The ICO's response to the Call for Evidence and roundtables on age assurance

Introduction

The ICO launched a call for evidence (CfE) in November 2021 to understand existing and proposed approaches to age assurance in the context of the Children's code.

In addition, between November 2021 and January 2022, six roundtables were held to explore this area in further detail. Both the CfE and roundtables gave the ICO invaluable insight into the perceptions and views of participants and we are grateful to those who took the time to respond to the CfE and attend the roundtables.

The views expressed were wide-ranging and sometimes conflicting, and were based on the capability or perception of age assurance at the time of the responses. The ICO recognises that the technology is developing rapidly, and that some of the concerns expressed may no longer be current.

The CfE and roundtables included responses or representatives from the following sectors:

- academia;
- age assurance technology providers;
- civil society;
- information society services (ISS);
- regulators;
- Children's commissioners;
- trade bodies and industry associations.

In total 52 organisations took part in the roundtables and 22 responses to the call for evidence were submitted. Overall, responses demonstrated that age assurance is in a nascent stage, and whilst solutions are developing rapidly, there is still uncertainty among stakeholders about what the ideal age assurance solutions are. Age assurance was seen as part of a package of measures to keep children safe but should not be seen as a 'silver bullet' to online safety. There was general agreement that reliance on one method would not be adequate, and a range of methods should be available to ensure inclusivity and accessibility.

A variety of issues were raised and whilst it is not possible to cover every point in detail, some key themes emerged which are summarised below. Please note this **section summarises the views of respondents to the CfE, and roundtables attendees. It is not a reflection of the ICO's views.**

Scope of the consultation

We called for evidence on existing or proposed age estimation approaches, novel approaches to age assurance, systems where data protection by design has been applied and the type of economic impact of age assurance approaches. This has enabled us to keep up with technological developments and deepen our understanding of how industry is responding to the Children's code and the requirement for age assurance.

The consultation did not seek evidence on uses of age assurance that are outside the context of the Children's code, or that could not be adapted to support the aims of the code.

Terminology

Throughout the report, the following terms are used:

- **Age assurance** is a collective term used to describe the range of techniques used to provide age estimation, age verification or age assessment.
- **Age verification** refers to the outcome of a binary question with only two options, which accesses information (such as passports or driving licences) to gain a level of confidence in the truthfulness of a binary outcome.
- **Age estimation**, on the other hand, refers to the outcome of a continuous assessment, where there is an estimation of age often based on algorithms. This does not result in a binary outcome but in a range of outcomes within parameters, such as someone is likely to be 21-25. An example may be the use of facial analysis.

Research undertaken by the Age Check Certification Scheme (ACCS) on behalf of the ICO provides more detail on these terms, which builds on the ICO's work outlined in the Commissioner's Opinion on the use of age assurance.

Development of technology

There were varying attitudes towards the maturity of emerging techniques. In general, concerns were raised that age estimation techniques are not yet mature, and are reliant on data processing activities that some find intrusive.

There was general agreement that more research and testing is necessary, particularly to improve the performance of Artificial Intelligence (AI) and biometrics techniques, to ensure their accuracy, to

promote fairness and non-bias, and to allow them to be used successfully at scale.

Conversely, others stated that age estimation methods were already technically feasible and operationally effective.

Some of these techniques are covered in more detail below.

Self-declaration

A user states their age or date of birth but does not have to provide any evidence to confirm it. There are a range of design options for presenting self-declaration. For example this can take the form of a tick box asking users to confirm they are over a certain age, a wheel where they select the year they were born, or a drop-down list where they choose their date of birth.

Stakeholder response: Respondents recognised that this measure was the most common age assurance practice. Some felt that there may be a place for self-declaration with strengthened safeguards, however many viewed this method as ineffective, easily circumvented and therefore not effective in protecting children from online harms. Some respondents felt that a neutral age gate balances protecting children's privacy and making the internet accessible. Following the call for evidence, the ICO undertook a joint research with Ofcom in summer 2022 which considered the attitudes of children and parents to age assurance measures, including self-declaration.

Hard identifier

The provision of an official document, such as a passport or driving licence, to verify an individual's identity and to demonstrate their age.

