Defining age verification and age assurance

February 2025

Executive summary

For many years, businesses, regulators and politicians have been saying it's either not possible or too hard to verify the age of people, particularly children, online. There has been a consistent message that effective and efficient age checks are too difficult, not scalable and too expensive. That they require identification, are an invasion of privacy and will exclude people who do not have the correct documentation.

However, age assurance technology has advanced to the point where it is now available for all online platforms. The technology is privacy-preserving, inclusive, scalable and low cost. As such, more regulators around the world are demanding that businesses use effective age assurance.

This report delves into the difference between age verification and age assurance to help businesses, governments or regulators.

Age verification, age assurance and age inference

***Age assurance** refers to various methods which are used to determine a person's age or age range. These methods offer different levels of certainty. Some determine a person's age to a very high degree of certainty while others provide a range or estimation for a person's age. These include:*

***Age estimation** measures infer an age or age range without other confirmed sources of information about the individual. This can involve the use of facial scans or other information such as behavioural patterns to estimate a person's age or age range.*

***Age inference** solutions use data signals—behavioral patterns, or account history—to determine whether an individual is likely above or below a certain age threshold. For example credit card ownership, mobile phone or email address history. For age inference, re authentication may be needed to reach a high level of assurance.*

***Age verification** determines a person's age to a high level of certainty, typically by verifying data against an external source. An example of age verification is using physical or digital government identity documents to verify a person's age.*

Most people are familiar with the term age verification. Most people will have been asked to prove their age when buying age-restricted goods or services, for example in a supermarket when purchasing alcohol.

It is used by many websites and apps to describe the process of asking someone to prove their age. It is also the term the press most often use when referring to the requirement of businesses needing to check the age of their consumers.

The correct term, however, in most scenarios would be age assurance. The business needs to be assured that their customer is of the right age.

You can get varying levels of assurance through the following techniques:

- Age verification
- Age estimation
- Age inference

A quick note on what is not age assurance

Age assurance does not include very basic self assertion methods, such as ticking a box to confirm age (“*Click to confirm you’re over 18*“) or entering a date of birth. This could, however, be used **in conjunction** with other methods that would provide additional evidence to confirm age to a required level of confidence.

Self assertion is the approach many websites have typically used for years; it is sometimes called an ‘age gate’. This method gives a very low level of assurance though (almost zero), as it relies on the honesty of the end user without any further method of checking their age.

Where no further checks are done, many children can bypass this method and access content which is not appropriate for their age. Unfortunately, children may not fully understand the impact of them pretending to be older. Self assertion also makes it easy for adults with malicious intent to lie about their age, pretending to be a child or teenager to access online spaces or features designed for children.

This method is now widely seen as ineffective by regulators and governments around the world, and is largely on its way out. The progression is to see which other methods it can be combined with, to increase the level of assurance.

A closer look at age assurance

Age verification

Age verification requires the customer to be verified to an ‘external source’, such as a passport, driving licence or credit card.

In a physical retail setting, the age verification process works as follows:

1) A shop worker suspects that a customer is under the legal age to buy an age-restricted item, they ask the customer to show some ID.
2) The employee checks if the customer matches the photo on the ID document. They will also attempt to determine if the document is authentic.
3) If the document is genuine and belongs to the customer, the sale of the age-restricted item proceeds.

There are, however, a number of flaws with this method. Studies have shown that people aren’t great at estimating ages. This means some workers will make mistakes and incorrectly estimate the age of some customers, not even challenging some people who are underage.

The manual inspection of the ID document also requires significant resources in terms of staff training, and places pressure on employees to accurately check documents. But the quality of fake IDs is now incredibly sophisticated, with fraudsters churning out masses of fakes in minutes at a very low cost. This makes spotting a fake with the human eye very difficult. Additionally, age checking is one of the most common triggers of abuse towards retail staff, and is subject to human factors such as bias, either conscious or unconscious.

In an online setting, an individual could be asked to upload their identity document which is then matched to their selfie. For this age checking method to be effective and to give a high level of assurance, these steps need to be achieved:

- Determining the authenticity of the document and extracting the relevant data
- Correctly matching the user to their document
- Ensuring a real person is uploading the selfie
- Checking the document and selfie images captured are real and not generative AI or bots

Without these complementary steps, a child could easily use their parent's driving licence to pass an age check. And someone could buy and use a fake document, tamper with the date of birth on a real document, or use a lost or stolen document.

Age estimation

Age estimation is when technology is used to estimate the approximate age or age range of the individual based on attributes other than an identity document. This could be achieved by looking at the face of the person and estimating if they are over the required age. Or it could be making an assumption that they are old enough due to how long they have been active online. The level of confidence in these 'estimations' can be influenced by a range of factors that we will explain in more detail in our next report. Most age estimation techniques are also reliant upon considering whether a buffer is proportionate for the required age threshold.

