

# The role of age verification technology in tackling child sexual exploitation and abuse online

NOVEMBER 2022

This intelligence briefing acts as a situational analysis of current approaches to and technological tools on age assurance, age verification and age estimation. It was compiled by Yoti, working in partnership with WeProtect Global Alliance.

## Executive summary

Just as we protect children offline - they can't freely walk into a nightclub or buy a bottle of wine - the same protections need to be implemented online.

Whilst there are many positive opportunities available; with increasing numbers of children accessing explicit content, chatting to strangers or being coerced into sharing images of themselves, action is desperately needed to safeguard children from the ever-growing dangers online.

This briefing explores the role age assurance can play in safeguarding children, the current regulatory landscape around age and different methods of age assurance.



Co-funded by  
the European Union

## Table of contents

Methods of age assurance, age verification, and age estimation .....	2
Why does age verification / assurance matter to child online safety? .....	5
What is the current landscape in terms of law, policy and implementation? .....	7
Tokenised approaches to age assurance .....	10
How does it fit within a child's rights framework? .....	11
What are the opportunities and challenges? .....	11
Future scanning .....	13
Recommendations .....	14
Further reading .....	14
Case study .....	15
Appendix .....	16

## Methods of age assurance, age verification, and age estimation

### In simple terms

Age assurance is the umbrella term for all types of age checking.

Age verification is typically referred to as methods linked to 'hard identifiers' such as presentation of an ID document, or in some instances checks to databases, or ownership of a credit card.

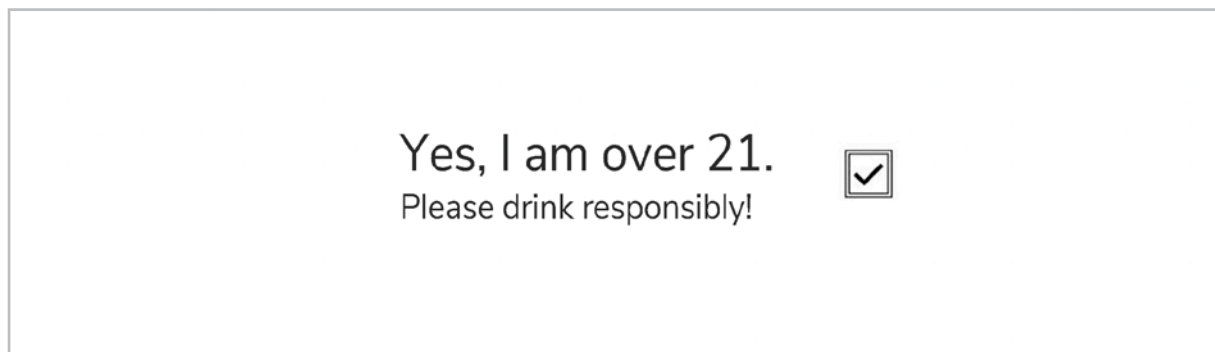
Age estimation is typically referring to methods, where no document is presented.

### How has age assurance evolved?

The first approach was traditionally self-assertion – just asking someone to insert their age or tick a box to confirm their age.

Given this is easily falsified and open to abuse, more effective and robust age verification is needed for almost all sectors.

The exception could be certain edtech settings; for instance a child self-selecting maths problems according to their age level.



## Ways to check age

<p><b>ID documents</b></p> <p>Age obtained from an ID document, which can also be matched to a photo or video of the individual.</p>	<p><b>Facial age estimation</b></p> <p>Age determined by AI that analyses the facial features in an image.</p>	<p><b>Database check</b></p> <p>Name, date of birth and address verified with a credit reference agency provider.</p>	<p><b>Mobile phone number</b></p> <p>Details are matched against records held by a mobile services provider.</p>
<p><b>Credit card</b></p> <p>Details are verified with a payments provider to confirm the user holds a credit card and is 18+.</p>	<p><b>Identity app</b></p> <p>A verified age attribute shared from a digital identity app, which is anchored to an ID document and a selfie.</p>	<p><b>Email verification</b></p> <p>A verified email is matched against a database and online activity that indicates the holder is 18+, such as a job post.</p>	<p><b>Social media proofing</b></p> <p>Age estimated by examining social media activity, eg account opening date, group memberships, contents of posts, friends</p>
<p><b>Open banking</b></p>		<p><b>Other biometrics</b></p>	

## Age verification, based on ID documents

We know that people can often prove their age in person, by showing a document. However in today's world this is not foolproof; it is very easy to buy fake documents online. There are also fake and stolen documents available on the dark web. Unless an organisation has sophisticated tools and their staff are trained in document verification at border control level, it is hard to accurately check the validity of a counterfeit document presented in person and to be sure that the owner is the person presenting the document.

Hence, the industry has developed sophisticated techniques for identity document validation. If you pass through an airport, you will often be asked to scan your passport at a physical terminal. Your live face is compared to the image on the document and in the background, checks are made that your name is not on sanctions lists.

A similar process to this can be undertaken online to assess either identity or age. A person is asked to upload their identity document. It is possible for the document to be reviewed and assessed for authenticity. A 'liveness' check can be undertaken to check that it is a live person presenting the document, rather than a video or photo attack. The face presented can be matched to the document.

Given this is laborious to undertake this multiple times, there are now digital identity apps, such as the Yoti app, whereby a person can go through this document upload and verification process once and then re-use their app to either prove their full identity or just their age.

Many internet users may have gone through an in person or online identity check to set up a mobile phone account or a credit card. Sometimes now these historic identity checks are referred back to as proof that someone is over 18.

In certain countries, there are also databases for electoral roll, credit reference databases or Open Banking protocols which may have good coverage. In some instances these are also used to assess age; however coverage can be patchy.