Stakeholder response: Hard identifiers were viewed as only appropriate in high-risk scenarios, and not where there is the potential to impact fundamental rights or expose users to disproportionate data requests. Age verification was seen to provide assurances about an individual's age compared to age estimation. However, it was noted that hard identifiers are not currently created for the digital world and risk excluding children who are unable to provide official documentation.

Account holder confirmation

An adult who is an existing account holder for a service provides consent for a child to access a service, confirming the age of the child, or confirming their position in a range of ages. This is usually done by the

adult with parental responsibility for a child and may be part of the parental consent process.

Stakeholder response: Requirements under Article 8 of UK GDPR, which allows for someone with parental responsibility to consent to a child's data being processed were highlighted. Concerns were raised that these provisions are not widely known. The gap in technology's ability to confirm the relationship between child and parent / guardian was highlighted and taking a risk-based approach confirming this relationship was suggested. It was also recognised that privacy intrusions may also arise from parents if there is an over-reliance on parental controls.

Circumventing age assurance controls was not always viewed as negative as parents may want authority over what their children access online. However, parental controls should not remove from online services the responsibility to safeguard children.

Biometrics

The use of facial, voice or other biometric information to estimate the age of a user; or the use of a variety of different biometric data (finger prints, iris, voice) to verify the age or identity of a user.

Stakeholder response: Biometric-based age estimation such as facial estimation was seen to pose challenges due to the unpredictable nature of aging. There were concerns that this technology is prone to errors and attacks. Furthermore, it was noted that the use of this technology may contribute to the normalisation of children to biometric processing, which may extend to other areas of life.

Behavioural profiling

The use of AI to estimate the age of a user through the personal data trail they create. This can take place by analysing a users' browsing history, their interaction with others, which accounts they choose to follow and so on.

Stakeholder response: Whilst there was recognition that profiling may be done in the best interests of the child, this technique was seen as intrusive. As the profiling would only occur after an initial period of use, there is potential for harms to materialise for children on a service before an age determination could be made through profiling their engagement, and protections put in place. In addition, for behavioural profiling to be effective and uphold children's data privacy, it has to be applied to everyone, including adults, in a safe environment for children. This makes

it more difficult to identify adults based on their behaviour in a restricted, secure environment.[1]

Issues around training data were raised a number of times, including its availability, which was highlighted as a barrier. There were concerns around testing using homogenous groups, and the risk of discrimination or bias when using AI and biometrics. This could potentially have a negative impact on marginalised groups.

Potential algorithmic biases of age estimation tools were seen as a risk. Respondents wanted to see risk mitigations in place, alongside an evolving set of standards, which develops at the same time as the technology.

On-device solutions

Providers of commonly used technologies, such as Google Android, Apple iOS, or Microsoft Windows, would allow users to verify their age on device. This verification could be undertaken by a variety of means, for instance providing a hard identifier such as a passport. The device would then provide an electronic token to apps demonstrating the users' age when an app is downloaded and operated.

Stakeholder response: The role of Apple and Google app stores was seen as key to developing a workable solution which avoids the repetition of data entry. A holistic, whole eco-system approach was seen to be beneficial, and would require closer industry collaboration and investment in solutions. However, this solution was also viewed as difficult to monitor when devices are shared.

Data protection considerations

There was concern from stakeholders that the requirement for age assurance runs counter to the data minimisation principle, as more personal data will be collected from individuals. The Commissioner's Opinion on the use of age assurance recognises that age assurance may require processing of personal data beyond that involved in the delivery of a core service. However, the Commissioner considers that, provided this processing is in line with the purpose limitation principle, ie it is adequate, relevant and limited to what is necessary, the use of age assurance is, in

[1] Whilst this can be said for every method of age assurance, it is a particular concern for behavioural profiling because of how this technique works. Behavioural profiling may not be an effective age assurance method to use where it is deployed in different environments offered by an ISS, as it may be limited in its ability to correctly categorise individuals according to their inferred ages based on the safeguards which might be in place.

many cases, likely to be an appropriate way of reducing the risk of harm to children online.

Some key data protection concerns which surfaced are discussed below.

