



Age-assurance technologies - how they work in practice

Introduction



Julie Dawson

Chief Policy & Regulatory Officer

julie.dawson@yoti.com

www.yoti.com

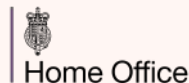
[@getyoti](https://twitter.com/getyoti)

Yoti has undertaken over 900m checks, over 1 million + checks daily

Social networks,
gaming & Kids sites



Law enforcement
& not for profit



Retail and ecommerce



PHILIP MORRIS
INTERNATIONAL



Gaming and telecoms



Adult operators



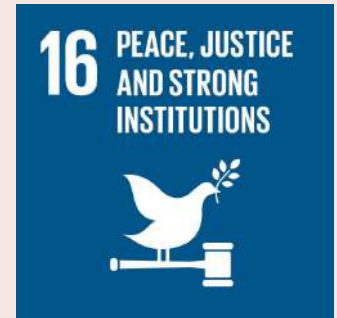
Over to you - What ID documents do you own?

Over 1 billion people **do not** own an **identification document**, according to the 2018

ID4D Global Dataset published by the World Bank, 13% of the global population

Sustainable Development Goal 16.9 aims to provide '**legal identity for all**'.

Until then - what ways can people prove their age if they don't own or have access to a document or don't feel comfortable to use it...



One of the widest selection of age assurance methods



Facial age estimation

Global



Digital ID app

Global



ID verification

Global



Age tokens

Global



Credit card check

Global



Mobile phone check

Regional



Database check

Regional



Email address check

Regional



Swedish Bank ID

Sweden



FTN

Finland



MitID

Denmark



Double anonymity

France



Social Security Number check

US



LA Wallet

US Louisiana



US Partner

US Florida



Facial age estimation

Instantly estimate a user's age based on a picture of their face.



Instant and anonymous.



Proprietary AI-powered algorithm with world-leading accuracy.



No pre-registration needed or ID document required.



Highly scalable system runs live and retrospectively.



All images instantly deleted and non-identifiable.



NIST2 approved passive liveness detection ensures user is real.



Flexible API to embed into your website, app or terminal.

[Read our white paper >](#)

How is it facial age estimation built?

In the **training stage** - we feed the neural network millions of diverse facial images, for which we know the subject's age (month and year) with confidence. After repeating the process a huge number of times, it arrives at sets of processing formulae which work best.



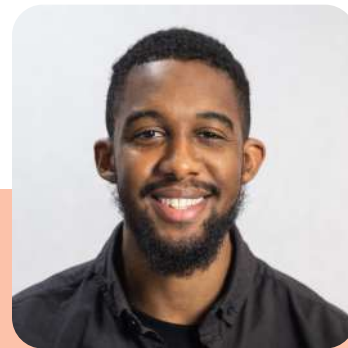
41 Years 1 month
Female



22 Years 3 months
Male




32 Years 7 months
Female




28 Years 6 months
Male


Facial age estimation - what levels of assurance?

Using facial age estimation technology to check age online can be considered 'high assurance' when multiple factors have been addressed.


**Liveness check**


Check the person behind the camera is a 'live' person and not a photo or video.




**Low assurance**


Level 1

**Liveness check**


**Independent testing**


Have a credible third party assess the technology for data compliance, bias and accuracy.





**Medium assurance**

Level 2


**Buffer**


**Liveness check**

**Independent testing**

**Injection attack detection**

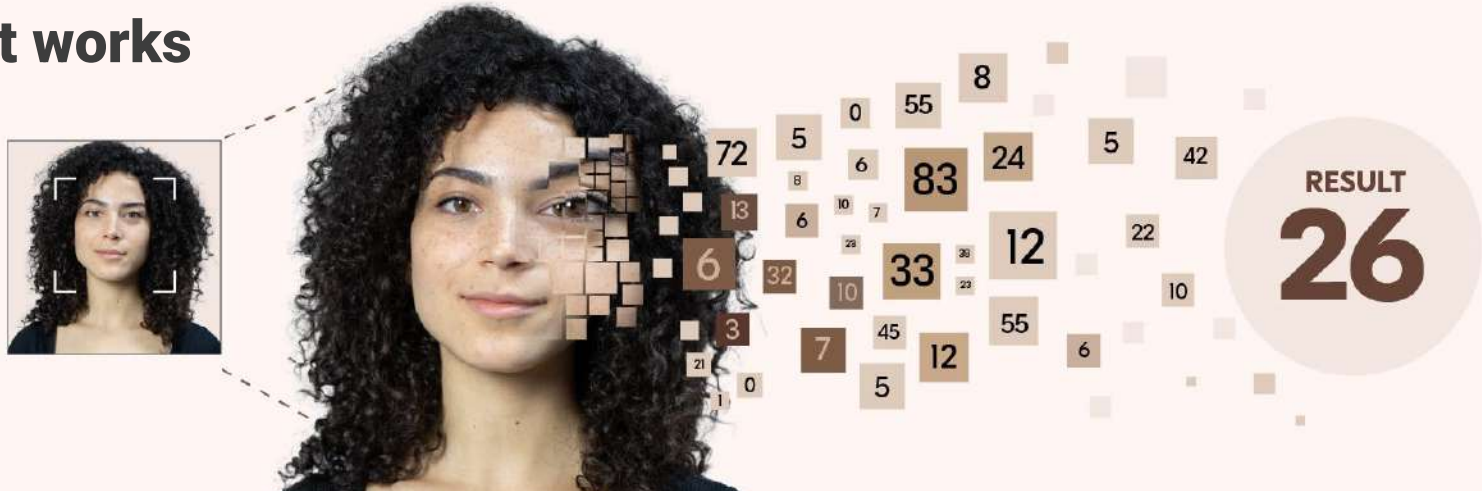
Add robust anti-spoofing technology at the point an image is being taken to detect injection attacks.



**High assurance**

Level 3

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.

