CIPL Children's Data Privacy Project

Age Assurance and Age Verification Tools: Takeaways from CIPL Roundtable

On February 16, 2023, CIPL hosted a virtual roundtable with representatives from CIPL member companies, data protection authorities, civil society and experts to discuss the role of age assurance tools, their effectiveness, appropriateness, and their role in providing a safe online environment for minors.

The event was a part of the CIPL's Children's Data Privacy Project, which was launched in 2022 and was the first in a series of "deep dive" roundtables to be held in 2023. Each roundtable will explore existing best practices and emerging options that address the key compliance issues and challenges identified in CIPL's policy paper "*Protecting Children's Data Privacy, International Issues and Compliance Challenges*," published in October 2022. Future roundtables will address the risk-based approach to the protection of children online, transparency, consent and other legal grounds for processing, as well as personalisation.

The purpose of the age assurance roundtable was to gather perspectives from participants on the methodologies and emerging best practices when confirming whether a user is a minor, so they are appropriately shielded from harmful or inappropriate content, and can thrive in a digital eco-system with age-appropriate content.

Legal Background

Global policy, legislative, and regulatory initiatives to protect children online increasingly require or expect providers of digital services to verify, or at least assess the age of their users.

Data protection legislation often imposes strict requirements regarding the processing of children's data (e.g., US COPPA, EU or UK GDPR). Related regulatory frameworks may sometimes specify additional safeguards (e.g., UK Age Appropriate Design Code, Irish Fundamentals, California Age-Appropriate Design Code Act).

Newer regulatory initiatives are requiring digital services to adopt measures that protect children from content, services, and products inappropriate for their age, and ensure access to safe and appropriate online experiences (e.g., EU Digital Services Act, EU Audiovisual Media Services Directive, EU CSAM Regulation proposal, UK Online Safety Bill, EU strategy for a better internet for kids (BIK+)).

Key Takeaways from the Roundtable Discussions.

1. **The methodology of age assurance and the timing of deployment depend on the nature of the service and its level and likelihood of risk to children.**

Different types of online services and platforms present different levels of risk (and benefits) to children and youths. Platforms range from adult-only to purposefully child-centric. The actual services on a platforms vary considerably. Some may allow public or private interactions and messaging. Others restrict or layer access to various functionalities. The features and designs specific to a particular service and the level potential risks to children, including the likelihood and severity of such risks, will

determine whether age assurance is required, which methodology is most appropriate, and how and when it should be deployed.

Most importantly, the chosen methodology should take the best interests of the child into consideration. Age assurance and privacy compliance must lead to the protection of children and minors in the digital environment, not from it.

2. There is no silver bullet. No methodology is better than another, but one could be more appropriate and effective for the specific use case.

Several age assurance methodologies are currently available to organizations (e.g., self-declaration models, AI-powered age-estimation approaches, biometrics-based tools, third-party provider services), and many others are in development (e.g., through standards). Each methodology presents different levels of accuracy, and each has unique strengths and weaknesses. Some are more privacy protective and others require collection of more information for the specific age verification or assurance purpose. There is no one-size-fits-all.

The utility and suitability of different age verification or assurance methodologies depend on the risk context of the underlying service(s), or how and on what type of device the service is likely accessed. Also, services providing layered functionalities might require layered age assurance (i.e., age assurance requested at different access points) and/or the use of multiple methodologies at different stages.

Choosing a specific methodology requires an assessment of the risks and benefits of different methods and their: proportionality: is the impact of using a given methodology proportionate to the level of harm that is being addressed or avoided by the use of given methodology. Choosing an age verification tool where age estimation would suffice might require disproportionate collection of personal data. Identifying the most appropriate method means balancing its effectiveness with privacy protections.

Regulatory expectations must also take into account the practical technical feasibility of different methods and their impact on user-experience (e.g. how seamlessly a method can be integrated in the user journey, whether it would require more than once devise).

