ORG OPEN RIGHTS GROUP

REGULATING AGE VERIFICATION

KEEPING USERS SAFE ONLINE

July 2025

ABOUT ORG

Open Rights Group (ORG): Founded in 2005, Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect individuals' rights to privacy and free speech online. We have followed the Online Safety Act since its inception, and worked on age verification duties in its predecessory, the Digital Economy Act 2017.

ABOUT THIS REPORT

Report written by James Baker and Jim Killock

Published in July, 2025

Published by Open Rights, a non-profit company limited by Guarantee, registered in England and Wales no. 05581537. Space4, 113-115 Fonthill Road, London N4 3HH.

CONTENTS

APPENDIX: TERMS AND CONDITIONS OF UK MARKET AV PROVIDERS 20

THE NEED FOR A MANDATORY PRIVACY SCHEME

When the UK last proposed age verification for adult content online, we analysed the deficiencies with the proposed code of practice for AV, which, as with the current Ofcom codes, left providers to make the decisions on what security is themselves.[1] In our view, at a minimum, a mandatory scheme is needed to ensure that AV systems initiated by the Online Safety Act 2023[2] universally reach a high standard of data security and privacy. While this would not mean that it has no privacy impact, nor would it ensure that AV achieves its goals, it would at least ensure the current free-for-all and potential privacy debacles are avoided. The UK stands alone on this among major European countries; other jurisdictions are at least attempting to address privacy concerns, either through legislation or regulators.

1 https://www.openrightsgroup.org/publications/analysis-of-bbfc-age-verification-certificate-standard-june-2019/
2 https://www.legislation.gov.uk/ukpga/2023/50/contents

REGULATING AGE VERIFICATION

Likewise, other European jurisdictions appear to be clearer about when Age Verification is required. In the UK, companies are interpreting their OSA duties much more widely.

Ofcom cannot mandate privacy standards within their existing OSA powers, but Ofcom and the ICO can work to ensure a voluntary standard exists which would ensure providers complied with their privacy duties in the Online Safety Act.[3] Industries can currently propose voluntary schemes within existing data protection legislation, which are overseen by the ICO.[4] Likewise, the ICO could take a similar role to the CNIL, and provide clearer guidance on what is acceptable or best practice.

THE OSA CREATES INCENTIVES FOR POOR SECURITY AND PRIVACY

By providing no minimum standard for Age Assurance, and instead relying solely on data protection law, the OSA allows the main drivers for age assurance to be primarily commercial: **Convenience**, **Cost** and **Compliance**. The commercial incentives for choosing a provider and AV system will include:

3 Section 22 (3) OSA
4 UK GDPR Articles 42 and 43 https://www.legislation.gov.uk/eur/2016/679/article/42

- **Convenience** to the platform; usually meaning US-based and local to the platform;
- **Cost**; meaning that some platforms will choose low cost AV providers who have lower security investments or collect user data in order to monetise it as part of their business model. This can also include **Monetisation** of data by the platform: meaning the platform may choose to increase the benefits it receives from AV by collecting more than needed
- **Compliance**, meaning platforms use AV to meet their broader legal duties, such as to identifying which of their users are children, and which are adult, for a wide variety of content or service decisions

US based services are inherently problematic, as providers are used to permissive legal conditions for personal data, and are subject to US surveillance laws. It is harder for the ICO to regulate a market with numerous small US, UK and EU providers, devising their own privacy arrangements, than a market governed by an agreed standards body.

Furthermore, breaches of data protection law are rarely if ever enforced against by the UK's Information Commissioner, with the exception of spam and cold calling. This means that companies are not running a financial risk even if they seriously break data protection rules. While reputational

risks do not go away, these are insufficient to stop bad decisions from being made, especially when faced with other business pressures.

Additionally, the range and potential ubiquity of unregulated AV systems risks users engaging with actual scams as users have little or no control over how they verify their age.

This risky and dangerous situation regarding Age Assurance is the opposite of what legislation should be seeking. As we have detailed elsewhere, the risks to users can be extremely high, should data ever leak. We already seeing a proliferation of tools with poor data practices that could pose risks to users.

In this document, we outline the key steps needed to make Age Assurance required under the OSA sufficiently safe for users to engage with it.

RECOMMENDATIONS FROM OUR REPORT

In our report on *How to Fix the Online Safety Act,*[5] we made a number of recommendations:

5 Dia J. Kayyali and Bernard Keenan, "How to fix the Online Safety Act: A rights first approach" https://www.openrightsgroup.org/publications/how-to-fix-the-online-safety-act-a-rights-first-approach/

‘Recommendation 28: Platforms should provide users with detailed documents regarding the use of their data so that they can understand the risks to their privacy and data.

