Committee Secretary
House of Representatives Standing Committee on Social Policy and Legal Affairs
PO Box 6021
Parliament House
Canberra ACT 2600

By email: spla.reps@aph.gov.au

17th November 2019

Dear Honourable Members,

Inquiry into age verification for online wagering and online pornography

The Age Verification Providers Association (AVPA) welcomes the opportunity to provide a submission to the House of Representatives Standing Committee on Social Policy and Legal Affairs' Inquiry into age verification for online wagering and online pornography.

Executive Summary

The core messages of this submission are:

1. Online age verification technology already exists; it is effective and already checking thousands of users a day for purchases as diverse as knives, fireworks, alcohol and betting.

2. Age verification can be implemented proportionately, adopting the appropriate level of assurance for the risk of the product or service involved.

3. Age verification can be designed to protect completely the identity of the users, by separating the age verification process from the age restricted websites which apply it, and by not retaining any personal identity data after checks have been completed.

4. This is the model envisaged for pornography under Part 3 of the UK's Digital Economy Act and the accompanying guidelines and age verification scheme from the regulator, which has been ready to go live in the UK for a year, but has been delayed by administrative errors and political decisions.

5. Equally, age verification can be implemented to provide a clear audit trail of how an individual user's age was checked, as is required for more highly regulated products such as gambling or the sale of offensive weapons.

6. Age verification for online pornography is widely supported by British adults, and specifically by parents and children alike. The UK devised an innovative solution to address the concern shared by users and indeed, by responsible adult content publishers that we need to prevent children stumbling across pornography when they are online. Policy makers wisely adopted an approach that the best should not be the enemy of the good to put some protection in place as soon as possible.

We set out below further detail and evidence in support of these key messages, and would be pleased to help the Committee further if it has additional questions, given our access to the leading technical and policy experts in this field within our membership.

About the Age Verification Providers Association

The AVPA represents all the main technology suppliers who have invested in the development of age verification solutions to support the implementation of age restrictions online.

Our current membership includes AgeChecked, AgeGo, AgeID, Avyourself, Equifax, GBG, Verime and Yoti, so ranges from start-ups to publicly listed companies. We are based in the United Kingdom, but members provide services globally and the Association engages with policy-makers around the world.

As an association, we work to:

- Inform and educate the public, industry, and media, on age verification solutions and technology.
- Promote a positive image of effective age verification and the age verification industry.
- Represent the industry to regulators and law makers for the advancement of best practice, socially-responsible age verification policy.

The AVPA was formed in 2018 from organisations involved in the UK's Digital Policy Alliance age verification working group, and created and in response to a need for a uniform voice of the industry.

The AVPA is governed by a representative Board drawn from its member organisations, and is a not-for-profit organisation.

Age Verification Providers Association Code of Conduct

The Age Verification Providers Association's Code of Conduct is a set of guiding principles our Members agree to follow when conducting business. Our aim is that these principles will drive high standards from the industry, assist in establishing best practice and create a collaborative approach to solving the problems of age verification.

The key goals of the Code are:

- To promote effective age verification
- To encourage age verification adoption in a manner compliant with regulations
- To encourage sound business practice
- To promote the highest levels of data protection and data control

Code of Conduct

AVPA Member organisations agree to the following five principles:

1. Fairness and transparency

How personal data is collected and how it is used should be clearly explained to the consumer. Data should be used for age verification and not additional unspecified purposes.

2. Use of appropriate verification methods

Data sources and technical methods against which consumers are checked should be reasonable and suitable to meet the requirements of regulators and client organisations, while recognising the sensitivities around release and use of personal data.

3. Privacy and Security

Data privacy should be paramount. Members should follow 'privacy and security by design' principles and make all reasonable endeavours to maintain the security of processed or stored personal data.

4. Accuracy

Members should take all reasonable steps to ensure the accuracy of data and rectify inaccurate data to maintain the integrity of their age verification systems.