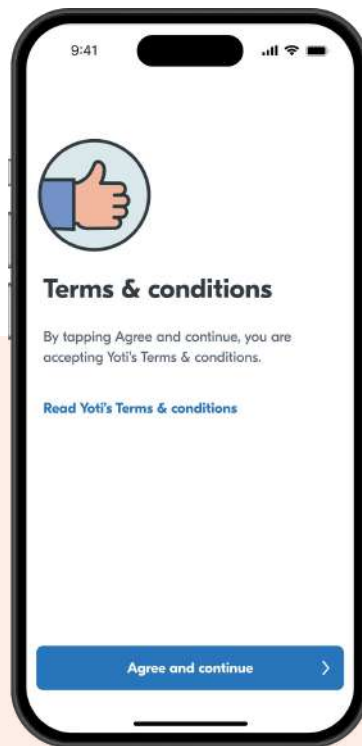
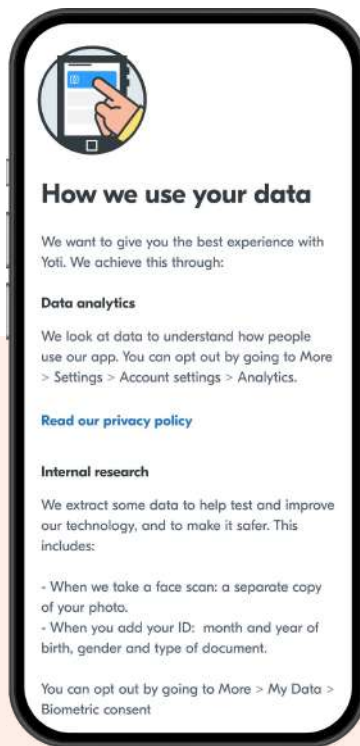
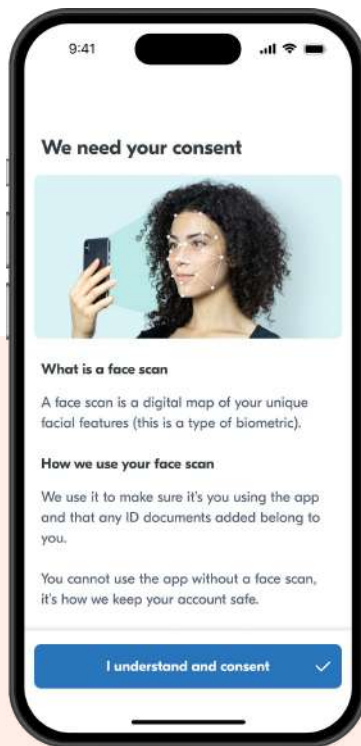
Instant process - scalable to tens of millions a day - no images are stored



Where does the data come from? for training & testing

Onboard and R&D opt-out screens in the Yoti app

We provide information to users at onboarding about our use of biometrics. This includes links to further information, including the full privacy notice, where the use of user data for R&D is extensively detailed. Users can opt out of their data being used for R&D at Yoti at any time, via the settings on the app.



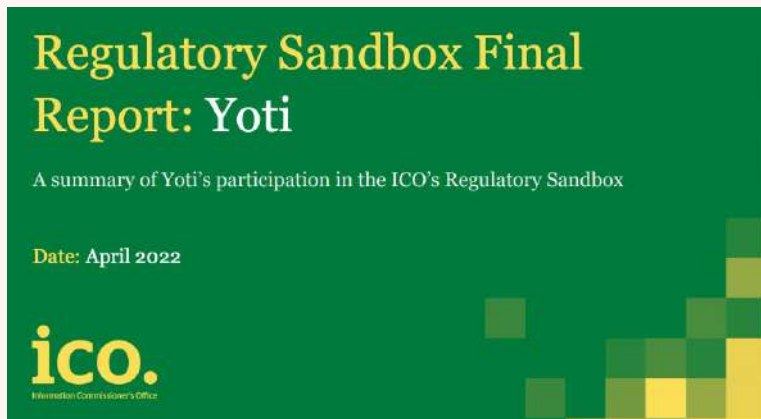
Is AI Facial Age Estimation - recognising anyone? NO

Detects a face & then analyses it



It is not a **1:1** verification or facial recognition or a **1: MANY** facial recognition

ICO Sandbox 2022 ahead of the Age Appropriate Design Code (AADC)



- Extended the data set from 6-70 to support the age bands in the AADC
- Co created explainer materials with young people, following Unicef guidelines
 - *Yoti's age estimation tool has demonstrated that it is possible to use biometrics to make a decision about an individual or treat them differently **without using that biometric data for the purpose of uniquely identifying that person.***
 - *Yoti's age estimation tool will **not result in the processing of special category data**.*

Where is AI Age Estimation deployed?



Retail, Home delivery
Click & collect



Kids sites,
Edtech



Govt CSAM



Adult websites



Social media,
Metaverse



Dating sites



Deployment

- **On a terminal** - retail EPOS, gambling terminals
- **SAAS** - assessing age or age band for person to access online ecommerce (tobacco/vaping/alcohol, pharma), social media/live streaming, gambling, gaming, adult content, dating
- **SAAS** - assessing age of adult to support parental consent
- **On premise** - law enforcement to assess age of victims & perpetrators in CSAM
- **On device** - eg prevent CSAM/nude sharing from phone / VR headset...
- **On device** - ensures solution effective even when connectivity is unavailable

Mean Absolute Error by age band

Mean Absolute Error by age band

Yoti facial age estimation accuracy										Mean estimation error in years split by gender, skin tone and age band			
Gender	Female					Male					All		
Skintone	Tone 1		Tone 2		Tone 3	All	Tone 1		Tone 2			Tone 3	All
6-12	1.1		1.3		1.5	1.3	1.1		1.2		1.3	1.2	1.3
13-17	1.0		1.2		1.5	1.2	0.8		1.0		1.3	1.0	1.1
18-24	2.3		2.2		2.5	2.3	2.0		1.8		1.8	1.9	2.1
25-70	2.4		2.7		3.2	2.8	2.3		2.6		3.1	2.7	2.7
6-70	2.2		2.4		2.8	2.5	2.0		2.3		2.6	2.3	2.4

How accurate is it for 6-18 year old and for 13 year olds

MAE
(Mean Absolute Error)