Many of the methods outlined above rely on the fact that someone owns a government issued identity document, or 'photo ID', with strong security features to prove your age in the first place or repeatedly prove your age. This might be effective for people who are lucky enough to own and have access to their document. However there are over 1 billion people on the planet who do not have photo ID. There are also people who may not have access to their document for a range of reasons. Hence, there is increasing focus on methods that do not rely on identity documents. These are often termed age estimation. It would however be simplistic to assume that they always offer a lower level of check.

There is clearly a black market for stolen and fake identity documents. There are more than over 99 million known lost and stolen identity documents registered with Interpol<sup>1</sup>. Evidence shows that we know that some young people will 'borrow' documents from their parents and we know that unless there are robust checks on who is using a document it may not be the rightful owner. Facts such as date of birth from electoral rolls can be shared digitally; and in some instances may be deemed too low a proof. Many parents set up mobile phone accounts for children so certain regulators may not accept these historic checks or may require additional checks to be undertaken to check that the user of a mobile phone or credit card is actually an adult.

<sup>1</sup> - <https://www.interpol.int/en/How-we-work/Databases/SLTD-database-travel-and-identity-documents>

## Age estimation approaches

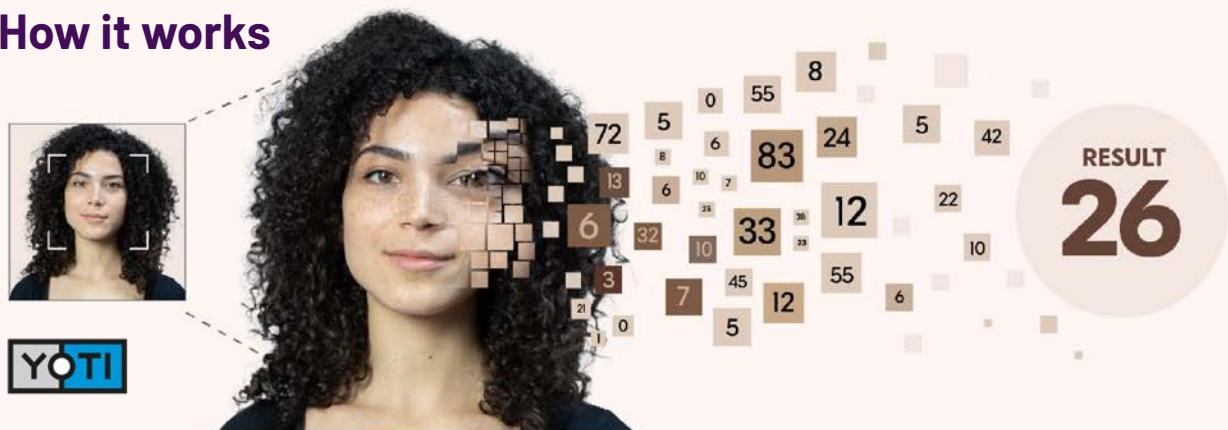
One of the most popular age approaches on the market, with consumers and platforms, is AI-based facial age estimation, which uses a selfie to estimate age. This method is being used globally at scale by a wide range of social, gaming, ecommerce, adult, gaming and retail organisations.

The AI is trained with lots of faces with a month and year of birth from all over the world - so when it sees a new face, it does a pixel level analysis and issues an estimated age. It uses facial detection (checking if this is a human face) and then facial analysis to analyse the

face presented. To the technology, the image is simply a pattern of pixels, and the pixels are numbers. So, it does not recognise anyone, as it has not been trained with any named photos. It learns 'this pattern is what 16-year olds usually look like', and 'this pattern is what 60-year olds look like'.

This makes it a 'privacy-friendly' approach as it doesn't require any personal details or ID documents. All images are instantly deleted once someone receives their estimated age - nothing is ever viewed by a human.

## How it works



### Detect face

A face is detected in an image and reduced to pixels. Each pixel is assigned a number that the AI can understand.

### Compute numbers

The numbers are computed by a neural network that has been trained to recognise age by looking at millions of images of faces.

### Determine age

The AI finds a pattern in the numbers and produces an age.

*Instant process - scalable to tens of millions a day - no images are stored*



## Other age estimation approaches

In addition, your online activity can be assessed - the sites a person visits, the amount of time someone has owned an account, the style and register of written language. All of these may give platforms behavioural indicators which they may use to give an estimate of your age.

## Fair competition

All of these approaches are available from independent third parties. Some global sites may also attempt to

build in-house approaches and operate with a blend of in-house and external approaches. The competition regulators, in the same way they have reviewed whether global platforms should control currencies such as the Libra cryptocurrency<sup>2</sup>, now have to reflect on the appropriateness and desirability of global platforms developing global age and or identity solutions.

<sup>2</sup> - <https://corporatefinanceinstitute.com/resources/cryptocurrency/libra-cryptocurrency/>

## Why does age verification / assurance matter to child online safety?

There are many vectors of abuse towards children online. One approach to improving the landscape of sites and the experience of children is to flip the narrative and consider which sites are likely to be accessed by children and require sites to be designed from the ground up to be suitable for people using them. This will not be an overnight change to the landscape; however if we make the comparison to the automotive industry it will start to change behaviours. The first automotive came into production in 1886. Seat belts were made mandatory in 1968 in the US. Child car seats became mandatory in 1985, and speed cameras emerged in 1987.

Age Appropriate Design Codes have been described as the equivalent of the arrival of the seat belt. In terms of parallels - the regular testing of automobiles and speed cameras in the road are the next stages where regulators will review the overall impact of the entirety of safety measures put in place and develop technology regtech solutions to aid in their work.

