A Multi-Stakeholder Dialogue on Age Assurance

Working Group on Law and Regulation

KEY TAKEAWAYS

Working Group Meetings

Virtual 10 October and 25 November 2024

Key Takeaways
A Multi Stakeholder Dialogue on Age Assurance

Working Group on Law and Regulation

Virtual Meetings 10 October and 25 November 2024

The Centre for Information Policy Leadership (CIPL) and the WeProtect Global Alliance are leading an ongoing multi-stakeholder dialogue on age assurance. As part of this initiative, the Law and Regulation Working Group held two online meetings to consider the opportunities and potential challenges for age assurance created by the emerging legal landscape (with a focus on the European and UK contexts), and to contribute to a shared understanding of legal and regulatory requirements.

Attendees represented a diverse range of organisations, including child rights, privacy, safety, academia, regulators, and civil society.

The discussion took place around a fictional case study to invite input from different stakeholders with different perspectives.

The case study sought to prompt discussion of the following topics:

1. The When: Risk-based approach to age assurance
2. The What: Age assurance and complementary measures
3. The Who: Roles and responsibilities in age assurance

Below are the key points from the discussion corresponding to the three topics listed above. Each section provides the relevant part of the case study (in blue text) for context.

Part 1: The When - Risk-Based Approach to Age Assurance

Case Study

Peter is an 11-year-old student who enjoys spending time with his friends. He is a confident, fun-loving kid and there is always a positive atmosphere in his group. Recently Peter got a new phone which makes him feel more connected to his friends, as they have joined the same 10 educational, social media, gaming and communication services.

All of the online services that Peter uses allow users to share and access public user-generated content. At first, his feeds on these services are filled with clips about the games he plays or silly jokes that made him laugh.

One day, however, a more interesting video popped up on one of these services. Out of curiosity, Peter clicks on it expecting it to be fun.

To his surprise, the video contains violent content. Peter watches it in full, and makes him feel uncomfortable.

All of the online services that Peter uses are likely to be subject to a number of risk assessment and mitigation obligations. For example, in the EU and the UK:

- Services that are 'very large online platforms' – Arts 34-35, DSA
- Services that are 'online platforms' – high level of privacy, safety, and security - Art 28, DSA
- Services that are 'data controllers' need to have a lawful basis for processing personal data and potentially a DPIA - with many using an AADC assessment where minors are involved – Art 6, Art 35, GDPR
- User to user service – Section 3, UK OSA
- Services that are 'data controllers' need to have a lawful basis for processing personal data and potentially a DPIA – UK GDPR
- Services may also need to follow the ICO Children's Code

Discussion Questions:

1. How should online services assess the risk of public user-generated content?
2. What mitigations should they put in place?

Key Takeaways from Part 1

- Age assurance should not be used solely to exclude children from inappropriate content but can also be employed to provide age-appropriate experiences that deliver tailored content. Knowing a child's age or age bracket can help ensure that children receive suitable content, supporting both children's online engagement and safer online experiences.

- Platforms face challenges in defining harmful content for children, given social, cultural, and developmental differences. There is limited guidance on age-specific harm assessments, which may lead to inconsistent evaluations across platforms. Assessing risks based on guidance from established legal frameworks, such as the "5Cs" – i.e., Content, Contact, Conduct, Contract, Context – can ensure a structured, uniform, and comprehensive evaluation.

- The use of recommender systems can raise data processing risks, especially when applied to children. Data protection authorities are increasingly focused on recommender systems especially where the recommendations are based on processing children's data. However, implementing mitigations measures, including age assurance, can reduce risks to the rights of children. In addition, recommender systems themselves can also serve as a mitigation measure for risks to children, by promoting age-appropriate content.

- Content moderation efforts via filtering, blocking and flagging can reduce the risk of exposure to inappropriate content will not always be 100% effective (as per the example in the case).

- Platforms and apps should reevaluate the types of content allowed in their terms of service. For example, where violent content is permitted, the platform may need to raise the minimum age for access and continue to improve content moderation measures to flag or filter such content for certain user groups. However, this is an iterative process that requires continued adjustment.

- Some platforms may not use age assurance because they assessed themselves as posing minimal risk to children in terms of privacy and safety. Regulators would not likely expect the use of age assurance measures for services that present minimal risk, but platform operators should nevertheless engage with regulators to ensure a common understanding of risk levels.

To conduct an appropriate risk assessment, it is important to understand a number of factors: the risk profile of a service, whether underaged users are likely to see harmful content, the type of harm, and the features of the service. Regulators such as the UK's Office of Communications (Ofcom) and Information Commissioner's Office (ICO) have issued consultations and published guidance on how platforms can determine whether a service is likely to be accessed by children. These platforms will then need to assess the risks they pose and take action to protect against such risks commensurate with the risk level. The ICO's Children's Code outlines 15 standards that online services must implement if their platforms are likely to be accessed by children. These standards are designed to guide digital services in their efforts to ensure that children's personal data is properly protected and that services meet specific safeguards for privacy and security.

Part 2: The What - Age Assurance and Complementary Measures

Case Study

One service Peter accesses has extensive mitigation measures to prevent young people from accessing violent content, for example:

Platform Design

- Service does not open to a UGC feed
- UGC on the service is only accessible for a limited duration
- Service displays warnings when accessing public UGC for the first time

Content Rules

- Service has clear guidelines and explainers to help users understand the rules
- Service has additional rules for public UGC requiring it to be suitable for 13+
- Public UGC cannot include violent content

Content Moderation and Enforcement

- Service has multiple layers of automated and human moderation
- All content is subject to automated review processes before dissemination to the public via recommendation systems
- All content is subject to human review before being widely recommended to the public via such systems
- All content is easy to report and the service responds promptly to reports

Monitoring

- The service sample tests the public content on its service - which shows very low prevalence of violent content
- The service monitors for underage accounts and promptly closes accounts reasonably suspected to be used by under 13s

One service has some mitigations in place but not all.