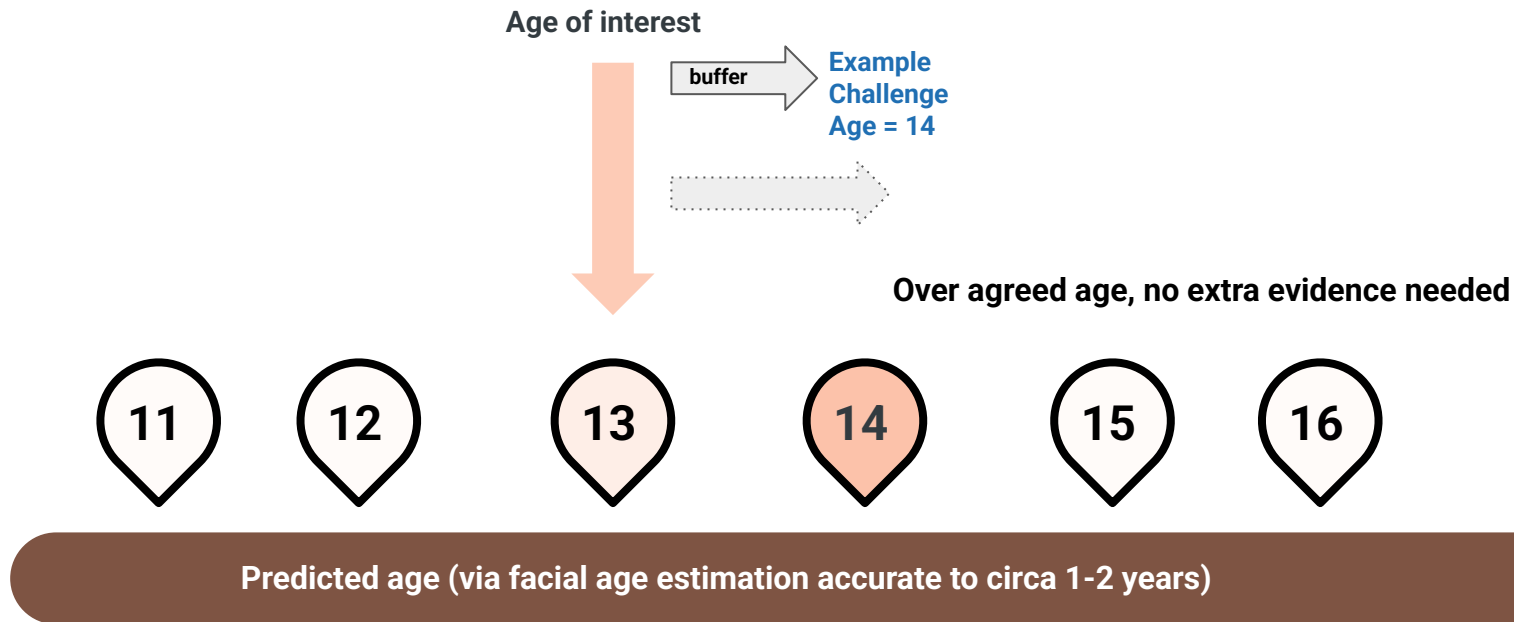
- 1.1 years for 13-17 year olds.
- 1.3 years for 6-12 year olds.

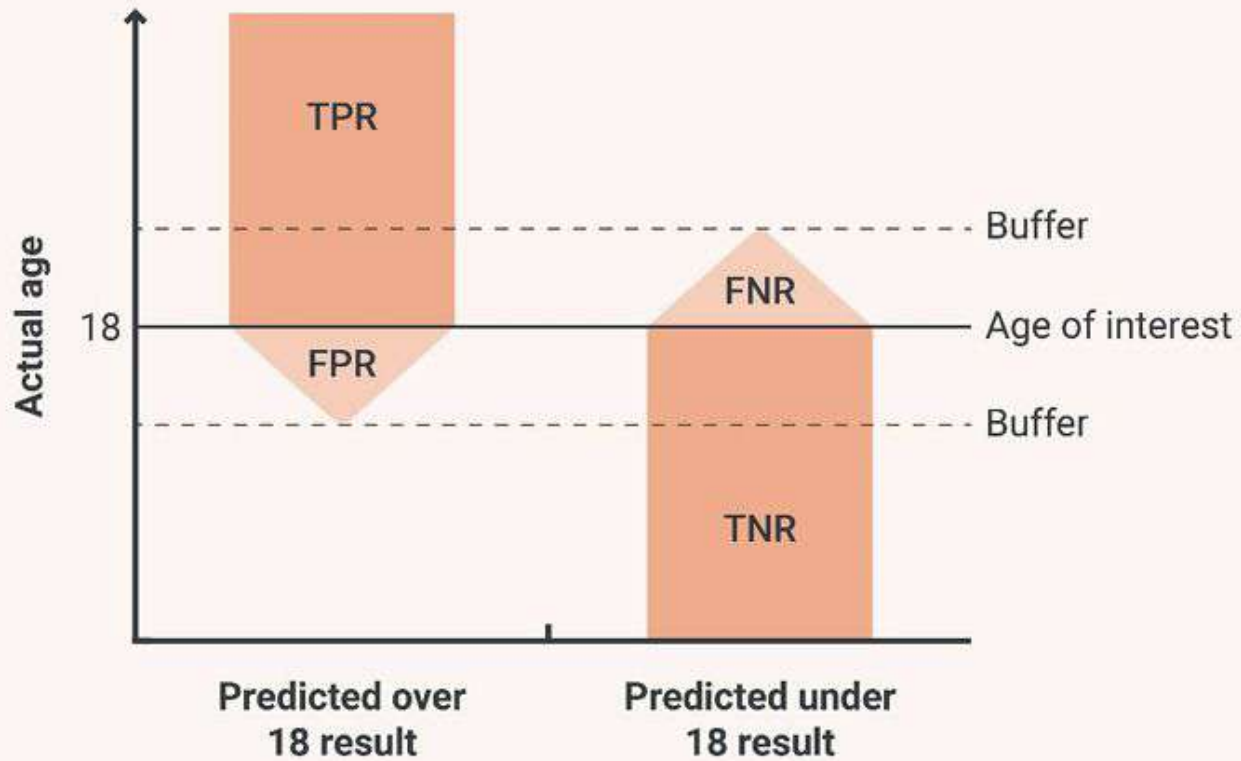
Age	Gender								All
	Female				Male				
	Skin Tone								
	Type 1	Type 2	Type 3	All	Type 1	Type 2	Type 3	All	
	MAE	MAE	MAE	Average MAE	MAE	MAE	MAE	Average MAE	
6	1.1	1.5	2.0	1.5	1.2	1.6	1.7	1.5	1.5
7	1.3	1.1	1.3	1.2	0.9	1.0	1.8	1.2	1.2
8	1.3	1.0	1.4	1.2	1.4	1.4	1.1	1.3	1.3
9	1.1	1.2	1.5	1.3	1.4	1.0	0.9	1.1	1.2
10	1.0	1.2	1.1	1.1	0.8	1.1	0.8	0.9	1.0
11	0.9	1.4	1.8	1.4	1.0	0.9	1.1	1.0	1.2
12	1.3	1.4	1.7	1.5	1.0	1.5	1.2	1.2	1.4
13	1.5	1.9	2.3	1.9	1.1	1.2	1.7	1.3	1.6
14	0.9	1.3	1.8	1.4	0.7	1.1	1.8	1.2	1.3
15	0.7	1.0	1.3	1.0	0.6	0.9	1.3	0.9	1.0
16	0.8	0.9	1.1	0.9	0.6	0.9	1.0	0.9	0.9
17	0.9	0.9	0.8	0.9	0.8	1.0	0.9	0.9	0.9
18	1.4	1.3	0.9	1.2	1.3	1.3	1.0	1.2	1.2
19	1.9	1.8	1.8	1.9	1.7	1.5	1.5	1.5	1.7
20	2.3	2.2	2.1	2.2	2.1	1.7	1.9	1.9	2.0