### Key statistics:

- A third of children aged between 8 and 17 with a social media profile have an adult user age.<sup>3</sup>
- 83% of parents agreed that age-verification controls should be in place for online pornography<sup>4</sup>.
- Many children - some as young as 7 years old - stumble upon adult pornography online, with 61% of 11-13-year olds describing their viewing as mostly unintentional<sup>4</sup>.
- In Italy, a survey found that 67% of boys aged 14-19 and 15% of girls have watched pornographic material. In Sweden, 92% of boys and 57% of girls of 15-18 years have watched pornography<sup>5</sup>.

<sup>3</sup> - <https://www.ofcom.org.uk/news-centre/2022/a-third-of-children-have-false-social-media-age-of-18>

<sup>4</sup> - [BBFC, 'Young People, Pornography and Age Verification' in 2020](#)

<sup>5</sup> - [https://www.wya.net/op-ed/exposure-of-children-to-pornography/#\\_ftn1](https://www.wya.net/op-ed/exposure-of-children-to-pornography/#_ftn1)

- In Finland, a survey with over 10,000 respondents revealed how young children are being exposed to porn and CSAM. A key finding revealed that 70% said they first saw child sexual abuse material when they were under 18. Of those, 40% said they were under 13 when first exposed to illegal images of children.
- Nearly a quarter of children surveyed in the UK (22%) said underage viewing of pornography negatively affected mental health and wellbeing, while 12% said it normalised abusive or exploitative behaviour<sup>6</sup>.
- A cross-sectional school-based survey<sup>7</sup> of 10,930 adolescents (5,211 males / 5,719 females), aged 14-17 years old was carried out in six European countries (Greece, Spain, Poland, Romania, the Netherlands, and Iceland). Anonymous self-completed questionnaires covered exposure to pornography, internet use and dysfunctional internet behaviour. They also measured psychopathological syndromes (measured by Achenbach's Youth Self-Report). The prevalence of any online exposure to pornography was 59% overall and 24% for exposure at least once a week. The likelihood of online exposure to pornography was greater in male adolescents, heavier internet users, and those who displayed dysfunctional internet behaviour.
- Last year, the Internet Watch Foundation (IWF) annual report reported an increase in the number of 'self-generated' sexual images of children, most likely due to lockdown as many people spent more time at home and were socially restricted<sup>8</sup>. These images were predominantly of 11-13-year-old girls, in their bedrooms or another room in a home setting. In 2021/2022, Childline delivered 234 counselling sessions in which young people spoke about the removal of online sexual images. This was a 19% increase compared to the previous year.

<sup>6</sup> - [Barnardos, 2021](#)

<sup>7</sup> - <https://www.mdpi.com/2227-9067/8/10/925>

<sup>8</sup> - [Internet Watch Foundation Annual Report](#)

Once you know the age of a child; it is then possible to meet the requirements of the Children's Codes or Age Appropriate Design Code and attempt to provide an age-appropriate and safe internet experience for children and young people.

For this reason, age importance is a fundamental building block. California has recently passed the Age Appropriate Design Code Act, which will come into force in 2024, in the wake of the Age Appropriate Design Code in the

UK, Ireland's "The Fundamentals for a Child-Oriented Approach to Data Processing"<sup>9</sup>, the Netherlands' "Code voor Kinderrechten"<sup>10</sup>, the EU's Better Internet for Kids Strategy<sup>11</sup> and Australia's e safety roadmap.<sup>12</sup>

9 - <https://www.dataprotection.ie/en/dpc-guidance/fundamentals-child-oriented-approach-data-processing>

10 - <https://codevoorkinderrechten.nl/>

11 - <https://digital-strategy.ec.europa.eu/en/policies/better-internet-kids>

12 - <https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification>



## With facial age estimation, once you know you're dealing with a child, you can...



Set geolocation to off but give the child the ability to turn it on if needed



Provide age-appropriate content



Be certain the online community is within the same age threshold



Supply easy-to-use tools so they can exercise their data rights



Turn off excessive notifications



Minimise the data you collect - don't store it



Shield their data. It shouldn't be used for things not in their interest



Use child-friendly language to explain platforms



Always be sure to treat a child like a child



## What is the current landscape in terms of law, policy and implementation?

The regulatory landscape in the field of age verification is fast evolving, with legislation requiring the use of age verification to protect users and audiences going through national and regional legislatures in all four corners of the world.

The gambling sector was the first to require identity verification checks, ahead of consumers placing bets, in many jurisdictions. Many countries have restricted the sales of goods such as alcohol and tobacco to children.

In certain parts of the world – such as the UK<sup>13</sup>, Estonia<sup>14</sup> and Australia<sup>15</sup>, there is now discussion as to how digital approaches to age verification can be used in retail contexts.

13 – <https://www.gov.uk/government/publications/age-verification-technology-in-alcohol-sales-regulatory-sandbox#:~:text=The%20Home%20office%20and%20office,alcohol%20under%20the%20Licensing%20Act>

14 – <https://www.strongpoint.com/news/the-first-automated-in-store-tobacco-sales-already-live-in-europe/>

15 – <https://code.retaildrinks.org.au/thecode/code-of-conduct>

## Which sectors require age checks?



Advertising



Video sharing site



Adult websites



Social media, Metaverse



Dating sites



Hospitality, live events



E-commerce alcohol, vaping



Nightclubs, bars



Gaming



Gambling

Sandboxes (an isolated testing environment) have been created by some regulators. The UK Information Commissioner’s Office, (ICO), invited technology approaches into the ICO Sandbox<sup>16</sup> to develop and extend mechanics such as facial age estimation to support the Age Appropriate Design Code<sup>17</sup>. The UK Home Office has

16 – <https://ico-newsroom.prgloo.com/news/ico-supports-projects-to-strengthen-childrens-privacy-rights>

17 – [https://ico.org.uk/media/for-organisations/documents/4020427/yoti-sandbox-exit\\_report\\_20220522.pdf](https://ico.org.uk/media/for-organisations/documents/4020427/yoti-sandbox-exit_report_20220522.pdf)

supported live pilots with major retailers to review in person digital age verification approaches<sup>18</sup>.

