Age Verification Providers Association
557B Wandsworth Road, London, SW8 3JD
+44 (0) 7811 409769 | iain@avpassociation.com

Committee Secretary
Senate Standing Committees on Environment and Communications
PO Box 6100
Parliament House
Canberra ACT 2600
ec.sen@aph.gov.au

21 November 2024

Dear Chair and Members,

Submission re: Online Safety Amendment (Social Media Minimum Age) Bill 2024

We are the global trade body representing 30 providers of privacy-preserving online age assurance technology and appreciate the invitation to make this submission to your inquiry.

We offer no view on the merits of limiting access to social media to children at any particular age, but can confirm that the age assurance technologies required to facilitate the implementation of this Bill are sufficiently accurate, accessible, privacy-preserving, cost-effective, and aligned with international standards.

1. Availability of Proven Technologies

Technologies to verify age online are mature, diverse, and widely deployable. These methods cater to different user needs, enabling secure age verification for children and adults without introducing significant barriers. We welcome the flexibility in the Bill to permit multiple methods created by delegating guidance to the Commissioner. This encourages innovation, offers choice to users and allows for pragmatic application of the law aligned to the state-of-the-art of the age assurance technology as it evolves.

- **Government-Issued IDs**: Users can verify their age using passports, driving licences, or other official documents. This process often involves scanning or chip-reading the ID and cross-referencing it with a selfie image, which undergoes liveness detection to prevent fraud.
- **Digital IDs**: Increasing adoption of digital IDs enables users to selectively share their age without disclosing other personal details. These reusable IDs integrate seamlessly into online ecosystems, and can be created by either government or certified private sector identity service providers.
- **Bank Records**: Open banking initiatives, such as Australia's ConnectID programme, could allow users to confirm their age by securely linking their banking profile with an age assurance service.
- **Facial Age Estimation**: Advanced algorithms estimate a user's age based on facial features. These tools are particularly beneficial for children and adults who lack official identification. Accuracy is continually improving, with systems capable of reliable estimation within ever narrowing average error margins as little as +/- 1.05 years (see appendix). A similar technique relies on hand gestures rather than facial mapping.
- **Email Estimation**: Through analysis of transactions associated with a user's email address, it is possible to establish with a high degree of confidence if they are over a particular age (see appendix)
- **Mobile Network Data**: Telecom providers can confirm a user's age based on subscriber records, building on their existing role in implementing adult content blocks in some jurisdictions.

With government support, wider access to authoritative data on the age of children can also be secured, allowing for exact age verification of minors through "one-way blind checks" that the age claimed by a child is accurate – this form of check does not give the age verification provider

The Age Verification Providers Association

Age Verification Providers Association
557B Wandsworth Road, London, SW8 3JD
+44 (0) 7811 409769 | iain@avpassociation.com

visibility of the data itself, only confirmation that the data already provided by a user about themselves is true.

2. Accessibility and Digital Inclusion
To mitigate risks of digital exclusion, age assurance providers offer a range of options. Users without access to traditional identification can utilise alternative methods such as facial estimation or professional vouching e.g a doctor or teacher confirms age in an online reference process. This flexibility ensures equitable access to online services while enforcing age restrictions.

3. Privacy-Enhancing Technologies (PETs)
Privacy is a core principle in the age assurance industry, and AVPA's members are committed to safeguarding user data through innovative solutions and regulatory compliance. Age assurance systems can incorporate advanced PETs to prevent data misuse:

- **Zero-Knowledge Proofs (ZKP)**: These methods verify age without sharing additional personal information. For instance, a ZKP might confirm to a social media platform whether a user is over 16 without revealing their exact date of birth or any other aspect of their full identity.
- **Double-Blind Verification**: Systems prevent service providers and verification providers from linking user identities to their online behaviour. This ensures that users remain anonymous while accessing restricted services.

4. Data Minimisation and Retention Policies
We welcome the requirements for privacy in Division 3 of the Bill. The AVPA advocates strict adherence to data minimisation principles. Only the data necessary for verifying age is collected, and it is deleted immediately after use. This reduces the risk of breaches and ensures compliance with privacy laws, such as the Australian Privacy Principles.

5. Transparent Consent Mechanisms
To build trust and comply with regulations, age verification processes must be transparent. Users are informed about how their data will be used, and their explicit, revocable consent is required before verification proceeds. Mechanisms are also in place for users to withdraw consent easily in line with the requirements of the Bill.