TPR for 6-12 year olds correctly estimated as under 13 is 99.5%.

Buffers and how to set them

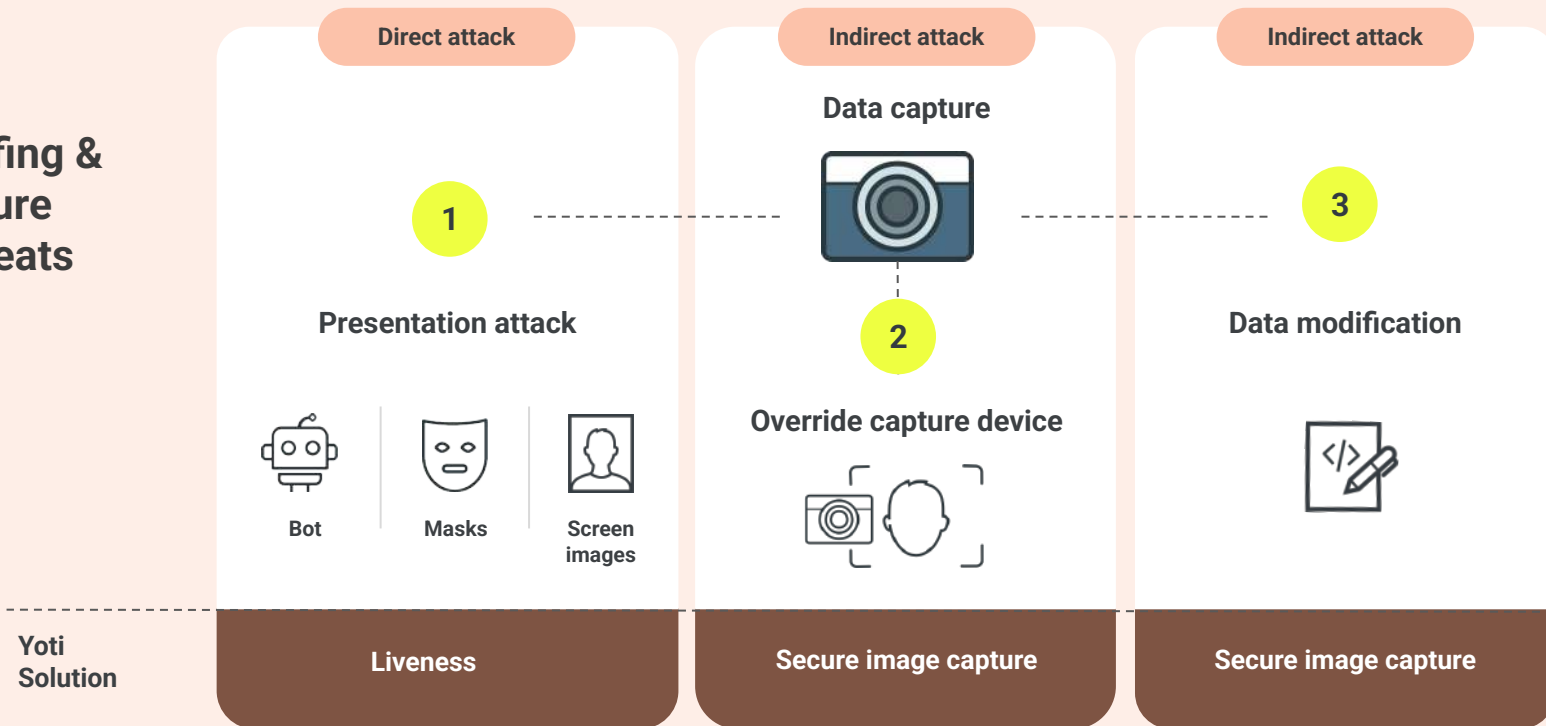
(e.g. where illegal to access under a certain age - more evidence may be required for those estimated to be close to 13).





How to meet the threat of generative AI?

Anti spoofing & Data capture attack threats



Anti-injection detection whitepaper

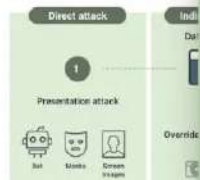


Yoti's response to the threat of generative AI

Our strategy for detecting the threat of generative AI focuses on early detection, i.e. the point at which the AI-generated image or video enters the verification process.

Bad actors can try to spoof the image input into the verification process by using presentation attacks (direct attacks).

Data capture attack threats



Yoti Solution

Liveness

Secure



On the threat of Generative AI

February 2024



Challenge

Advancements in various fields, generative AI also brings challenges. Some notable concerns associated with generative AI

include the ability to create highly convincing deepfake content, including images and videos, which poses the potential for misinformation, fake news and the erosion of authentic and generated content.

Generative AI is also used to create synthetic identities and realistic forged documents, which can be used to bypass verification systems and may be exploited for fraudulent activities and unauthorised access.