The main shift in thinking in recent years has been the evolution from blocking people under a certain age from doing certain things; to considering what is age appropriate at different ages.

18 – <https://www.gov.uk/government/publications/age-verification-technology-in-alcohol-sales-regulatory-sandbox>

As outlined above, there are now Children's Codes and Online Safety Bills evolving in the UK<sup>19</sup>, Netherlands<sup>20</sup>, Ireland<sup>21</sup>, Australia<sup>22</sup>, the EU and most recently California<sup>23</sup>. These regulators are considering what in terms of content, contact and conduct should be designed from the get go to be age appropriate by platforms. Once age has been assessed, it becomes possible to act in the best interests of that child or adult. In practical terms that could be to turn off notifications late at night, not allow geolocation tracking, turn off age inappropriate advertising or profiling. In terms of contact, it is then possible to disallow children from being contacted by over 18s - who may groom or coerce them into sharing explicit images of themselves. In terms of content moderation, that can also be adapted to be age appropriate, for instance not allowing profanities.

In addition there are over a dozen countries around the world which have bills in discussion, specifically reviewing the access to adult content - Germany, France, Ireland, Italy, South Africa, Canada, Australia, New Zealand, Poland, the Philippines, the state of Utah and the UK. Recently, the ICO clarified that adult-only services are in scope of the Children's Code if they are 'likely to be accessed' by children.\* (See links in Appendix.)

In Europe, GDPR established the concept that processing children's data required special care. There are a number of pieces of legislation where age assurance and age appropriateness are referred to - from the Audio Visual Media Services Directive (AVMSD), the Digital Services Act, and the Digital Markets Act. This is also specifically mentioned in the Better Internet for Kids Strategy. The EU also funded the EU Consent Project<sup>24</sup> which led to a pan European pilot of interoperable age verification and parental consent approaches.

In the US, 'COPPA', the federal Child Online Privacy Protection Act<sup>25</sup> which came into force back in 2000 implies that websites directed at children or who learn a user is under 13 should check age before their data can be processed legally. The Kids Online Safety Act<sup>26</sup> is under review by Congress alongside the Children and Teens Privacy Protection Act (COPPA 2.0)<sup>27</sup> and the PROTECT Act<sup>28</sup>.

There is increasing focus and awareness of what can "harm the physical, mental or moral development" of a child, and also stopping the algorithmic targeting of children. Several high-profile court cases have shone a spotlight on current practises; such as the Molly Russell Case and Coroner's Report,<sup>29</sup>

The following matters were raised during the Inquest:

1. There was no separation between adult and child parts of the platforms or separate platforms for children and adults.
2. There was no age verification when signing up to the on-line platform.
3. That the content was not controlled so as to be age specific.
4. That algorithms were used to provide content together with adverts.
5. That the parent, guardian or carer did not have access to the material being viewed or any control over that material.
6. That the child's account was not capable of being separately linked to the parent, guardian or carer's account for monitoring.

*'I recommend that consideration is given by the Government to reviewing the provision of internet platforms to children, with reference to harmful on-line content, separate platforms for adults and children, verification of age before joining the platform, provision of age specific content, the use of algorithms to provide content, the use of advertising and parental guardian or carer control including access to material viewed by a child, and retention of material viewed by a child.'*

19 - <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/>

20 - <https://codevoorkinderrechten.nl>

21 - <https://www.dataprotection.ie/en/dpc-guidance/fundamentals-child-oriented-approach-data-processing>

22 - <https://www.legislation.gov.au/Details/C2021A00076>

23 - [https://leginfo.ca.gov/faces/billTextClient.xhtml?bill\\_id=202120220AB2273](https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273)

24 - <https://euconsent.eu>

25 - <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>

26 - [https://www.blumenthal.senate.gov/imo/media/doc/kids\\_online\\_safety\\_act\\_-\\_one\\_pager.pdf](https://www.blumenthal.senate.gov/imo/media/doc/kids_online_safety_act_-_one_pager.pdf)

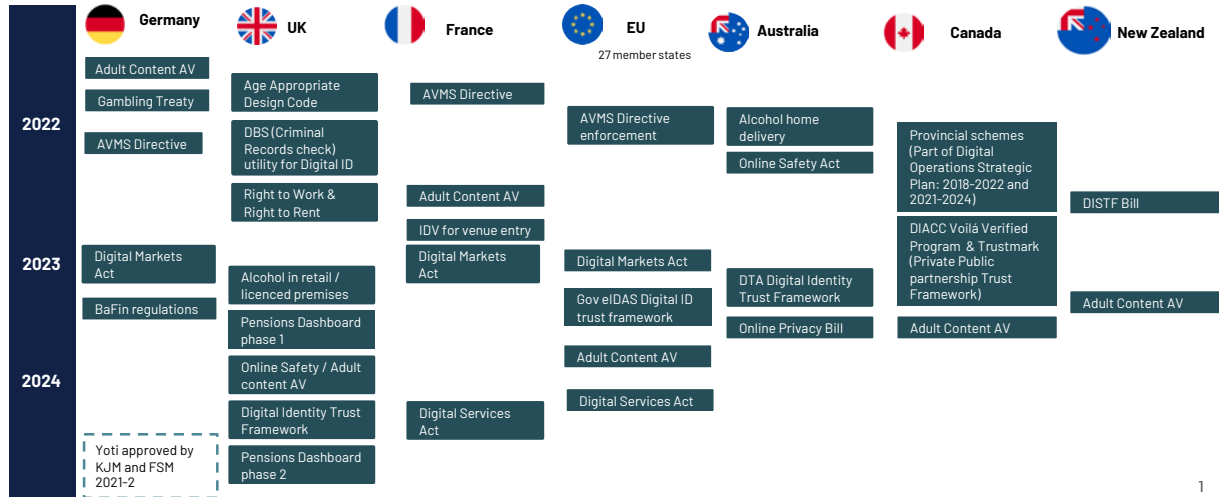
27 - <https://www.markey.senate.gov/news/press-releases/senator-markey-celebrates-successful-passage-of-children-and-teens-privacy-legislation-through-senate-commerce-committee>