Recommendation 29: Ofcom and the ICO should work with industry to create a high standard for privacy in age verification.

Recommendation 30: Ofcom should recommend that age verification solutions include the use of high, independently managed data protection standards, and meet interoperability and accessibility needs.

Recommendation 31: Future legislation should incorporate privacy, accessibility, and interoperability requirements for age verification and assurance.’

Recommendation 32: Section 81 duties should be redrafted in future legislation to ensure no impact to privacy and as minimal impact as possible on free expression.

EXISTING AV STANDARDS AND WORK AT THE EU

A number of existing standards have been developed, such as the Age Check Certification Scheme (ACCS)[6] and PAS 1296,[7] but they are general in nature. While worthwhile, they are in our view insufficiently focused on the problems that must be addressed for the OSA's purposes.

All AV standards and legislative attempts have been criticised for potential privacy problems and for their likely ineffectiveness, but all European Union efforts contrast with the UK in attempting to address the privacy questions seriously and directly.

EUROPEAN UNION

The European Union expects that Age Verification will be needed for adult sites, although this is likely to be narrower than the UK's uses. They are undergoing a debate about how to establish high security and privacy techniques across member states, and have as a first step published an open source demonstration app.[8] While the EU's approach has difficulties,

6 https://accscheme.com/
7 https://www.en-standard.eu/pas-1296-2018-online-age-checking-provision-and-use-of-online-age-check-services-code-of-practice/
8 https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification ; see https://digital-strategy.ec.europa.eu/en/factpages/blueprint-age-verification-solution-help-protect-minors-online for a simple view of the way AV apps should function under the scheme

and also remains voluntary at the EU level, the UK could draw on this work as it progresses,[9] especially as it has the aim of producing a "user-friendly and privacy-preserving age verification method",[10] backed by legal requirements to protect fundamental rights.[11]

Some EU member states have also shown significant regulatory concern regarding age verification. For example, France's laws targeting access to pornography,[12] does not discuss privacy duties, however, their data protection authority has been active in setting the need for privacy,[13] developing recommendations since 2021,[14] and in 2022 recommending and demonstrating Zero-Knowledge systems for age verification.[15] It has also taken steps to prohibit pornographic websites from collecting identification documents. Likewise, the Spanish data protection authority

9 See https://ageverification.dev for an overview of the technical requirements
10 https://digital-strategy.ec.europa.eu/en/policies/eu-age-verification
11 Measures proposed by the Commission as best practice must have "due regard to the possible consequences of the measures on fundamental rights enshrined in the Charter of all parties involved" https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065#art_35
12 Article 227-24 of the French Criminal Code,
13 Commission Nationale de l'Informatique et des Libertés (CNIL). "Online Age Verification: Balancing Privacy and Protection of Minors." June 2021. https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors
14 https://www.cnil.fr/en/recommendation-7-check-age-child-and-parental-consent-while-respecting-childs-privacy
15 https://linc.cnil.fr/demonstration-privacy-preserving-age-verification-process

has established a Decalogue of Principles regarding online age verification.[16]

16 Decalogue of principles: Age verification and protection of minors from inappropriate content https://www.aepd.es/guides/decalogue-principles-age-verification-minors-protection.pdf

HOW TO REGULATE AGE ASSURANCE UNDER THE OSA

1. DEFINE THE GOALS OF AGE ASSURANCE

Age Assurance or verification is being employed to satisfy OSA compliance goals, but this is not the same as a social purpose. As a result, it is being used in new and unintended ways.

For example it is being used to check whether someone is adult or child, merely to access certain features or content, with a high and unintended cost to free expression. As noted above, it is also being used by platforms and providers for new business purposes such as gathering more personal data.

In order for regulators to be able to define and minimise the risks, the OSA needs to define closely when and where third party age assurance tools are actually needed, and ensure that uses are narrow, rather than expansive.

2. DEFINE MINIMUM LEGAL REQUIREMENTS FOR AGE ASSURANCE

The Online Safety Act must be amended to require that Age Assurance tools:

- meet high standards of data security
- ensure data minimisation for the user
- reduce data retention to the minimum necessary for the AV provider
- provide as little information as possible to the platform / publisher
- prohibited from using data for secondary uses, such as profiling and behavioural tracking
- are interoperable, so users can choose their own trusted Age Assurance tool
- meet the needs of vulnerable adult users
- are certified as meeting these standards

and that the certification body must be obliged to

- make their standards public and freely available
- make their register of approved providers public

- make regular public reports including details of any security or privacy issues in the period

Not all age verification systems need to comply with an OSA standard, but those employed for OSA purposes in our view must, given their widespread and compulsory nature, and their use regarding adult content and services.