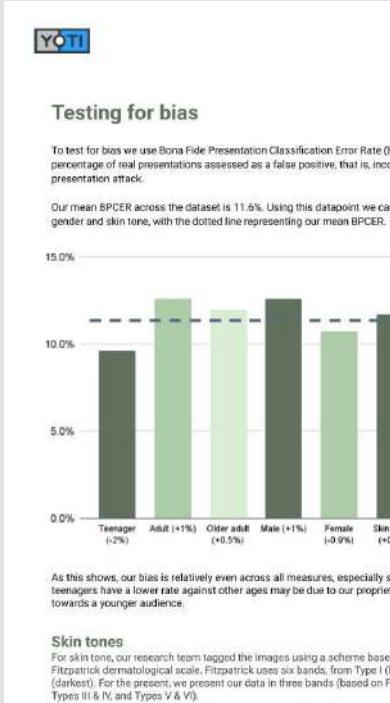
The use of synthetic images and videos raises privacy concerns, especially when they feature individuals without their consent, as people's likenesses are used in ways they did not intend.

Impact:

Generative AI can be used to fool biometric authentication systems, compromising the security of systems relying on facial recognition, fingerprint or voice authentication.

Generative AI can be used to create sophisticated phishing attacks, including fake emails and messages, which become more challenging to detect and mitigate as the technology evolves.

Liveness whitpaper

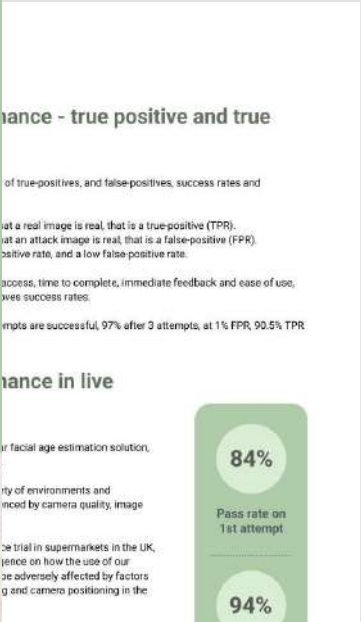


YOTI

Yoti MyFace[®] Liveness

White Paper | Full version

March 2023



Other resources

White papers



Facial age estimation - [LINK](#)



Liveness detection - [LINK](#)



Anti injection attack detection - [LINK](#)

Video explainers

We partnered with Youtuber **Be in Touch** to help talk about how AI really works, based on the Unicef principles for explaining AI to young people.

3 minute explainer

[LINK](#)

2 part explainer

[video - part 1] 8 minute [LINK](#)

[video - part 2] 12 minute [LINK](#)

Meta video explainer

[LINK](#)

Attitudes to Facial Age Estimation - Playverto Research findings

Results from children



- 50% were curious about how the technology estimates their age
- 84.6% of children said they understand why websites check age
- 67.5% understood what the selfie was for & how it would be used
- 88.3% found the instructions to use easy to understand
- 62% of children said they were either likely or very likely to use it again

Case Studies -

How Meta is making Instagram age appropriate



Industry
Social media



Methods
Facial age estimation

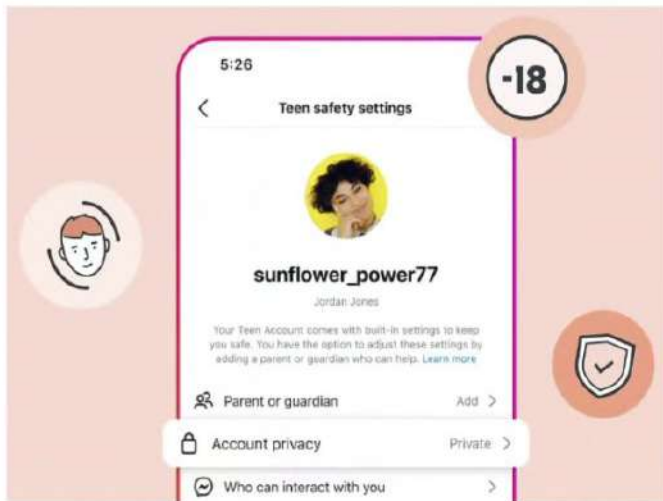
Instagram is a social networking app with 1.386 billion users globally.



1. When someone changes their date of birth from below 18 to 18+, they're asked to prove their age.
2. We power the video selfie method, which is analysed by our facial age estimation AI. We also run a liveness check to make sure it's a real person.
3. We tell Meta in under a second if the user is over 18 and delete the image instantly.

81% of users prefer using age estimation to uploading ID

Instagram Teen Accounts (launched 17 Sept 2024)

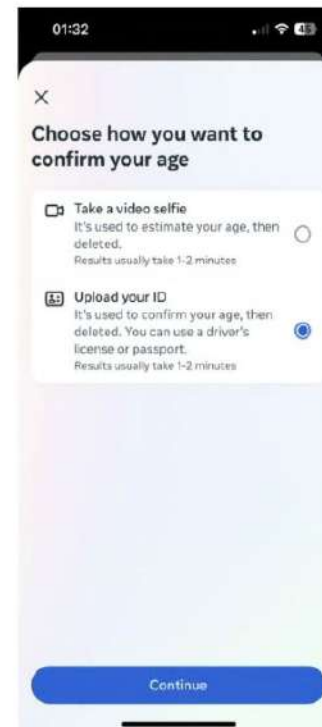


Enforcing Teen Accounts

Teens attempting to change their birthdate or use a new account with an adult birthdate are being asked to verify their age via facial age estimation or IDV.

Takeaways

- We're introducing Instagram Teen Accounts to automatically place teens in built-in protections and reassure parents that teens are having safe experiences.
- Teen Accounts will limit who can contact teens and the content they see, and help ensure their time is well spent.



How we're helping Yubo age verify 100% of users



Make new friends



Industry

Social media



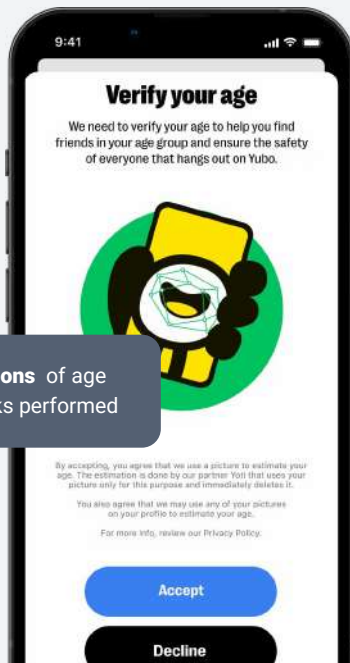
Methods

Facial age estimation

ID verification

Yubo is a social networking app for teenagers with 60 million users.