28 - <https://www.lee.senate.gov/2022/9/lee-bill-protects-victims-of-image-based-sexual-abuse>

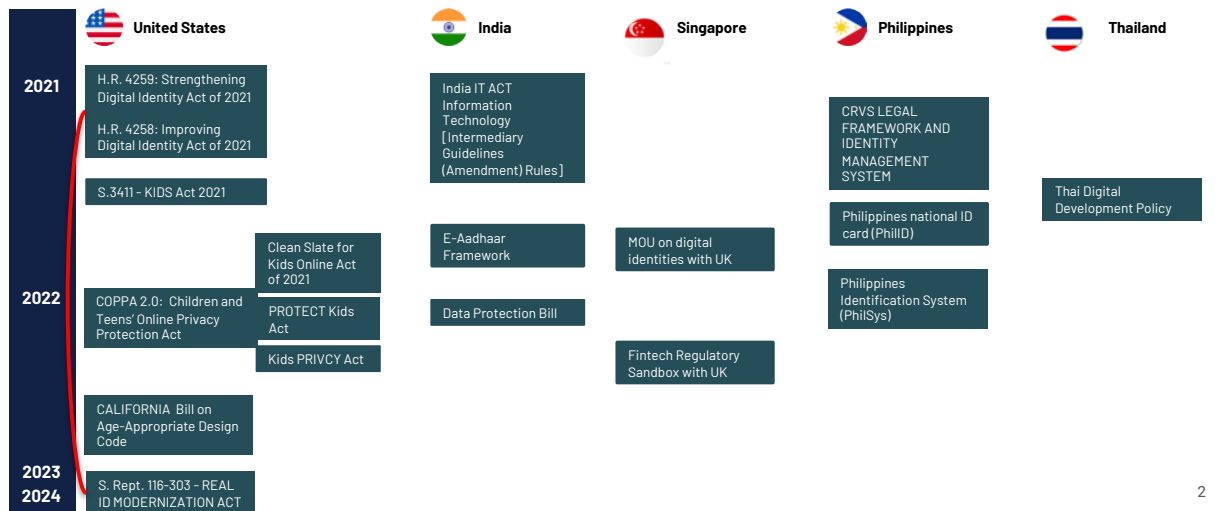
29 - [https://www.judiciary.uk/wp-content/uploads/2022/10/Molly-Russell-Prevention-of-future-deaths-report-2022-0315\\_Published.pdf](https://www.judiciary.uk/wp-content/uploads/2022/10/Molly-Russell-Prevention-of-future-deaths-report-2022-0315_Published.pdf)



## Age and Identity Verification Regulations across countries



1



2

## Tokenised approaches to age assurance

Building on the success of the EU Consent project<sup>30</sup> there are now interoperable, tokenised age verification approaches. This can further reduce friction for consumers and reduce the cost of compliance.

<sup>30</sup> - <https://euconsent.eu/>

### Make verification last longer with reusable age tokens





Age tokens are digital proof that someone has proved their age to a relying party.


They allow users to access other integrated websites without proving their age again.

Tokens don't contain any identifiable information, just the result (eg: 18+ or 21+) and information on how the check was performed.


### What's inside an age token?


**Time:** the time the check was performed. 


**Liveness:** the type of liveness check performed. 


**Visitor ID:** an identifier that can group multiple tokens to a device session. 



**Type:** the type of age recorded. 

**Age:** the result of the original age check. 

**Method:** age verification method used. 

**Issuer:** the issuer of the age token. 

Age tokens don't contain any personally identifiable information

## How does it fit within a child's rights framework?

There are a number of child's rights to be respected. The ICO gives examples and information on how age assurance impacts children's rights under the United Nations Convention on the Rights of the Child (UNCRC):

- [Article 2: Non-discrimination](#)
- [Article 12: Respect for the views of the child](#)
- [Article 16: Protection of privacy](#)
- [Article 31: Access to leisure, play and culture](#)
- [Article 33: Protection from drug abuse](#)
- [Article 34: Protection from sexual exploitation](#)
- [Children's code recommendations on age assurance](#)

## What are the opportunities and challenges?

### Opportunities

There is now a relatively mature market for age verification with many providers and a respected trade body, the Age Verification Providers Association (AVPA)<sup>31</sup>, which outlines clearly online which organisations provide which range of ten types of age verification services<sup>32</sup>. The German age regulator, KJM,<sup>33</sup> has been operating in age verification for over a decade. It lists over 90 approaches which have been approved for the German market.

There are many instances across multiple sectors of the successful implementation of age verification at scale. There has been a successful pan-European interoperability pilot run under the EU Consent project with a robust governance function comprising leading child rights and privacy expert academics, European data protection regulators, global platforms and child safety experts.