Transparency

Whether children understand age assurance processes and ensuring parents understand what data is being collected about their children was seen as fundamental.

Purpose limitation

Concerns were raised about the potential for data collected for the purposes of age assurance to be used for other purposes, such as profiling for targeted advertising. This was of particular concern if biometric data had been collected.

Data minimisation

The importance of not creating and retaining new databases of personal data for age assurance purposes were highlighted. Public misconceptions around age estimation retaining personal data were raised as a key area that needs to be addressed in order to ensure trust and confidence in these technologies. There were substantial concerns about the ability to ensure data minimisation when age assurance may require collecting additional personal data. Furthermore, it was recognised that more data will be collected from everyone, not just children.

Data minimisation measures such as hashing and tokenisation were welcomed.[2] Digital Identity was seen as an effective way to assess age whilst ensuring that data minimisation is adhered to. These decentralised measures were also viewed as having the potential to reduce security risks.

Accuracy

There was scepticism around using mean average error (MAE) rates alone to measure rates of accuracy. Respondents noted that inaccuracies particularly impact women and people of colour. The age range 13-18 was

[2] Hashing is a technique that generates a fixed length value summarising a file or message contents. For example, if a common identifier is hashed by both parties, then the hashes will only match if the data is an exact match for both parties. Tokenisation replaces data such as a bank account number or date or birth with a random data string generated by an algorithm. The token contains the value of the data being protected without it being disclosed.

seen as being especially challenging to estimate due to the need to be very accurate to meet legal requirements, such as the age of digital consent under UK data protection law. A standardised approach to measuring overall level of assurance was suggested. However, it was also acknowledged that machine learning (ML) outperforms age assessments undertaken by humans. The need for redress when age estimation measures fail was seen as a necessary feature. Some organisations felt that some errors that lead to denying access to those who meet age requirements is the trade-off for ensuring that children are safe, when it is possible for errors to be corrected.

Accountability

Children's Rights Impact Assessments (CRIA) were suggested as an effective way to identify and recommend mitigations for any risks or impacts to children, particularly in relation to bias, discrimination and exclusion. A CRIA could include or support a data protection impact assessment (DPIA) by holistically assessing the use of age assurance on children's rights, including if they are unable to use the method provided by an ISS. Accountability was noted as particularly critical for the use of algorithms or automated technologies, not only to instil trust and confidence in how these are used, but to ensure these are fit for purpose and perform as they should. Stakeholders highlighted that certification schemes and international standards were another potential option to ensure accountability.

Children's rights

Stakeholders recognised that children are not a homogenous group and there are different considerations about how to protect them. Late teenagers were seen as young adults, and some felt there is a discord with requiring parental consent for this age group. Some children may lack resources to verify their ages (for example through hard identifiers) and this was seen to have the potential for marginalisation. Risks that organisations may exclude access where they cannot verify someone's age were highlighted which may have a 'chilling effect'.

Some stakeholders felt that there are risks to children by not giving them opportunities to learn through online experiences. A certain level of risk was seen to be necessary so children can learn.

Economic considerations

The importance of industry and government alignment on approaches to age assurance were noted. The euCONSENT project was seen as having the potential to fundamentally impact the economics of the age verification market.

Cost was viewed as likely to be determined by the age assurance method employed, with the market setting prices that could become more competitive as technology matures. Some respondents noted that it was unlikely that medium or large organisations would be priced out of conducting age assurance, although this implicitly suggests that smaller companies may be impacted by the cost of buying in age assurance services.

Respondents highlighted the economic and societal costs of not having age appropriate application of ISS and the harm that can result, such as children seeing data-enabled inappropriate content, being nudged to provide further personal data than they want to, and being at risk of online child abuse in environments without age appropriate protections[3]. However, fears were raised that developing age assurance measures may not be cyber secure and this may impact overall cost, for example from developing robust codes and having to use additional security mechanisms.

The additional friction which some age assurance measures may create were seen to be problematic and may reduce the number of users on a platform who may turn to competitors. This was a particular concern if there is no market or industry standard for age assurance that applies to all companies. Furthermore, there were fears that adults may be more susceptible to fraud if they become more willing to provide hard identifiers.