Millions of age checks performed



By accepting, you agree that we use a picture to estimate your age. The estimation is done by our partner Yoti that uses your picture only for this purpose and immediately deletes it.
You also agree that we may use any of your pictures on your profile to estimate your age.
For more info, review our Privacy Policy.

Accept

Decline



Make sure there's enough light to take a good photo.

1000s of accounts suspended

1. Users prove their age with a live selfie during onboarding. This is captured within the Yubo app to prevent false images being used.
2. The image is analysed by our facial age estimation AI. We also run a liveness check to make sure it's a real person.
3. Anyone that fails the checks is asked to prove their age with an ID document.

How Meta is making Instagram age appropriate



Industry
Social media



Methods
Facial age estimation

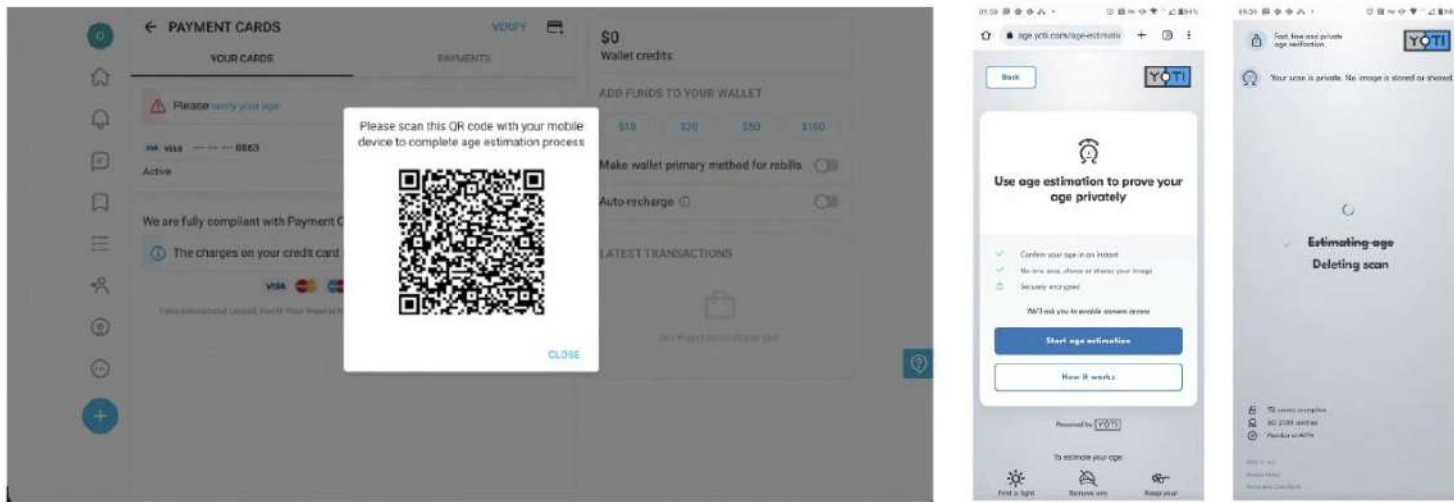
Instagram is a social networking app with 1.386 billion users globally.



OnlyFans - 18+ age verification of subscribers to adult content



Use case: using Yoti facial age estimation in certain jurisdictions, including Japan, to confirm those setting up Fan accounts (subscribers to Content creator feeds) are over 18.



"Ensuring our users are over 18 is a priority for OnlyFans and an important element of protecting our community. We work with Yoti because their market leading age assurance technology provides the right balance between accurately assessing users' ages and respecting their privacy" - Keily Blair - CEO, OnlyFans

Read more:

https://www.yoti.com/wp-content/uploads/Onlyfans_Case-Study_120623.pdf



Gaming with Avakin Life for 18+



Results

Adult players on Avakin Life can now choose to verify their age to unlock exclusive game features. Any players who are suspected to be underage are also asked to confirm their age; increasing trust and safety in the game.

Avakin Life players who have not verified their age cannot access age-verified spaces. This ensures players aged 18+ can confidently interact and chat with other adult players, while also enhancing the safety and player experience for younger audiences.