The EU Consent Project has led to the development of now rapidly evolving international age standards<sup>34</sup>, which are due to conclude in the coming 12-18 months. (IEEE 2089.1, Best Practice for Age Verification, ISO PWI 7732 – Age Assurance Systems Standard). These build on the already existing publicly available specification for age assurance.<sup>35</sup>

31 - <https://avpassociation.com>

32 - <https://avpassociation.com/find-an-av-provider/>

33 - <https://www.kjm-online.de/aufsicht/technischer-jugendmedienschutz/unzulaessige-angebote/altersverifikationssysteme>

34 - <https://avpassociation.com/standards-for-age-verification/>

35 - Online age checking. Provision and use of online age check services. Code of Practice PAS 1296:2018 <https://knowledge.bsigroup.com/products/online-age-checking-provision-and-use-of-online-age-check-services-code-of-practice/standard>

The changing regulatory landscape means more businesses are considering how best to implement robust age verification. Clearly, this has to be balanced with privacy and data protection rights. In meeting the regulatory requirements, the process of assessing age may entail a degree of friction.

Thankfully, there are age verification technology approaches, such as facial age estimation and the use of digital age verification and digital identity apps, which allow individuals to just prove their age online, or the fact that they are over an age threshold (such as over 13 or over 18), without sharing any other personal details - which meet the current publicly available specification for age checking (PAS 1296:2018).

Going forward there is clearly scope for more regulators to build on the solid foundations of age standards and implement similar, consistent Age Appropriate Design Codes. It is promising that the timeline for implementation is now set, following passing of legislation by the California legislature<sup>36</sup>; the home of many of the world's global platforms, to adhere to this approach.

36 - <https://californiaaad.com>

## Challenges

One of the challenges for regulators is to understand the sheer range of methods for age verification that have evolved over time and to assess the relative levels of robustness, efficiency, coverage and availability at scale – as well as to ensure adherence to various privacy and data protection laws. It is too simplistic to assume that hard identifiers are always the ‘best’ or most secure age assurance option.

Worldwide, more than one billion people do not have access to identity documents. So age assurance solutions need to be accessible and inclusive. Individuals should ideally be given choice as to how they prove their age, and be presented with a variety of privacy-preserving options that respect existing data protection laws.

Some identity verification methods may offer a precise indication of age, for instance linked to a document, however may have a weak level of authentication that the correct person is using that document. However not everyone around the world has access to an identity document, particularly minors. So, in contrast, age estimation approaches have the merit of being more socially inclusive, and can offer inbuilt authentication. In lower risk settings, age buffers may not be deemed proportionate; whilst in high risk scenarios, age estimation approaches may need a year buffer to be applied. (e.g. to access an 18 plus service, the person may need to be estimated at over 21 years of age).

Regulators need to consider the level of determination needed for a committed person to circumnavigate each method and to actively test the overall effectiveness of the entirety of techniques deployed by a given content, social, gaming or other platform on a regular basis to enable age appropriate access. Independent audit bodies are needed to ensure that age assurance methods are transparent in terms of their accuracy levels, bias across skin tone and gender and to ensure that providers offering AI approaches are instantly deleting data and that datasets are collected in accordance with GDPR.

## Summary

To sum up – there are now a wide range of age verification and age estimation approaches. A person’s name is not needed to know they’re the right age. A range of tools now exist that let users prove they’re the right age for a service without sharing any personal information.

Regulators are also working out what technology they need to undertake their enforcement role and perform that at scale. It is interesting to see how certain regulators are already embracing AI approaches<sup>37</sup> and the use of avatars in their regulatory role. We expect to see an evolution of regulators harnessing digital technology themselves to automate testing at scale; in order to ensure that there is a ‘level playing field’ in terms of enforcement. There are now sharing forums across regulators where best practice is being shared.

The emerging standards for age assurance are embracing the full range of age assurance options. Companies are increasingly reviewing the range of options and deploying several age assurance options side by side.

There are now a number of global organisations who have embraced techniques such as facial age estimation to create age appropriate experiences and safeguard young people online, with companies such as Meta<sup>38</sup> and Yubo<sup>39</sup> leading the way. But there needs to be greater support and education around the world to understand the evolution of privacy preserving age assurance solutions and the important role they can play in protecting children and improving online safety.

37 – <https://www.medienanstalt-nrw.de/presse/pressemitteilungen-2022/2022/maerz/default-89c6b2daa0/mit-kuenstlicher-intelligenz-zu-einer-modernen-medienaufsicht.html>

38 – <https://about.fb.com/news/2022/06/new-ways-to-verify-age-on-instagram/>

39 – <https://techcrunch.com/2022/09/14/yubo-is-about-to-verify-the-age-of-all-its-users-using-facial-age-estimation/>

## Future scanning

### What does the future of age verification and regulation for 'age appropriate design' look like?

The first age checking standard was the PAS 1296:2018<sup>40</sup>. This standard has been built on and there will soon be international ISO<sup>41</sup> and IEEE<sup>42</sup> standards, which regulators will be able to refer to in legislation.

Regulators are starting to review how they embrace technology in their own horizon scanning, test purchasing, mystery usage/shopping, case management and enforcement activities.

Regulators are beginning to understand that pursuing individual legal cases one at a time, is time and cost inefficient. In order to regulate an industry effectively, they need to ensure that there is a level competitive playing field and not to just penalise or review the activities of just the top 5-10% of organisations. Falling costs and interoperable tokens for age verification solutions will make it easier for low and high traffic organisations to comply with age appropriate design codes.

In a parallel to the transparency reporting<sup>43</sup> that is required, in terms of child sexual abuse material prevention, regulators in parts of the world where 'age appropriate design' is required will be asking platforms to produce their own risk impact assessments to explain how they are acting in the best interests of the child and developing proportionate approaches for age appropriate access to content, goods and services.