3. MAKE CERTIFICATION MANDATORY

The government must establish **mandatory certification** requirements for all age assurance providers operating under the Online Safety Act. While voluntary standards or schemes are insufficient to ensure security, privacy, and public confidence, they currently can be recommended by Ofcom in their guidance, but it is not expected that Ofcom would have any role in shaping such a standard.[17] Likewise, Ofcom's guidance can make reference to the 'principle' of interoperability, ie users choosing their own AV tool, but Ofcom cannot mandate it.

17 Section 82 of the Online Safety Act directs Ofcom to produce guidance on what constitutes effective age assurance. This allows Ofcom to recommend standards that include technical and privacy standards. https://www.legislation.gov.uk/ukpga/2023/50/2023-10-26/data.html

REGULATING AGE VERIFICATION

Making a scheme mandatory would require a change to the Online Safety Act. A single high standard should be enforced and adopted, given the problems we note above.

Recommended Actions:

- Amend the Online Safety Act to require that AV tools used under the act are certified
- Amend the OSA to ensure a single standard is adopted and a certification body is appointed
- Amend the OSA to give the power to the ICO or Ofcom to appoint the certification body to create and maintain a detailed standard and for the state regulator to approve changes to the standard

---

4. ENFORCE THE STANDARD FOR ONLINE SAFETY AGE ASSURANCE

Either Ofcom or the ICO must ensure that the certification standards body meets the standards required by the Act. Depending on the mechanism, one or other would approve the standards body. Age Assurance providers would then sign up to the certification body, which would make checks to ensure compliance.

In the event of non-compliance, Ofcom or the ICO should be able to:

- Issue financial penalties
- Receive grievances, complaints and deal with potential non-compliance
- Require secure data deletion where standards are breached or certification lapses.
- Compensate individuals if they are directly impacted by a breach

DEVELOPING A DETAILED STANDARD

Much of the work of developing detailed security standards has already been done. Without going into the full detail of what one could look like, we would expect a standard to cover:

- data and metadata minimisation and other requirements made by the amended act
- use of zero-knowledge techniques where possible
- cryptographic requirements for data in transit or at rest
- limits to logging
- industry standards for cybersecurity that will be employed
- vulnerability testing to be employed, especially threat-led testing
- bounties for vulnerability detection and systems for responsible vulnerability reporting
- use of standardised risk assessments and response plans and their review by the standards body
- disclosure of breaches and reporting of vulnerabilities

- processes for swift fixing of vulnerabilities that are detected

The detailed standard can reference other existing Age Verification standards and schemes, but in our view needs to exist in its own right to meet the requirements created by making Age Assurance ubiquitous and mandatory for certain sites and users.

APPENDIX: TERMS AND CONDITIONS OF UK MARKET AV PROVIDERS

GRINDR

Grindr is a location-based social networking and online dating application for gay, bisexual, queer, and transgender people. Its users may face particular risks if their data is not properly protected.

Grindr will use biometric verification technology from Facetec. Users will have to complete a video selfie or submit a video selfie with an official photo id document, such as a passport or driver's licence.

Facetec's privacy policy states that data might be held in jurisdictions that have different data protection standards:

> **"Transfer of Personal Information Outside Your Home Country**
>
> FaceTec is located in the United States. The personal information that we (and our service providers) collect and

> process is governed by U.S. law. If you access the Site or Software from outside the U.S., please be aware that personal information collected through the Site or Software may be transmitted to, processed, stored, and used in the U.S. or other countries or places in which we do business. Data protection laws in those jurisdictions may be different from those of your country of residence. Your use of the Site or Software, or the provision of any personal information, constitutes your consent to the processing, use, sharing, storage, and transfer of your personal information to the U.S. or elsewhere, as set forth in this Privacy Policy."

They also state they will share identifying information with online advertisers, through marketing cookies.

> **"Business & Commercial Purposes for Disclosure**
> We may disclose your personal information for the following purposes:
> - Advertising and marketing, including targeted advertisements.[18]

While this is common for many sites that use advertising cookies, it would be particularly problematic if data is collected that shows the user has logged into

18 https://dev.facetec.com/privacy-site

Grindr and shares this onwards. Depending on the product's configuration, this could be a concern. Grindr have previously been fined by the Norwegian data protection authority for sharing user data in this way.[19]

BLUESKY

Age assurance provider: Kid Web Services (KWS)

According to Bluesky, Over 18s can prove their age through payment card verification, ID scans, and face scans'.