Facial age estimation within a parental consent flow at 25+

Liveness check

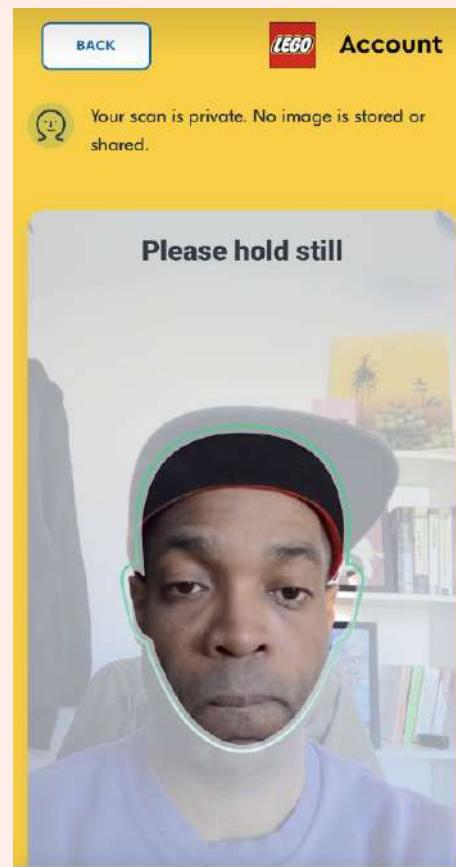
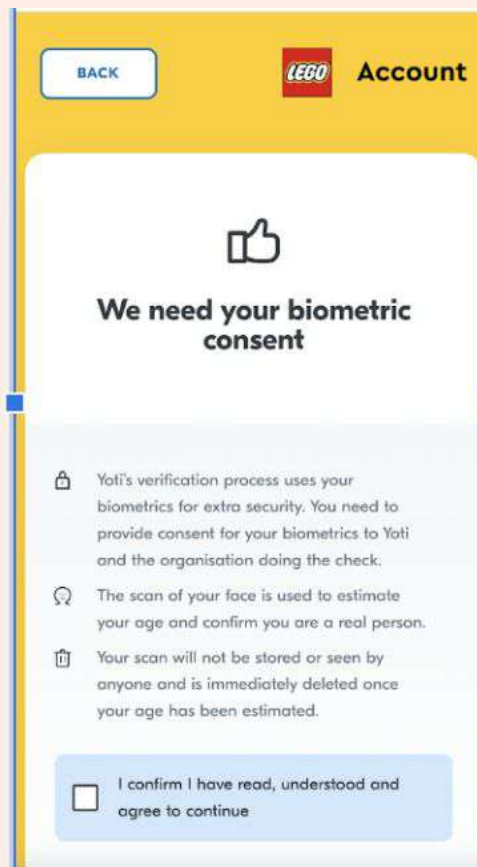
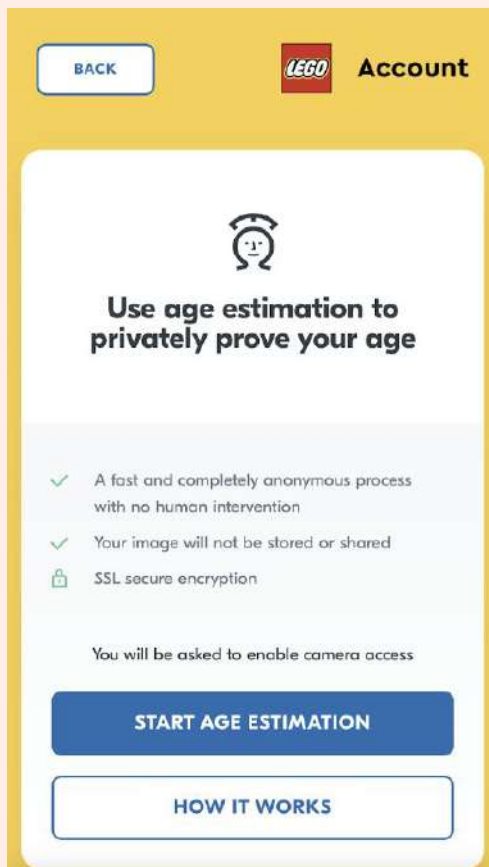
Check the person behind the camera is a 'live' person and not a photo or video.



Face capture + estimate

Analyse the facial patterns to anonymously estimate age





NIST Facial Age Estimation

The first global benchmark for an Age assurance approach -

NIST has published a [report](#) with the full results of the FATE testing program. NIST evaluated Yoti's facial age estimation on over 11 million images of people, aged 0-99.

In the visa category, Yoti has the best MAE (Mean Absolute Error) of 2.0 for 6-17 year olds, the key age group to ensure effective over 13 and over 18 age checks to help keep children safe online.



 Press releases

May 30, 2024

Yoti facial age estimation evaluated in the NIST Face Analysis Technology Evaluation...

Yoti proven to be the most accurate facial age estimation algorithm for those aged 13-16, a key age group for online age regulations and chil...

Expert body review

KJM



FSM



ACCS



NCC Group



NIST



Australian
Govt benchmarking



UK Online Safety Act (Ofcom)

Jan 2025 Detailed Guidance On Heaa For Part 3 & Part 5 Services

Methods capable of being highly effective	Methods not capable of being highly effective
Open banking	Self-declaration of age
Photo-identification (photo-ID) matching	Age verification through online payment methods which do not require a user to be over 18 (Debit cards)
Facial age estimation	General contractual restrictions on the use of the service by children
Mobile-network operator (MNO) age checks	List is for Part 5 services Non-exhaustive
Credit card checks	
Digital identity services	
Email-based age estimation	

UK Age assurance should simultaneously effectively protect children, allow access for adults and preserve privacy (OFCOM)

4 key criteria for HEAA (no set figures – yet)

Technical accuracy (in lab)

If age assurance, use "challenge age" approach

Keep under review over time

Robustness (real life)

Multiple environment

Consider circumvention

Reliability (reproducible & trustworthy evidence)

Ensure trustworthiness of data sources

Reproducibility guidelines for AI (ongoing basis)

Fairness (avoids bias & discrimination)

AI – diverse data sets; test results to assess for bias

Standards development



IEEE 2089.1-2024
**IEEE Standard for Online Age
Verification**



ISO/IEC CD 27566-1
Information security, cybersecurity
and privacy protection- age
assurance systems- Framework

Part 1: Framework

Under development



PAS 1296:2018
Online age checking- Provision and
use of online age check services-
Code of practice

<https://www.yoti.com/wp-content/uploads/2023/12/Yoti-Age-Estimation-White-Paper-December-2023.pdf>

#CQIQualityLive

A maturing industry

- ✓ A healthy ecosystem of providers
- ✓ Global standards in place
- ✓ Adoption by global organisations
- ✓ Independent audits with consistent measurement
- ✓ Transparent benchmarking at scale
- ✓ An established trade body
- ✓ Sectoral research undertaken
- ✓ Regulatory reviews in various jurisdictions

Tokenisation of age checks

Age Tokens

Remove friction for returning users

Users can prove their age once and gain continued access to an **ecosystem of age-restricted websites**.

This is powered by a **network of reusable age tokens**. They keep users anonymous and verified.

How it works :



1 User proves their age.



2 An anonymous age token (18+) is added to their browser.



3 User freely visits other websites that accept the token criteria.



4 User visits a website with other requirements and is asked to prove their age again.

Yoti has strong certification traction, instilling trust in the platform, a key to winning the network

Yoti's internationally recognised standards & accreditations build trust with consumers, businesses and regulators.

Yoti strives to be transparent, inclusive, ethical, and accessible with algorithms free from material bias.