Independent auditors and benchmarking will be needed to look under the bonnet of age assurance approaches. They will also be needed to review the totality of safety measures which platforms deploy to assess their overall efficiency in terms of acting in the best interests of the child and meeting each element of the Age Appropriate Design Codes.

### What are platforms and consumers opting for?

Increasingly, platforms are looking for methods that are data minimised, privacy preserving and low friction. There is also increasing adoption of inclusive estimation methods that do not rely on identity documents - such as facial age estimation.

Social media is a case in point - where up until now self-assertion and tick boxes have been used; however, now they are starting to look at how to build in age appropriate design to their services. It is not illegal for an under 13 to access social media, but it is against the terms of service of many organisations. Hence, facial age estimation is a promising step forward for many organisations wishing to adhere to Children's Codes in an inclusive and privacy preserving manner.

In terms of key trends, we see that when platforms offer consumers a range of methods side by side, currently the most popular and lowest friction approach is facial age estimation. There will no doubt be more innovations in this area.

UNICEF has set out excellent guidelines and principles<sup>44</sup> in terms of explaining AI to children. Industry and regulators have a duty to provide transparent, clear materials to civil society, the public and regulators to build understanding and trust in age assurance approaches. Consumers will expect straight forward explainer videos and education materials as well as privacy policies written in clear age appropriate language. Co-creation of products and services with young people and undertaking research with young people is increasingly seen as best practice.

An example is research by Play Verto<sup>45</sup> in conjunction with Yoti, which looked at young people's attitudes towards facial age estimation. Some 62% of children said they were either likely or very likely to use it again. In most cases they found the technology easy to use and understand, and 50% were curious to understand how the technology could estimate their age.

40 - <https://www.en-standard.eu/pas-1296-2018-online-age-checking-provision-and-use-of-online-age-check-services-code-of-practice/>

41 - <https://euconsent.eu/download/iso-working-draft-age-assurance-systems-standard/>

42 - <https://standards.ieee.org/ieee/2089.1/10700/>

43 - <https://www.law.cornell.edu/uscode/text/18/2258A>

44 - <https://www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf>

45 - <https://www.playverto.com>



## Recommendations

Below are some key recommendations that regulators of age assurance should encourage:

- **International Standards** adherence and direct mention within regulation.
- **Consumer education materials in plain language** following the UNICEF Policy Guidance on AI for Children<sup>46</sup>.
- **Education, and experiential feedback from young people** as to their experience of safety tools.
- **Transparency** - Publish transparent, clear details in plain English about how solutions are built, using mechanisms such as white papers.
- **Independent accuracy reviews** and implementation reviews by a third party, trusted and accredited auditors like the ACCS Age Check Certification Scheme<sup>47</sup>.
- **Independent bias review** of algorithms by recognised experts or auditors.
- **Interoperability** - Collaboration in terms of interoperability e.g. EU Consent Project.
- **Dialogue with trade bodies** - Age Verification Providers Association (AVPA), Open Identity Exchange (OIX), Online Safety Tech Industry Association (OSTIA)<sup>48</sup>, each with clear codes of conduct.<sup>49</sup>

<sup>46</sup> - <https://www.unicef.org/globalinsight/reports/policy-guidance-ai-children>

<sup>47</sup> - <https://www.accscheme.com>

<sup>48</sup> - <https://ostia.org.uk/>

<sup>49</sup> - <https://avpassociation.com/membership/avpa-code-of-conduct/>

## About this briefing

This briefing was supported by Julie Dawson, Chief Policy & Regulatory Officer at Yoti.

Yoti is shaping the future of digital identity. Yoti was founded in April 2014 and more than 12 million people have downloaded the free digital identity app to transform the way they prove their identity and have more privacy over their personal data. Yoti has performed over 550 million age checks in the recent period. With a team of over 500 people working together to shape the future of digital identity, Yoti's innovative solutions include age estimation, identity verification, digital identity, age verification and esignatures.

## Further reading

- [UNICEF paper Policy Guidance AI for Children](#)
- [Baroness Kidron 5 rights Bill](#) (Age Assurance (Minimum Standards) Bill)
- [Yoti Age Estimation May 2022 White Paper](#)
- [Yoti facial age estimation FAQs](#)

---

## Case study Yubo using Yoti facial age estimation to age verify 100% of users

Yubo, a live social discovery platform for Gen Z, is the first major social media app in the world to implement comprehensive age-verification for all its users, a groundbreaking milestone in a key area of concern in online safety today. In partnership with Yoti, Yubo first introduced this age-verification system in May for users ages 13 and 14, with the goal of scaling verification across all ages by year-end.

The new system mitigates risks of child abuse and other such acts by preventing bad actors users who might misrepresent their age from joining the platform. Age-verification technology separates users into different communities based on age bands to ensure that contact is age appropriate and deter interaction between teens and adults – a unique feature among social media platforms today.

Yubo's new age-verification system prompts first-time users signing up for an account, or existing users who haven't yet been verified, to take a real-time photo of their face on the app, using Yoti's facial age estimation technology.

Yoti's technology accurately estimates age by looking at an image of a face, which is analysed as a pattern of pixels. The technology converts the pixels to numbers and matches them to an age. Designed with privacy at its core, the system has no way of linking a face to a name.

If analysis detects a discrepancy between the age provided and Yoti's facial age estimation, additional identification steps to access Yubo are required. This happens through an in-app process overseen by Yubo Safety Specialists in accordance with "privacy by design" principles set forth by European data privacy laws.



---

## Appendix

### Key definitions

**Age assurance:** Age assurance refers collectively to approaches used to provide assurance that children are unable to access adult, harmful or otherwise inappropriate content when using Information Society Services (ISS); and estimate or establish the age of a user so that ISS can be tailored to their needs and protections appropriate to their age.