3. Organizations need guidance on adequate age assurance criteria and risk taxonomy to perform proper risk assessments.

Existing regulatory guidelines, such as the ICO Age Appropriate Design Code, the Irish Fundamentals for a Child-Oriented Approach to Data Processing, the California Age-Appropriate Design Code Act, and the CNIL's 8 recommendations to enhance the protection of children online are helpful to organisations, as well as the regulatory engagement and readiness to provide further tools and guidance.

However, different national norms and cultural contexts create diverging and occasionally conflicting requirements, exacerbating compliance issues for organizations operating globally. For example, the use of biometric for age assurance may create risks of non-compliance with national or state laws in some jurisdictions, but may be embraced in others. Equally, carrying out appropriate risk-assessments is still a challenging endeavour for companies, with many testing and working with purpose on

developing best practices and methodologies for age verification and assurance. At the same time, regulators are keen to understand and see the industry response and progress.

research has been conducted into creating a spectrum of activities and typical environment that may create harms for children. However, there is no complete convergence, nor consensus on the granularity of "risky" services, specific use cases and taxonomy of risks or harms, nor on how to conduct acceptable risk assessments . Appropriate risk assessments must focus on the risk to the child or minor and must go beyond data protection and take the best interest of the child into consideration, including empowering children in their online experiences.

Regulators equally stress the need for organisations to conduct and document a full and comprehensive Data Protection Impact Assessments (DPIAs) when processing children's personal data and to be able to share such an assessment with regulators on request. Such DPIAs must contain a risk assessment of risks of harms to children and teens, as opposed to only risks and harms to organisations. Finally, DPIAs must document how organisations performed any balancing of different rights, risks, including any trade-offs.

There are still unanswered questions, such as how to operationalise those concepts through a repeatable and systematic process, or how to account for the changing developmental stages of children and teens when designing products and services and developing risk frameworks.

There is a real need for regulatory convergence and co-ordination. Initiatives such as the UK Digital Regulatory Enforcement Forum, the collaboration between the UK ICO and Ofcom on the children's safety and data protection and Global Online Safety Regulators Network have been mentioned as good examples of fora that enable coordinated and cross-regulatory discussions.

4. To be effective, design and deployment of, age assurance tool should continuously research and consider children's behaviour and motivation.

Research shows that children may lie about their age to access online services. This behaviour can be attributable to a number of factors, e.g., confusing information from service providers regarding access, confusing guidance from parents, and simplistic age declaration queries, or just simple curiosity and determination to experiment and take part in online world. Even though children and teens have a good understanding of online harms, they tend to be highly motivated not to be excluded, restricted, or relegated to a lesser version of the service they are seeking to access and in more charge of their choices.

Understanding children's motivation and drawing from parallel age assurance scenarios in the analogue world can support better design, transparency and trust and ultimately lead to a more successful and appropriate approach to age assurance.

5. Age assurance is only one of the tools available to keep children safe online; it cannot be used in isolation.

Organizations cannot rely on age assurance alone. Keeping children safe online and protecting their data protection and other rights will require a combination of measures to ensure compliance with various data protection and other legal requirements and regulatory guidance, such as privacy and safety by design and default, appropriate user-centric transparency, content moderation and

personalisation of content, parental consent for certain ages and family specific controls, and age-appropriate services (or child friendly spaces within services).

The more organisations comply with the granular requirements and standards of the UK Age Appropriate Design Code, or Irish Fundamentals, or California Code or France's CNIL guidance, the less often they will be required to resort to age verification and assurance as the ultimate protective measure from data protection point law of view.

6. Constructive engagement and sharing of information is essential for development of bottom up standards and certifications for age verification and assurance

Many organizations, especially the larger ones, have made serious investments and commitments to develop best practices for age verification and assurance. They are testing available age assurance methods and exploring new solutions, for instance through participatory design testing. As research and with it our understanding evolves, it is imperative that all stakeholders (industry, policymakers, regulators, civil society) continue engaging and sharing in ongoing dialogue regarding expectations and progress.

There will likely be a need for further developments of standards and certifications, that are accepted throughout multiple jurisdictions and by multiple organisations. These can only be developed in a collaborative way, with the participation of all stakeholders. This will be necessary to ensure a more ready and systematic adoption of appropriate tools and techniques, and ultimately ensure greater protection for children and youths online.