6. False Positives and Negatives
While no system is entirely error-free, we adopt strategies to address inaccuracies in age estimation systems. For instance, users mistakenly flagged as underage can appeal decisions and submit additional identification or use professional vouching. Similarly, estimation systems can use "buffer zones" to reduce the risk of false positives by requiring users to appear several years older than the minimum age.

7. Circumvention Risks
We should briefly address common concerns about bypassing age verification systems:

- **Shared Devices**: Periodic re-authentication (checking it's the still the same user who did the age check) ensures that access granted to an adult does not inadvertently extend to a child using the same device.
- **VPNs and Location Spoofing**: Platforms can detect VPN use and block such traffic. Alternatively, they may require users to verify their location is outside Australia through additional methods, similar to systems used in online gambling to enforce jurisdictional restrictions.

8. Alignment with Risk and Stringency

We would like to emphasise that the level of stringency in age verification systems should be proportional to the risk of harm associated with a platform or service. For example:

The Age Verification Providers Association

Age Verification Providers Association
557B Wandsworth Road, London, SW8 3JD
+44 (0) 7811 409769 | iain@avpassociation.com

- **High-Risk Services**: Platforms hosting adult content or material related to self-harm require the most stringent verification methods, such as official ID checks or facial age estimation with higher accuracy thresholds.
- **Moderate-Risk Services**: For social media platforms targeting a general audience, less intrusive methods, such as email or facial age estimation with broader tolerances, may suffice.

These are questions the eSafety Commissioner already well understand and we would argue for legislative rules and eSafety Guidance to clearly define acceptable error margins and verification standards based on risk.

9. Cost-Effectiveness and Interoperability

The cost of age verification services has dropped significantly due to technological advancements and increased competition. While early systems cost over $1 per check, the UK government recently reported an average cost 19 cents (AUD) per check with discounts for high volume, and a downward trend in pricing through interoperability and technical development. Providers typically charge for the initial verification but allow free re-use of the results across platforms for a year or more.

Interoperability greatly enhances user convenience by enabling a single verification to be recognised across multiple platforms. Initiatives like euCONSENT's AgeAware® ecosystem facilitate the secure sharing of verification tokens, reducing redundancy and costs for users and service providers.

10. Alternatives

While many social media platforms make parental controls available, parents need to be aware of them, capable of using them and determined to do so, and not to be persuaded by children to remove them. In a recent US Senate Judiciary Committee hearing, Snap CEO Evan Spiegel revealed that approximately 20 million U.S. teenagers use Snapchat, but only about 200,000 parents utilize its Family Center supervision controls, suggesting that only about 1% of parents implement parental-control features.[1]

Restricting app downloads based on age is a blunt instrument that may exclude users unnecessarily. Many apps contain content suitable for all ages alongside age-restricted features, requiring a more nuanced approach.

11. Recommendations and Conclusion

Society has imposed age-restrictions for the past 100 years. As our lives move increasingly online, it is not surprising that there is a widespread desire to apply those same controls on the Internet. Our industry was created to enable this, mirroring the real world including the way a cashier might be satisfied a customer looks well over 18 before selling alcohol without requiring proof, and how bar staff only concern themselves with a drinker's age, not their full identity.

We were fortunate to accelerate the development of our technology through the foresight and sponsorship of the European Union. Australia, through its proposed pilot of age assurance and this legislation, now has the opportunity to take up the mantle and deploy the next generation of this technology, which will incorporate important concepts such as device-based, double-blind design.

Yours sincerely

Iain Corby
Executive Director

[1] https://techcrunch.com/2024/01/31/snap-ceo-says-20-million-u-s-teens-use-snapchat-but-only-200000-parents-use-its-family-center-controls/

The Age Verification Providers Association

Age Verification Providers Association
557B Wandsworth Road, London, SW8 3JD
+44 (0) 7811 409769 | iain@avpassociation.com

Appendix – Age Estimation

Facial age estimation - Originally, age assurance was developed solely to determine if a user was an adult, to address use-cases such as the purchase of alcohol or access to online wagering and adult-only content.

More recently, a need to assess the age of minors has arisen, driven by a desire to enforce not only minimum ages for the use of social media, but also data protection laws where younger children may, for example, require parental consent before agreeing to share personal data. Obviously, not all of the methods described above are suitable, in whole or in part, for children. Fewer children than adults will have a passport, none will have a credit record or a driving licence, only some will have a bank account etc.