**The UK Children's Code (formerly known as the Age Appropriate Design Code or 'AADC'):** The Children's code (or Age appropriate design code to give its formal title) is a data protection code of practice for online services, such as apps, online games, and web and social media sites, likely to be accessed by children. It was developed by the United Kingdom's Information Commissioner's Office (ICO).

**Age verification:** Age verification is one form of age assurance to determine a person's age with a high level of certainty by checking against trusted, verifiable records of data. It is generally associated with methods that verify age or age-range to a higher level of confidence than the alternatives.

**Age estimation:** Age estimation is one form of age assurance. Age estimation is a process carried out by an Age Check Provider or an Age Check Decision Maker to establish that a citizen is likely to fall within a category of ages, over a certain age or under a certain age to a specified level of confidence by reference to inherent features or behaviours related to that citizen.

**Bias:** Bias is an inclination, prejudice, preference or tendency towards or against a person, group, thing, idea or belief. Biases are usually unfair or prejudicial and are often based on stereotypes, rather than knowledge or experience. Bias is usually learned, although some biases may be innate.

**Child:** In accordance with the United Nations Convention on the Rights of the Child (1989), a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier.

**Facial age estimation:** Facial age estimation technology accurately estimates a person's age based on a 'selfie' photograph. This approach doesn't require any personal details or ID documents, and all images are instantly deleted once someone receives their estimated age – nothing is ever viewed by a human. It can't link a name to a face or identify anyone. This is the difference between facial analysis and facial recognition.

It is against the law, for example under UK General Data Protection Regulation (GDPR)<sup>50</sup>, for an age verification provider to ask you for a photo for the purposes of estimating your age, and then keep it for any other purpose unless you give clear and explicit consent.

**Facial recognition:** Facial recognition is about using your face as a password. If a biometric feature is to be used as a key to unlock a previously determined record of your age, then enough unique data points need to be stored to allow for the user to prove they are the same person. This data can be stored locally on a device, or encrypted before being stored centrally, but again only accessible with a digital key controlled by the user themselves.

**Liveness detection:** Liveness detection is a capability of a biometric system to differentiate falsified biometric traits presented to its sensors from the genuine ones. Liveness detection is the central component in biometric security as it prevents fraudulent enrolment attempted with synthetic traits.

**Tokens:** Age Tokens are digital proof that an age check has been completed by a relying party. This proof combined with proof of ownership of the check provides confidence that the individual presenting the Age Token has the same age identifiers described in the Age Token. This process is completed without revealing any identifiable information about either the subject, the original relying party, or any other relying party.

---

<sup>50</sup> – The UK GDPR absorbs the privacy compliance requirements of the European GDPR and combines them with the requirements of the UK's Data Protection Act.

## Acronyms

AADC - Age Appropriate Design Code	ISO - International Organisation for Standardisation
AVMSD - Audio Visual Media Services Directive	IWF - Internet Watch Foundation
AVPA - Age Verification Providers Association	KJM - Commission for the Protection of Minors in the Media
BBFC - British Board of Film Classification	OFCOM - Office of Communications
CSAM - Child Sexual Abuse Material	OIX - Open Identity Exchange
GDPR - General Data Protection Regulation	OSTIA - Online Safety Tech Industry Association
ICO - Information Commissioner's Office	UNCRC - Convention on the Rights of the Child (1989)
IEEE - Electrical and Electronics Engineers Standards Association	

## Links to national and regional legislative sites outlining existing and proposed age verification related legislation.

**Germany** [https://www.gesetze-im-internet.de/stgb/\\_184.html](https://www.gesetze-im-internet.de/stgb/_184.html)

**France** [http://www.senat.fr/amendements/2019-2020/483/Amdt\\_92.html](http://www.senat.fr/amendements/2019-2020/483/Amdt_92.html)

**Poland** <https://opornografii.pl/article/premier-zapowiedzial-wdrozenie-projektu-zaproponowanego-przez-sts>  
<https://opornografii.pl/article/stowarzyszenie-twoja-sprawa-prezentuje-projekt-przepisow-chroniacych-dzieci-przed-pornografia>

**Ireland** <https://www.oireachtas.ie/en/bills/bill/2020/57/>

**South Africa** <https://justice.gov.za/salrc/dpapers/dp149-prj107-SexualOffences-PornographyChildren2019.pdf>

**New Zealand** <https://www.classificationoffice.govt.nz/about-nz-classification/new-zealands-classification-law/>

**Italy** [https://www.legislationline.org/download/id/4357/file/Italy\\_CPC\\_updated\\_till\\_2012\\_Part\\_1\\_it.pdf](https://www.legislationline.org/download/id/4357/file/Italy_CPC_updated_till_2012_Part_1_it.pdf)

**UK** [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/944310/Online\\_Harms\\_White\\_Paper\\_Full\\_Government\\_Response\\_to\\_the\\_consultation\\_CP\\_354\\_CCS001\\_CCS1220695430-001\\_V2.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944310/Online_Harms_White_Paper_Full_Government_Response_to_the_consultation_CP_354_CCS001_CCS1220695430-001_V2.pdf)

**Philippines** [http://legacy.senate.gov.ph/press\\_release/2021/0527\\_prib1.asp](http://legacy.senate.gov.ph/press_release/2021/0527_prib1.asp)

**Canada** <https://parl.ca/DocumentViewer/en/43-2/bill/S-203/third-reading>

**Australia** [https://www.aph.gov.au/Parliamentary\\_Business/Bills\\_Legislation/Bills\\_Search\\_Results/Result?bld=r6680](https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bld=r6680)

**Utah** <https://le.utah.gov/~2021/bills/hbillenr/HB0072.pdf>