place.
- Part of the approach to online safety must also be to incentivise children and young people to remain on the age appropriate pages.
- Schools often lack resources to provide the necessary media literacy education (focused on stranger danger).

Ethical and Other Considerations

- Age assurance must be equitable, privacy and security minded.
- Ethics require organisations to consider "should we do this?", as well as "what if we don't do this". A benefit to many may override a risk to few.
- Rights-based language and frameworks form the cornerstone of age assurance principles.
- The process of standard-making needs to be much more inclusive – large portions of the world remain undocumented, and barriers to inclusion for CSOs remain very high in some countries as an example.
- How do we adapt approaches for those who have different needs based on socio-economic status, disability, familial structure and many other markers of difference?
- Suggestions to rethink the 'magic number 13' and whether other age bands relate to developmental needs for children and teens.
- We should consider who we mean when we refer to "the child" – the term reflects different realities in different jurisdictions.

Action Points and Next Steps

As a next step, we plan to set up a number of smaller dedicated working groups on the following topics:

- **Law and regulation**: to consider relevant legal and regulatory frameworks in the international context, including suggestions for where greater legal clarity is needed, potential challenges (e.g., overlap, conflicting proposals, different roles of companies in the age assurance ecosystem), and opportunities to advance interoperable age assurance.

- **Risk assessments**: 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 and consider both risks and benefits.

- **Regional and global perspectives**: to gather international insights on age assurance, including regional, cultural and socioeconomic factors that may require variations, and assess lessons learned for a global approach.

- **Future mapping**: to explore and map emerging activities relating to age assurance, including the development of standards, technology and partnerships.

These four groups will meet virtually and will seek to gather insights from a variety of experts. They will produce a short paper (or other relevant output) setting out their discussions and learnings, drawing on the foundations of the March roundtable in London.

If you are interested in joining one of these working groups, please contact Natascha Gerlach (NGerlach@huntonak.com) and Eden Tayyip (ETayyip@huntonak.com) or Iain Drennan (Iain@weprotectga.org) by **Friday, May 31, 2024**.