Recommendations from the Call for Evidence and roundtables

The CfE and roundtables have highlighted some priority areas for the ICO's further policy work in relation to age assurance:

- **Recommendation one:** International cooperation and alignment around age assurance, which could include endorsement of standards and the use of codes.

  The ICO's response: The ICO is engaging with stakeholders internationally to ensure that as the discussion around age assurance develops, we share learning and encourage alignment of standards. Examples of this work include: a network of data protection authorities (DPAs) where we share information and progress on age assurance in our jurisdictions. The ICO is also involved in the development of the ISO standards and the IEEE standards.

[3] The ICO has developed a taxonomy of harms that provides further detail on the types of harm that can occur in relation to processing personal data: Overview of Data Protection Harms and the ICO Taxonomy

- **Recommendation two:** Domestic regulatory coordination, particularly for digital identity solutions.

The ICO's response: The ICO is in close contact with Ofcom as the Online Safety Bill continues its passage through Parliament. We will be working closely with Ofcom to ensure that where there are areas of common interest, such as in age assurance, there is regulatory alignment to reduce confusion and compliance burdens for organisations. Our joint statement with Ofcom sets out how we will work together. We continue to engage in conversations with the Department for Digital, Culture, Media & Sport (DCMS) and the Government Digital Service (GDS) on the UK Government's plans for Digital Identity.

- **Recommendation three:** ICO endorsement of certification schemes and frameworks in the UK.

The ICO's response: The ICO has approved two sets of data protection criteria for ACCS's Age Check Certification Scheme and Age Appropriate Design Certification Scheme. One of these sets specific data protection requirements for organisations operating or using age assurance products, and the other applies to the data processing operations of ISS subject to the Children's code. The ICO encourages organisations to consider obtaining certification under these schemes as a way of demonstrating compliance with UK GDPR and the Children's code (if applicable). This is in line with our ICO25 strategic plan for the next few years. The ICO remains open to industry bodies which would like to discuss the development of codes of conduct or certification schemes for their sector or processing activity. The codes and certification team are contactable via: certification@ico.org.uk and codesofconduct@ico.org.uk

- **Recommendation four:** Wide engagement with third party technology developers to understand emerging technologies as well as with ISS.

The ICO's response: The ICO continues to be in contact with a wide range of ISS which are developing or deploying age assurance technologies. We also engage with the Age Verification Providers' Association (AVPA) and are keen to continue engagement with ISS which are using novel and innovative ways to age assure their users. We welcome contact from organisations which would like to initiate a conversation with us. The team can be contacted at ageassurance@ico.org.uk

- **Recommendation five:** To consider data driven harms to children, including the impact of AI.

The ICO's response: The ICO has undertaken an initial analysis of age assurance technologies against our harms taxonomy. The ICO is also in the initial stages of considering the privacy intrusiveness of age assurance methods and the potential harms this may cause to children. Additionally, the ICO's Technology team is undertaking more work on the use of AI procurement more broadly, including how transparency information is provided by vendors to buyers of services, which include age assurance.

- **Recommendation six:** Provide a steer on appropriate efficacy rates.

The ICO's response: The ICO commissioned research into ways of measuring the efficacy of age assurance measures which is the first step towards providing industry with suggestions for appropriate standards. The ICO plans to test these standards through further research.

- **Recommendation seven:** Engage directly with children on their views and experiences around age assurance.

The ICO's response: The ICO commissioned joint research with Ofcom in summer 2022 which considered the attitudes of children and parents to age assurance measures. This provided useful insight in terms of how families assessed risks and how they balance the trade-offs between privacy, ease of use, and other factors. The ICO will continue to review whether there is scope to undertake further research in this area, to ensure that the voices of children are reflected in our policy development.

- **Recommendation eight:** Develop and promote simplified guidance and communications materials, and raise awareness of the Children's code.

The ICO's response: The ICO has a number of resources on the Children's code hub for industry as well as for schools. We will continue to improve on the products we provide, to ensure they are easy-to-follow for organisations, as well as to assist in improving children's awareness of their rights. As our policy position on age assurance develops, we will consider what other outputs will assist organisations with conformance with the code, as well as the wider data protection legislation.