Facial age estimation emerged as a more accessible option. The algorithms used to estimate age are improving by the day, and six examples were recently tested by the US Federal Government National Institute of Standards and Technology (NIST), and we would commend their report to the Committee as evidence for consideration in its own right[2]. One of our members, Yoti, publishes regular White Papers disclosing the accuracy of their estimation tool[3].

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	1.3	1.4	1.7	1.4	1.2	1.3	1.4	1.3	1.4
13-17	1.3	1.5	1.7	1.5	1.0	1.4	1.6	1.3	1.4
18-24	2.4	2.3	2.4	2.4	1.9	1.9	2.0	1.9	2.1
25-70	2.8	3.2	3.9	3.3	2.6	3.1	3.2	2.8	3.0
6-70	2.5	2.7	3.3	2.9	2.2	2.6	3.0	2.6	2.7

A degree of error is inevitable, so a policy-decision is required to accept an approximation, knowing some underage users will be false positives. The proportion of false positives can be reduced by testing if a user appears to be a couple of years older than the minimum age – the difference being termed a "buffer", and its width determining with statistical certainty the expected proportion of false positives. NIST specifically studied this in their analysis.

Email address analysis - Email analysis has also proven to be an effective method. Another of our members, VerifyMy, has just published a White Paper which sets out the accuracy that has achieved4. Out of 847 individuals actually under the age of 18 who were tested, they estimated only 19 to be older than they were (2.24% false positive rate of the testing set), and no-one's age was overestimated by more than 2 years.

[2] https://pages.nist.gov/frvt/reports/aev/fate_aev_report.pdf
[3] https://www.yoti.com/wp-content/uploads/2024/04/Yoti-Age-Estimation-White-Paper-December-2023.pdf
[4] https://verifymyage.com/email-address-age-estimation

The Age Verification Providers Association

Age Verification Providers Association
557B Wandsworth Road, London, SW8 3JD
+44 (0) 7811 409769 | iain@avpassociation.com

Estimated minimum age	Actual age 6	7	8	9	10	11	12	13	14	15	16	17	Total
insufficient data	6	5	8	3	3	2	5	10	17	15	28	23	125
7	1	1	1	1	1	0	0	0	0	0	0	1	6
8	0	0	3	6	5	5	4	6	8	0	3	2	42
9	0	0	1	4	6	6	2	8	4	1	4	3	39
10	0	0	0	0	6	4	7	14	10	1	3	2	47
11	0	0	0	1	1	9	16	16	11	13	3	4	74
12	0	0	0	0	0	0	15	23	16	15	3	0	72
13	0	0	0	0	0	0	1	19	22	13	15	12	82
14	0	0	0	0	0	0	1	2	26	63	23	7	122
15	0	0	0	0	0	0	0	0	2	15	47	18	82
16	0	0	0	0	0	0	0	0	1	1	40	64	106
17	0	0	0	0	0	0	0	0	0	2	3	43	48
18+	0	0	0	0	0	0	0	0	0	0	1	1	2
Total	7	6	13	15	22	26	51	98	117	139	173	180	847

False positive: overestimated age (grey figures)
True positive: didn't overestimate age (yellow figures) - therefore, restricting access to something the user shouldn't be able to access.
Insufficient data: where we do not have enough data to provide a meaningful response or reliably estimate the user's minimum age. This can be due to the email address being newly created, invalid or rarely used, for example.

Hand gesture analysis – in a recent innovation, whether a user is over or under a certain age can be estimated with >99% accuracy based on three hand movements. This is due to the correlation of age with the operation of tendons in the hand.

Where estimation is used, there is a need to provide alternative methods to correct false negatives, for example when a 14 year-old has been estimated to look under 13 so is initially denied access to social media (assuming 13 is the applicable minimum age). In this case, the user might first be asked if they do have a suitable ID document, such as a passport. Ideally, the Australian federal, state and territory authorities would also facilitate access to the many sources of data they hold on children's ages – schools, social security benefits, healthcare etc. But there must also be a third level – age assurance of last resort – to ensure that no child is excluded simply because they look too young and lack paperwork – that can be achieved through professional vouching. Social media site Yubo has for several years also addressed this through allowing parents to contact them and after a short interview be relied up to vouch for their child's age as well.

But for the vast majority of people who are by definition more than +/- 2 years of any given minimum age, age estimation is a quick, convenient, privacy-preserving and effective method of age assurance.