SERVICE RESTRICTIONS WITHOUT VERIFICATION

If users don't verify their age, they can still have a Bluesky account. However, not only will 'adult-appropriate' content be blocked but they will not be able to use services such as direct messages. This restricts the freedom of expression of over and under 18s using the platform.

KWS FINGERPRINTING AND REJECTION OF PRIVACY SIGNALS

KWS' privacy policy states that they do no respect 'do not track' signals from browsers. '

Do Not Track

19 https://www.datatilsynet.no/en/news/aktuelle-nyheter-2023/record-fine-grindr-confirmed/

> Your browser settings may allow you to automatically transmit a "Do Not Track" signal to online services you visit. There is no industry consensus as to what site and app operators should do with regard to these signals. Accordingly, unless and until the law is interpreted to require us to do so, we do not monitor or take action with respect to "Do Not Track" signals.[20]

They also collect information about the type of device you are using to create a fingerprint for you

> **Verification information.** Information you provide when you respond to a request from, or by us on behalf of, a Partner to verify your age, as well as your email address. The information you will be asked to provide depends on the country in which you are located and will include some, but never all, of the following information: your name, date of birth, mailing address, credit or debit card information, a personal identity number (such as a CPF number in Brazil, a CURP number in Mexico, certain digits of a RRN number or i-PIN in the Republic of Korea, and certain digits of a US

20 https://www.kidswebservices.com/en-US/privacy-policy#International-transfer-of-personal-information

social security number in the US), a cell phone number, an identity document or face scan.

- **Device and usage information.** When you interact with KWS, we automatically collect information about your devices (computers, phones, tablets etc.) and your use of and interactions with KWS, including in order to identify your country and language. We do this using cookies, server logs, web beacons, or similar technologies. **Device information** includes data about the operating systems and hardware and software versions, device identifiers, internet protocol (IP) address, login data, browser type and version, time zone setting, country and language, browser plug-in types and versions.

REDDIT

AGE ASSURANCE PROVIDER: PERSONA

Reddit has chosen Persona, a US-based company to provide age assurance. US based services are inherently problematic, as providers are used to

permissive legal conditions for personal data, and are subject to US surveillance laws.

RETENTION AND USE OF DATA

Persona claim the right to use data collected for purposes including advertising and research.[21] They retain documents that are uploaded, and delete them after three years if the customer ceases to interact with them.

They also have a broad clause allowing the use of data for product development and research.

RECORDING BIRTH DATES FOR ADVERTISING

Reddit is also recording users actual birth date, rather than whether they are over 18, in order to better target advertising and content recommendations.

> How will Reddit use my age information?
>
> Your birthdate is used to verify that you are of the minimum age to access certain restricted content on Reddit. It will also be used to ensure an appropriate ads experience for users, including disabling ads personalization and limiting ads in sensitive categories (for example, alcohol or

21 https://withpersona.com/legal/privacy-policy

gambling) for those under 18. Additionally, if you are below the minimum age to access restricted content, you are not permitted to moderate communities that are dedicated to NSFW or mature content.

Following verification by a trusted third-party identity verification provider, Reddit will securely store only your verified age information consisting of your birthdate and verification status (not the verification / photographic materials) in your account so that you do not have to enter it each time you attempt to access age-gated content in the future. Verified age information will not be visible to other users or advertisers, and will be used to enhance content relevance and ad experiences, as outlined in our Privacy Policy. We do not sell your personal data to third parties, including data brokers.

Visit our identity verification provider's Privacy Policy to learn how they process your personal information.[22]

22 https://support.reddithelp.com/hc/en-us/articles/36429514849428-Why-is-Reddit-asking-for-my-age

GENERAL CONTENT RESTRICTIONS AT REDDIT

As well as pornographic content, Reddit will restrict access to content also ask users to verify their age to access content:

> Restricted Content for Minor Users
>
> The following categories of content have been identified as content that should be restricted for UK users under 18:
>
> - promotes suicide, deliberate self-injury, and eating disorders;
> - incites abuse or hatred against people based upon protected characteristics;
> - bullying content;
> - promotes violence or "depicts real or realistic serious violence against a person, an animal, or a fictional creature";
> - promotes challenges or stunts that are likely to cause serious injuries;
> - encourages people to use harmful substances or substances in harmful quantities;

- content that shames people based on body type or physical features; and
- content that promotes or romanticizes depression, hopelessness and despair.