5. Responsibility

Members acknowledge that they have a collective responsibility to maintain a positive public image of the age verification sector.

Online age verification technology already exists; it is effective and already checking thousands of users a day.

Age verification technology is evolving quickly, but legislation globally has not taken advantage of this and kept pace with the move to online products and services. In some cases, existing laws for the real world have been applicable on the web and required some form of age checking online – in other cases, the move to a virtual environment has circumvented legislation.

The UK government has adopted a principle that what is illegal in the offline world should be illegal in the online world, and several laws and regulations have either been amended or are under review to achieve this.

Initial attempts at age verification online were simple and easily evaded. They ranged from simply displaying an adults only warning, to asking users to confirm they met an age restriction by ticking a box, to asking for a date of birth, up to demanding that copies of identity documents are either scanned or mailed to share proof of age.

This was clearly not adequate for most products and services where legislation sought to impose age-restrictions.

Online age verification has been developed to provide the appropriate level of assurance for each product or service.

These range from the use of social, biometric or facial recognition technology, through credit reference agency checks up to the validated use of physical proof of age, checking their validity against databases of record or secure reads of passport NFC chip details. Tokenisation of proofs of age can mean 'verify once, use many times' sytems can be utilised.

In the UK, a code of practice, PAS 1296, was developed to provide a standard for age verification. This is now being developed into a Specification, against which providers can be audited, and it is intended to develop a British or International Standard based on the current PAS 1296. By building age verification regulation around a common standard, there will be a significant opportunity to save costs to government, regulators, industry and consumers, while also ensuring the solutions are effective and can be audited as such.

It is also important to consider the competition implications of the structure of age verification to encourage an open and competitive independent sector, rather than it becoming an opportunity for further oligopolistic domination of the internet by leading global platforms. Again, taking a standards based approach offers the basis of a competitive, interoperable marketplace, improving choice and quality for consumers while keeping price down, however it features in the value chain.

Adopting common standards also provides a basis for educating the public about AV, and its effectiveness at different levels, to reduce over time the extent of any false assurances; parents could become familiar with low, medium and high standards of assurance, learning the chances of their child being able to buy a knife would be very low, but that a 15 year old might find a way to access pornography if they are technically smart – again much as in the

offline world where parents might not be surprised their 17 year-old was served a pint in a bar on holiday, but would be more concerned if they were able to bet high stakes in a casino where they'd expect a higher standard of check.

It can be implemented proportionately, adopting the appropriate level of assurance for the risk of the product or service involved.

It would be a mistake to adopt a one-size-fits-all approach to age verification. Doing so would clearly increase the risk of the unintended consequences you are considering as part of your terms of reference:

So, for example where there is no need to retain an audit trail of age verifications, then personal data should not be retained, thus vastly minimising the risk of a privacy breach.

Where an audit trail is required by regulators or the law, still personal data need not be retained, rather only the pseudonimised record of the verification events themselves.

Where personal data storage is required by regulators or the law, additional data protection techniques are employed in line with applicable legislation - in the UK this was the Data Protection Act 2018 which brought the EU's General Data Protection Regulations into force.

The term "vectors of trust" is used in the PAS code of practice to refer to the matrix of sources of age verification, which are varied and continue to evolve, each of which carries its own degree of certainty and the number of sources used. By setting a standard for the tolerance allowed for each level of assurance, multiple combinations of solutions can be adopted to deliver the same level of confidence in the outcome.

For example, intelligent software can be used to estimate age based on photos or videos. For a jurisdiction with legal age restriction of 18, and a threshold set to 25 years, the latest technology's current mean error rate is 0.31%. For a threshold of 23 years, the error rate is 0.75%. In other words, accuracy is over 99% if the system is set to allow only customers who its analytics conclude are over 23 based on their image. Even a solution reliant on a passport, identity card or driving licence might only offer a percentage level of accuracy, after accounting for the risks of forgery, impersonation or theft. This is no different from the offline world, where there are no systems which offer 100% verification – even passport checks at borders will miss some fake or recently stolen passports.