One other service has no mitigations but prohibits under 18 accounts from accessing public content. The other seven services have no mitigations at all.

Discussion Questions

1. Is age assurance necessary for:

- The platform with extensive mitigations to prevent young people from accessing violent content?
- The platform that has some mitigations but not all?
- The platform that prohibits under 18 accounts from accessing public UGC content?
- The other platforms with no mitigations?

2. If age assurance is required, then what kind of age assurance is appropriate for the platforms in each category (low-risk, medium-risk, high-risk)?

- Declared age?
- Highly effective age assurance?
- Multiple methods to maximise accessibility?
- Path for those who cannot successfully pass age assurance to avoid impact on user rights?
- Parental oversight/control?

3. Does this differ in the EU vs UK?

4. How might this differ for adult content?

5. Does the kind of risk (content, conduct, data processing) shift the dial for what is required?

Key Takeaways from Part 2

- A key challenge for online services is determining the appropriate risk threshold for the implementation of age assurance measures. Few platforms are risk-free and even highly effective mitigation measures are unlikely to be 100% effective. This raises questions about acceptable risk levels – e.g., would one inappropriate video per 100 be an acceptable risk level, or should a stricter threshold apply (one per 1000)?

- Risk assessments should include an evaluation of the appropriateness and utility of mitigation measures, keeping in mind that certain mitigations may address safety issues but may not address other concerns, such as the lawfulness of data processing.

- From a data protection perspective, age assurance measures that process personal data must be lawful, fair, and effective to meet GDPR standards. Services employing such measures must therefore take into account the type of data they are processing and whether the processing itself could be considered high-risk. If high-risk processing is identified, the GDPR may require a Data Protection Impact Assessment to evaluate mitigations in place and ensure the protection of personal data in compliance with the Regulation (n.b. Recital 75 GDPR regarding DPIAs for children's data).

- Recommender systems can serve as a risk-minimising measure by tailoring content appropriately. These systems can help strike a balance between offering personalised experiences and maintaining safety.

- The use of age assurance measures for services that do not require users to sign-in requires further exploration and development. Allowing access without sign-in can protect user privacy, provide streamlined access, and accommodate those with technical limitations. However, the absence of a sign-in process can also introduce risks. It makes age verification and personalisation potentially more challenging with an increased risk of underage users accessing age-inappropriate content. It also makes it more difficult to track and hold individuals accountable for their actions on the platform. Parental controls to manage what children are accessing online may equally be linked to specific accounts.

Part 3: The Who - Roles and Responsibilities in Age Assurance

Case Study

Age assurance could be implemented at different levels for Peter:

- The operating system account Peter uses to access his device
- The app store account that Peter uses to download apps
- The 7 online services that have no mitigations for registration
- The 1 online service to support its 18+ age gate

The age assurance tool used by some services only says “yes - over 18” or “no - under 18”. As a result, these services must regularly check or reverify users' ages to ensure that their information remains accurate and up-to-date. Other services are using more robust age assurance tools and collect age data once, but the process is more complex and, in one case, Peter hit an error and has not been able to finalise the process.

Feeling frustrated, Peter:

- Minimises the services he accesses
- Finds a service on the dark web that does not use any age assurance (and also has no mitigations)

How would these solutions operate under existing European legal frameworks?

EU	UK
DSA - provider	OSA & codes - provider
GDPR/guidelines - data controller	UK GDPR/AADC - data controller
AVMSD - provider	AVMS Regulations - provider
DMA - gatekeeper	DMCCA - SMS firms

Discussion Questions

1. Who has primary responsibility under the different legal regimes under discussion? Are there any conflicts?

- Can we separate responsibility for age assurance and for complementary/ alternative measures?
- What data processing considerations arise?
- What are the opportunities for interoperability in this scenario?
- How do current regulatory regimes treat interoperability versus service-level responsibility?
- What duties are owed to users? By which party? Does this change depending on the method for age assurance?

2. What are the pros and cons of distributed approaches vs investigating a centralised, interoperable solution? And what is possible under the current regulatory framework?

- What are the options to make distributed approaches interoperable?
- Does a centralised approach shift the burden of responsibility?
- What are the liability considerations for each approach? Where would additional regulatory guidance be useful?
- What happens with shared or sold devices?
- What effect does digital identity have on Peter's issues?
- Could a centralised approach work in a legislative environment where different services already need different age assurance?
- How can we assess proportionality/reasonableness of the options? (e.g., cost)

Key Takeaways from Part 3

- The online ecosystem is complex, with users interacting from a variety of entry points, devices, and services.
- Many services are interconnected, potentially adding to the complexity of responsibilities among device providers, operating systems, app stores, and content providers.
- Clarity on the allocation of liability under different legal regimes is essential to ensure a shared understanding among stakeholders, a clear recognition of implementation challenges, and the effective development of policy choices leading to practical solutions.
- Collaboration among the different industry players in the online ecosystem is necessary for the development of pragmatic solutions. It should not be a binary choice between a centralised system or a distributed system. Industry should explore ways of sharing and/or distributing intelligence (such as age signals) and developing due diligence measures to ensure the holistic protection of young users where possible.
- Developing age assurance solutions can be particularly burdensome to SMEs.
- Challenges and workarounds to potential solutions—such as the increased usage of virtual private networks (VPN) to bypass location-specific measures — need to be taken into account when trying to develop effective age assurance measures.

Who We Are

The Centre for Information Policy Leadership (CIPL) is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for 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 www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. 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.