Age assurance and age appropriate design: what is required?

Concerns for children's online safety recently focused on the new evidence of the possible negative effects of Instagram on teen mental health reigniting long-standing questions of how best to protect children from accessing harmful content. Age assurance is a much-debated topic in relation to children's online safety, often cited as a plausible solution to creating an age-appropriate online environment. But what exactly is age assurance and when should it be implemented by online platforms? For www.parenting.digital, Professor Simone van der Hof discusses the legal requirements for age assurance and the suitability of different verification methods. Based on her recent research as part of the euConsent project, she argues that many of the methods currently used are either inefficient, privacy-invasive or raise issues for children rights.

Legal requirements for age assurance

Age assurance is an umbrella term referring to methods for ensuring the age of users of online platforms with varying degrees of certainty. The more specific concept of age verification includes proof that someone is over a certain age. Although there is no general obligation to verify the age of users, European Union and national laws do contain specific obligations to distinguish between adults and children in certain cases, given the specific vulnerability of children in view of their age and development. These obligations may also apply to digital services offered by online platforms.

A mapping of laws in the EU and the UK by the euConsent project found that there are age verification obligations for the provision of some content, goods and services applying both offline and online. Leaving national differences aside, age verification is required for certain forms of harmful content (mostly 18+ content that includes extreme violence and porn), gambling services (with ages ranging from 16-21 years), and the sale of alcohol and tobacco. Moreover, data protection law in the EU and the UK has a higher level of protection for children (i.e. persons under 18) which may make it necessary to establish whether a person using the digital service is over 18 years of age. Although data protection law does not explicitly mention this obligation of age verification, it is generally assumed to exist implicitly because otherwise, it is not possible to take into account a higher level of protection of children's personal data. An exception exists when the digital service by default takes into account the higher protection of children.

The suitability of different age assurance methods

There are various methods of age assurance and their suitability depends on the applicable laws and regulations and the specific context. The legislation in which an age verification obligation is laid down may impose additional requirements on the methods although mostly the method is left open. Or other additional requirements are imposed in order to protect vulnerable groups, including children. In gambling, for example, the law may require that customers are registered centrally.

In this context, it is also important not to see age verification as the silver bullet for online child safety but rather as one of the methods of protection. This is recognised, for example, in the Audio Visual Media Services Directive which lists it as one of the appropriate methods for video platforms, among other methods such as age rating and parental control. And indeed some countries have age classification systems for harmful content that is not 18+.

This also takes into account the fact that not all children are the same and what is unpleasant for some to see at a certain age is appreciated by others. This approach also offers parents the opportunity to make their own decisions, preferably in consultation with their children. In that respect, evidence shows that age ratings are seen as advisory rather than mandatory by parents. Of course, age classification must also be implemented in a meaningful way on video platforms.

Date originally posted: 2021-11-17

Permalink: https://blogs.lse.ac.uk/parenting4digitalfuture/2021/11/17/age-assurance/

Blog homepage: https://blogs.lse.ac.uk/parenting4digitalfuture/

Another form of age assurance that is receiving a lot of attention is age estimation. This involves estimating the age of users based on artificial intelligence. Age estimation has margins of error and is, therefore, not a suitable method for complying with legal obligations on age verification. This is because there is a good chance that children will gain access to harmful content or services that are adult only when the system makes an incorrect estimation. Conversely, adults may be denied access unjustifiably. In the latter case, the system may point to the possibility of identifying oneself with a traditional ID, such as a passport or driving licence, but this defeats the purpose of implementing age estimation. Therefore, it would be better to implement age verification directly, also from the point of view of liability.

Implications for data protection

Age verification does not always have to involve the processing of personal data and some methods are more privacy-preserving than others. For example, there are methods where the verification process takes place entirely on the user's device. This has a number of major advantages. Legal requirements, in particular data protection law, may be imposed in cases of processing personal data. When personal data is not processed, these legal requirements will not apply to the online platform or the AV provider when the verification process is outsourced to a third party. Another advantage is the avoidance of creating a central database of identity information that is vulnerable to external attacks or other data breaches.

However, we also see new methods emerge that may raise privacy and trust issues such as the already mentioned age estimation which is based on AI and potentially also biometric data. This can lead to "Catch 22" situations when the processing of biometrics for age verification is only lawful if the user has given explicit consent but age verification must first take place to determine whether that user has even reached the age of digital consent.