By adopting a standards based approach, legislators can determine a proportionate response depending on the risks associated with each product or service, and the age verification industry can provide standardised solutions to meet any given level of assurance and audit.

There is of course always a risk that new protections for children may push adult consumers into unregulated/illegal environments or to other legal forms of these activities but this is minimised if the policy intent is to achieve an equal level of proportionate age verification across the offline and online environment.

The risk of evading protections by going to offshore, unregulated websites has to be addressed through enforcement, be that through financial blocks on income streams to those websites from the domestic market or through more direct site blocking through internet service providers. But in the offline world, there are equivalent challenges to extending jurisdiction beyond any country's borders; this is not usually seen as a reason not to impose rules domestically. And a standards based approach adopted globally will provide increased opportunity for international agreements and collaboration to raise standards internationally.

Age verification can be designed to protect the identity of the users, by separating the age verification process from the websites which need to check only age, not identity.

The UK's development to AV for online pornography recognised at the outset that there would be concerns about data protection – indeed linking adults' personal details with their browsing history would clearly be a blackmailer's charter, attracting the attention of sophisticated hackers – hence the imperitive to create a system for anonymous AV . It adopted a privacy-by-design solution, deliberately separating the AV process from the adult websites where an age check would be required. Moreover, the AV process was based on the principle of data minimisation so personal identity data was not retained any longer than needed to complete an age check. In most cases, this would be no more than a few seconds. The consumer would not then use any personally identifiable data when accessing adult sites, and any checks were based on pseudonymised credentials.

The best way to prevent hacking sensitive personal data is not to keep any personal data – and this is how AVPA members approached the UK solution for pornography.

This is the model that has been ready to go live for online pornography in the UK for a year, but has been delayed by administrative errors and political decisions.

Reporting about the delays to the implementation of AV for pornography in the UK has often focused on concerns raised by campaigners who have been opposed to any limits on the freedoms of the internet. These focused on what they portrayed as the Achilles heals of the policy – privacy and data security.

The reality was that there was a change of heart within government, in the context of an imminent general election. Implementing any restrictions to online pornography was not going to be universally welcomed, in spite of its popularity in polling (see below), and while AVPA members had committed to solutions which guaranteed data security and privacy, the legislation left scope for compliance with the law without adopting the non-statutory safeguards the regulator sought to add.

The UK government is still explicitly committed to introducing AV for pornography, but has suggested it will now do so as part of a broad solution addressing the wider spectrum of online harms. We are very close to government thinking on this, and it is clear that there is no new solution at any stage of maturity.

There are clearly lessons to be learnt from the development of this solution – but those we have identified relate mostly to communications – to raising public awareness and maintaining credibility that policies will be enforced to drive adoption by content publishers. There were no significant, valid criticisms of the solutions provided by AVPA members, either based on privacy or technology..

To address briefly those arguments we heard most often:

- It was the case that technically sophisticated teenagers could circumvent AV for pornography, but they would need knowledge of how to use a VPN or other mechanisms which younger children would very rarely if ever have. The policy goal was to prevent young children stumbling across pornography – and the arrangements which were ready to go live would have delivered on that aim.
- Social Media was not in scope for the regulations, but this was a policy decision, not a technical limitation.
- It was also true that minors could use borrowed credentials to access adult content – but this is analogous to an older sibling sharing an adult magazine with a younger sibling.

The AV scheme in the UK would bring the online world up to similar levels of protection as the offlinel world. And of course, there are opportunities to build on the initial solutions towards "AV 2.0" which might add more validation, perhaps through spot checks or intelligent software

assessing the use of AV credentials, in the same way credit card payments are kept under surveillance for signs of fraudulent use.

Equally, age verification can be implemented to provide a clear audit trail of how an individual user's age was checked, as is required for more highly regulated products such as gambling.