UKDIATF Certified



Right to work & rent, and DBS schemes

SOC 2 Type 2



Certified for technical and organisational security process

ISO 27001



Certified for security management standards

B Corp Certified



Highest standards of social & environmental performance

Age Checking



PAS 1296:2018

KJM



Approved by German Commission for Youth Protection (KJM)

Cabinet Office & CESG

GPG 45

Aligned to GPG45 Standard

CIFAS



Certified for information security management standards

FSM

FSM

Approved by German Association for Voluntary Self-Regulation of Digital Media

ACCS



Approved by the internationally recognised standards of the ACCS

WEF



Global Coalition for Digital Safety

Tech Coalition



Use of tech for keeping children safe online

WeProtect



Global Alliance Against Child Sexual Abuse Online

FOSI



Works to make the online world safer for kids and their families

OSTIA



Industry body for UK orgs operating in online safety

7

Key business principles 2014

4

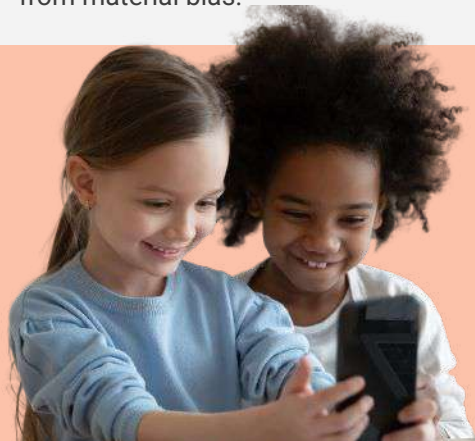
Trust Guardians 2015



Certified B Corp 2015



Fair Tax Mark 2017



What is ongoing



Keep asking for
feedback from
the stakeholder
community

Invite ethical
hackers



Sharing
accuracy at 13
years

Taking part in
benchmarking



Attitudes
survey

Accessibility

Language
localisation



Bias review

White papers
- liveness
detection
- Anti
injection



Research e.g. masks

New approaches -
EUDI wallet, email...

Tokens
interoperability

Thank you and feel free to ask further questions



Julie Dawson

Chief Policy & Regulatory Officer

julie.dawson@yoti.com

www.yoti.com

@getyoti

Resource List

Links

- [Amsterdam Global Age Assurance Summit 8-10th April, 2025](#)
- [Discussion paper: Where in the stack should age assurance happen ?](#)
- [Infographic summary A3 what is and what is not age assurance?](#)
- [Case study - How Yubo pioneered 100% user age estimation to drive safety and trust among Gen Z](#)
- [White paper facial age estimation](#)
- [Investigations announced into how social media and video sharing platforms use UK children's personal information | ICO](#)
- [Age appropriate design: a code of practice for online services | ICO](#)
- [Age assurance for the Children's code | ICO](#)
- [ICO real-world examples and case studies of different approaches to age assurance or an age-appropriate experience](#)
- https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en
- <https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer>
- [Statement: Age Assurance and Children's Access – Ofcom](#)
- [EDPB adopts statement on age assurance, creates a task force on AI enforcement and gives recommendations to WADA | European Data Protection Board](#)

Defining your age token criteria

You can define the criteria for what type of age tokens you accept based on the requirements in each jurisdiction.



The **maximum time** a token can be considered valid.



The **method of age verification** used.



The type of **age** - over/under or date of birth.



The **age threshold** a user must fall within.



The **type of liveness check** performed.



The **type of authenticity check** performed.

What's inside an age token?

Time: the time the check was performed.



Type: the type of age recorded.

Liveness: the type of liveness check performed.



Age: the result of the original age check.

Visitor ID: allows an owner to provide zero knowledge proof of ownership to multiple age tokens.



Method: age verification method used.



Issuer:

the issuer of the age token.



Age tokens don't contain any personally identifiable information

The Regulatory Landscape

European Union

Digital Services Act (DSA)

- + Requires platforms - especially VLOPs - to implement age verification as a risk mitigation measure, especially for services likely to be accessed by minors and for content that could be harmful to children
- + Art.35 references age verification as a risk mitigation measure, but does not prescribe exact methods, instead requiring a risk-based, proportionate approach.

General Data Protection Regulation (GDPR):

- + Sets a minimum age (13–16, depending on the country) for children to consent to the processing of personal data by information society services (Article 8)

United States

Kids Online Safety and Privacy Act (under discussion)

- + Required platforms to identify known minors and implement strong, default safeguards - including limited communication, restricted data sharing, reduced addictive features, and clear parental controls - shifting focus from age checks to a broader duty of care.

United Kingdom

UK Online Safety Act

- + Required all in-scope online platforms to conduct a children's access assessment by April 16, 2025, to determine if their services are likely to be accessed by children. A Children's Risk Assessment is then due in July 2025.
- + Mandates "highly effective age assurance" for services with harmful content (e.g., pornography) by July 2025.
- + Platforms must implement robust age checks for under-18s, using methods such as photo ID matching, facial age estimation, mobile operator checks, and digital identity services.
- + Platforms must specify age assurance measures in their terms of service and enforce them consistently.

Australia

Online Safety Amendment Act

- + Social media platforms designated as "age-restricted social media platforms" must take reasonable steps to prevent children under 16 from creating or maintaining accounts.

Discussion paper - where in the stack should AV happen?

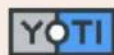


Age assurance technologies have evolved significantly over the past decade, with approximately 50 organisations developing tools ranging from age verification to age estimation and inference. Some of these tools are now independently audited and comply with global standards. There's also benchmarks like the *Global Guidelines for Biometric Technology (NIST)* evolution of AI facial age estimation. These approaches are designed to minimise consumer burden and be simple for organisations to integrate, within a matter of hours.

In this discussion paper, we explore where age assurance checks should sit in the consumer journey and in the tech stack; if it should be a one-off check at set up or both at set up and at the point of accessing a service, for added safeguarding. We will explore how re-authentication can lower the cost of repeat checks. Another approach described is a **layered approach** to age assurance combining:

- Age verification during device setup.
- Periodic re-authentication at the device level.
- Age checks at service access points.

1. <https://www.icsa.com/ageproof>
2. <https://www.association.com/agechecks-for-age-verification/>



Discussion paper

Where in the tech stack should age assurance sit and how should it be done?

January 2025



Author
Julie Dawson,
Chief Regulatory and

Order or friction on adults

has been in the age assurance journey overly sidestepping the user experience of unboxing a new device it is relatively straightforward to set up the struggle. And data transfer can take a few the storage on the old and the new phone, undertaking an age check at the moment of

age checks, you would in addition be asked to go then or age inference check, of your choice. a individual, that could take from a few seconds to

ding,

- How often should re-authentication be required?
- How would this be relied on with open-source operating systems? (For instance Linux is open source, so it is conceivable that only operating system level age verification can be disabled or modified by the user of the system to generate false results)
- Who is responsible for preventing the age verification information being used by predators to target minors?

es to consider undertaking checks at other levels in checks. In the next section we try to outline some p and negative, intended and unintended