Moreover, data-driven or special category (i.e. sensitive) personal data-based methods do not necessarily comply with the fundamental principles of data minimisation and privacy by design. This is acknowledged by ICO, although they do see possibilities for privacy-friendly facial scans or hand geometry systems. But whether we should embrace these methods goes beyond privacy and includes the question of whether the age-appropriateness of content and services should be determined by online platforms themselves based on often inscrutable algorithms. Parents would like discretion to determine what is age-appropriate for their children, including the ability to override restrictions. This may not be possible when users are automatically profiled for age appropriateness.

Another issue under data protection law is that the method chosen must provide a sufficient level of assurance given the degree of risk involved (risk-based approach). When personal data of children are processed, it can be assumed that there is a high risk. However, we now see that digital services almost exclusively use self-declaration to verify age. This is a method that can be easily circumvented and, therefore, provides an insufficient level of assurance. The result may be that personal data is not processed lawfully.

Age verification and child rights

The rights of children based on the UN Convention on the Rights of the Child (1989) impose specific requirements on verification methods. Age assurance methods that can, and sometimes must, contribute to the well-being of children online must themselves be age appropriate by design. In addition to being privacy-friendly, verification methods must also be child friendly – their functionality and data processing must be understandable to children. In a recent study, we noticed, for example, that some digital services automatically determined whether we met the minimum age of digital consent of the country from which we signed up, which implies that location data is being processed but this information was not transparent.

It is important that age verification methods are effective and proportionate and respect all children's rights, not just protection rights but also children's civil and political rights. Therefore, it is strongly advised to perform a Child Rights Impact Assessment to determine how verification methods may impact children, to assess how to implement legal requirements with the best interests of children in mind, to address any concerns, including privacy concerns, and to implement age-appropriate safeguards. Such an impact assessment is not a one-off exercise because the use of verification methods in practice may require adjustments.

Date originally posted: 2021-11-17

Permalink: https://blogs.lse.ac.uk/parenting4digitalfuture/2021/11/17/age-assurance/

Blog homepage: https://blogs.lse.ac.uk/parenting4digitalfuture/

It is essential to involve children and parents when designing and developing age verification methods because they are best placed to indicate their experiences, expectations and concerns. Children's experiences also vary significantly based on their circumstances and specific stage of development (evolving capacities). What is accessible and understandable for some children or parents may not be accessible to others. Design and development must, therefore, ensure that methods are suitable to all children and parents concerned.

This also means that verification methods should be context-sensitive and inclusive so that children are not excluded when they cannot use them for any practical reasons (e.g. due to physical or cognitive barriers). Age assurance should also be unbiased and non-discriminatory bearing in mind that some, often vulnerable and marginalized, groups of children might not have access to verification methods or might be discriminated against by automated outcome systems. Children must also be offered accessible instruments enabling them to make complaints when their interests or rights are not observed or to get support in using verification methods in ways that are age-appropriate.

Future developments

This brings us finally to the question of what methods of age assurance exist that meet all the above requirements. The answer is short: to my knowledge, none. There are examples of existing or under-development decentralised solutions that are privacy-preserving but we do not yet know whether they meet the requirements from a child rights perspective. Self-declaration methods are used most often but in many cases they are unfit for purpose. Other methods that are used are mostly "traditional" and developed for offline identification, such as credit cards or ID documents. Not everyone owns such identification, hence such methods are not inclusive. In addition, identification is unnecessary if you only need to know whether someone is over 18 years of age and in that case these documents disclose more personal data than necessary. Given the affordances of digital technologies, including the potential for surveillance, it is of great importance that new methods are developed that take children's rights and privacy seriously.

Find out more

Age-appropriate design and the role of age verification, a presentation by Prof Simone van der Hof at the Safer Internet Forum 2021

Date originally posted: 2021-11-17

Permalink: https://blogs.lse.ac.uk/parenting4digitalfuture/2021/11/17/age-assurance/

Blog homepage: https://blogs.lse.ac.uk/parenting4digitalfuture/

Methods for Obtaining Parental Consent and Maintaining Children Rights, A presentation by Prof Simone van der Hof at the euCONSENT conference on Online Child Rights, Age Verification and Parental Consent: finding the balance

Date originally posted: 2021-11-17

Permalink: https://blogs.lse.ac.uk/parenting4digitalfuture/2021/11/17/age-assurance/

Blog homepage: https://blogs.lse.ac.uk/parenting4digitalfuture/

Date originally posted: 2021-11-17

Permalink: https://blogs.lse.ac.uk/parenting4digitalfuture/2021/11/17/age-assurance/

Blog homepage: https://blogs.lse.ac.uk/parenting4digitalfuture/