Regulation around age verification and Know Your Customer ("KYC") checks for gambling is evolving fast in Great Britain, the USA and other jursidictions.

For example, GB recently introduced a requirement for Age Verification before players may access free-to-play games or free credit bonus offers from operators. For this purpose, a simple AV check is required where the regulator may not require an individual audit trail. Data retention is minimised so, for example, one AV provider only keeps a record of how they checked an individual's age, not the actual personal data that supported that e.g. "John Smith was verified on 1/1/2019 by checking with his mobile phone provider, and was found to be over 18" – the provider does not need to keep his phone number, his date of birth, address or any other personal data but can offer sufficient reassurance to a regulator in the event of a compliance investigation.

If a player wishes to add their own funds to an account, then the GB Gambling Commission requires a more extensive KYC check, including AV, and wider anti-money laundering measures. In this case, AV suppliers will confirm details provided by the customer to the gambling operator as required; any personal data supplied by the customer for this purpose when funding their account can therefore be retained by the gambling operator once validated, rather than by the AV supplier.

There are a range of different models adopted by AV suppliers when they contract with gambling operators, but common to them all is the principle of data minimisation.

Age verification for online pornography is widely supported by British adults, and specifically by parents and children alike. The UK devised an innovative solution to address the concerns shared by users and indeed, by many adult content publishers that we need to prevent children stumbling across pornography when they are online. Policy makers adopted an approach that the best should not be the enemy of the good.

BBFC funded research by Revealing Reality showed widespread support for AV for online pornography:

- 83% of parents agreed with the statement "there should be robust age-verification controls in place to stop children (under 18s) seeing commercial pornography online"
- 56% of 11 to 13-year-olds agreed with the statement "I want to be locked out of websites that are for 18-plus-year-olds"
- 75% of parents in the survey thought their child hadn't seen pornography online, but in reality 53% of their children reported that they had in fact seen it.

A survey[1] by Internet Matters of 2044 parents found:

- 52% think a child may believe online pornography represents typical sex
- 48% say it's improper sex education leaving a child with an unrealistic view of 'normal' sex

---

[1] Source: Internet Matters report 'We need to talk about porn' – November 2018 – a survey of 2044 parents
https://www.internetmatters.org/resources/infographic-impact-of-seeing-online-pornography/
https://www.internetmatters.org/hub/news-blogs/parents-say-online-porn-gives-children-extreme-unrealistic-idea-of-sex

- 44% feel it may impact children's understanding of what normal sexual relationships should look like
- 38% believe it will set expectations to engage in specific sexual acts as part f a relationship
- Objectification of women and use of violence
- 47% are concerned about poor portrayal of women in pornography including violence and abuse
- 34% think children will become desensitised to brutal/violent content, becoming less upset, anxious or disgusted over time

Impact on body image and self-esteem:

- 27% believe it encourages poor self-esteem as they judge themselves against the actors
- 34% of parents say it harms their kid's body image (lack of confidence in their own body image)

Lack of understanding of consent:

- 36% say it gives improper education about asking for and getting consent

Addiction:

- 33% fear that children will become addicted to porn

Conclusion

The UK has led the world on AV in terms of legislation, regulation and technology for a wide range of products and services, including online gambling and pornography. It offers a model for age verification that Australia could follow quickly. Clearly solutions would need to be adapted in any new jurisdiction, but the core building blocks are already in place and could be applied in Australia within months rather than years.

AVPA members continue to invest in this field, working in partnership with governments around the world to develop a standards-based approach to AV, reducing the costs of ensuring that legislation and regulation keeps pace with technology and delivers ever more effective child protection online.

Please do not hesitate to contact me with any further questions the Committee may have – we would be pleased to respond in writing or in person and make the technical, regulatory and change management expertise of our members available to your inquiry.

Yours faithfully,

Iain M. Corby

Iain M. Corby
Executive Director
Age Verification Providers Association