Age thresholds

The current status quo, at least In some countries, such as the UK, businesses selling 18+ goods or services follow the Challenge 25 policy. Challenge 25 was introduced because studies showed that retail staff found it difficult to guess the age of a person, so they often made mistakes. By introducing a 7 year buffer, it reduced the chance of staff selling age-restricted items to underage customers. If staff have to judge that a customer is over 25, rather than over 18, they are less likely to serve someone who is underage.

Age estimation technology can be used with age thresholds, mirroring those already used in store. For instance, an online retailer selling 18+ items could use age estimation technology with an age threshold of 25. This means the technology needs to estimate the age of someone as 25 or over for them to pass the age check. Users who are younger than this threshold (aged 18-24) would need to use another method to prove their age.

The threshold that platforms enforce is influenced by the accuracy of the estimation technique and the age of interest. It might also be set by regulators. For instance the German regulator, KJM, currently requires regulated businesses with 18+ content to set an age buffer of 5 years, meaning people need to be estimated as 23 years or older.

It is important to note, models are constantly improving in terms of accuracy and fairness and regulators are following improvements in accuracy so that potentially a more fair and accurate system can be implemented than the current over 25 or 40 model.

Proportionality

Proportionality is also very important when deciding on an age threshold. Regulators will need to consider what are accessible alternative options for those people (e.g. aged 18-24) to prove their age, and provide clear guidance on the age thresholds platforms need to use when using age assurance technology.

Regulators and companies will also need to consider if they must know the exact age of someone or if knowing which age band someone falls in is sufficient. This could mean that higher risk or regulated sectors, such as those selling age-restricted items or platforms with adult content, need to verify age to a high level of assurance.

In practical terms, retailers do not under any circumstances want to sell tobacco or alcohol to under 18s as they could lose their licence. So they might choose a higher threshold, such as 7 years, in line with a Challenge 25 policy. They would then offer another method for those who are estimated to be below 25 years.

A gaming or social media platform, however, might be happy to just know which age band a player falls in. For example, knowing whether someone is over 13 or under 18 means the platform can tailor the content and deliver an age-appropriate experience.

Privacy

Aside from checks for gambling, where Know Your Customer (KYC) checks are required, the vast majority of regulators agree that protecting the privacy of the individual when ascertaining their age is critical.

In most scenarios, a business just needs to know that their user is of the right age or age range. For instance, a platform with adult content just needs to be certain that only people aged over 18 are accessing their site. They do not need to learn anything else about the user. They do not need to know details like the user’s name or even their date of birth.

Balancing privacy with effective age checks is important to build trust and acceptance of age assurance:

- Many people do not want their identity linked to certain websites
- There might be concerns that personally identifiable information could be used inappropriately online
- People might want to share as little information as possible when passing age checks
- Some customers do not want retail, hospitality or security staff checking their driving licence given it contains their home address

When it comes to age assurance, regulators and businesses prefer that the user is not identifiable from the data used to determine their age. For this reason, the vast majority of age assurance methods have been designed to be data minimised and protect the identity of users. These methods are privacy-preserving, non-intrusive and can be configured to only return the age result required by the business. This means people can prove their age in a data minimised way, for example sharing just the fact that they are ‘Over 13’, ‘13-17’, ‘Under 18’, or ‘Over 18’.

The ‘perception of privacy’ by the end user however will vary from person to person. It is also critical that the end user has confidence in the age assurance solution and consequently that they trust no personally identifiable information is going to be shared or kept.

Finally, people need to be able to choose which age assurance method they’d like to use. This lets people select the method they trust and the one they feel the most comfortable with. It also ensures age checking is as inclusive and accessible as possible.

Fairness, origins and independent external review

Another clear requirement is for all age assurance approaches to meet equity regulations and AI regulations. Platforms typically deploy a range of solutions to allow consumers the choice of which methods they prefer, given that not all methods will suit all people.

On the data protection front, it is vital to understand the source of data that is used to build algorithms, and that the data has been collected in accordance with privacy regulations. An independent audit is also needed to show accuracy and bias levels.

Clearly as circumvention attacks evolve, regulators will also require independent evidence and certification of liveness detection and anti injection attack detection. And where methods involve checks to documents or databases, to provide a high level of assurance, checks are needed to confirm the document is authentic and belongs to the person presenting the document.

Memberships, associations and accreditations

WeProtect GLOBAL ALLIANCE

OSTIA ONLINE SAFETY TECH INDUSTRY ASSOCIATION

AVPA The Age Verification Providers Association

ISO 27001:2013 • ISO 27701:2019 CERTIFICATION™ intertek

ISO 27001:2013 CERTIFICATION™ intertek

ISO 9001:2015 CERTIFICATION™ intertek

SafetyTech Innovation Network

AICPA Service Organization Control Reports AICPA SOC 2 Formerly SAS 70 Reports

POINT DE CONTACT .NET

Reviewed by

Age Check Certification Scheme

FSM

kjm Kommission für Jugendmedienschutz

NIST

nccgroup

YOTI

To find out more visit **yoti.com**