Age Verification Providers Association
12110 Sardis Avenue Los Angeles California 90065
+44 (0) 7811 409769 | iain@avpassociation.com

Chair Abrams and Members
House Criminal Justice Committee
Ohio House of Representatives
Columbus, Ohio

May 2, 2024

Dear Chair Abrams, Vice Chair Williams, Ranking Member Brown, and esteemed colleagues of the House Criminal Justice Committee

House Bill 295, the Innocence Act

We are the global trade body representing 27 suppliers of privacy-preserving age verification technology. We are a politically neutral organisation, so do not offer any view as to whether lawmakers in Ohio should take action to prevent children from being exposed to pornography online, but do wish to help the Committee to understand clearly how online age verification is conducted, and support this Bill as an effective piece of legislation from a technical perspective.

We have given evidence in other states both to legislatures (watch what we said this month in California here for example) and, when necessary, in federal courts which have considered the constitutionality of similar measures, for example in Texas where House Bill 1181 was confirmed by the Fifth Circuit of Appeal and is now in force, with enforcement action already underway.

If American technology can put a man on the moon, we can easily verify the ages of Internet users without disclosing their identity.

The age verification industry was created when, in 2017, the UK government passed the Digital Economy Act required adult websites to make sure that British children would no longer stumble across hardcore pornography when online. The adult industry appreciated immediately that its consumers would be reluctant to share any personal data directly with them, so instead turned to third party suppliers who could be closely regulated, and provide assurance to users that whatever personal data was used to confirm their age would neither be passed on to the websites they wished to visit, nor retained by the age verification (AV) provider they chose.

This simple structural measure provided the basis for continued anonymity while providing sufficient evidence to the websites that they could demonstrate to the courts that they had exercised reasonable efforts to prevent child access to their content.

Age Verification Providers Association
12110 Sardis Avenue Los Angeles California 90065
+44 (0) 7811 409769 | iain@avpassociation.com

We will address two key aspects of the Bill before your committee – the ease of use of the wide variety of methods of age verification, and the data minimization designed into these approaches so personally identifiable data need never be retained:

Reasonable age verification methods

For access to obscene content, the Bill then requires "reasonable age verification measures". It is pragmatic to keep the bill technologically neutral, although at present we note it lists certain specific methods in an exhaustive list rather than as examples. As we have explained above, age verification is a relatively new technology, and is advancing quickly. So, legislation such as this Bill is right to define the outcome required – that access to harmful materials by minors is prevented – but not to stipulate in statute the exact means.

To give the Committee an understanding of what we would define as "reasonable age verification methods", based on agreed international standards, these would include:

- **Remote electronic identification verification technology (eIDVT)** – government issued physical identity documents such as passports or driving licenses are scanned as an image using the user's mobile phone camera or webcam, or, in some cases where this is included, a computer chip in the document can be read by a smartphone. The user is asked to provide a live selfie image which can then be electronically compared to the image from the ID, and provided the two match, then the age information is recorded and can then be used as the basis of age verification.

  Note that this technology already uses extensive measures to detect fake, stolen or altered ID, including ID generated as an image using Artificial Intelligence (AI), and potentially injected into the process in place of the image from user's camera. Liveness detection is also used to check that the "selfie" is from a real person, not a photo, or, again, a AI image injected instead of the actual user's image.

  Once the age has been established, the data from the ID and the selfie image are both deleted from any servers where they were processed.

- **Online banking integration** – Some AV providers have reached agreement with banks to allow a customer to log into their online banking and give consent for the bank to confirm their date of birth to the AV provider.

- **Credit Reports and other transactional databases –** A user can give consent for an AV Provider to check with Credit Report bureau if the age they are claiming is accurate. Typically, the user will have to give some further reassurance that they are the person whose credit report they are claiming belongs to them; for example, knowing about some recent payments they have made. Other authoritative databases can play a similar role, with their own approaches to authentication of the user claiming the age data relates to them.

- **Facial age estimation** – through machine learning, algorithms can now predict to within 1 ½ years mean average error the age of a user from a selfie image. The National Institute of Standards and Technology (NIST) have been testing competing solutions from providers and are expected to publish their findings this week, prior to

Age Verification Providers Association
12110 Sardis Avenue Los Angeles California 90065
+44 (0) 7811 409769 | iain@avpassociation.com

the Committee's hearing. While some people have expressed concerns about adults sharing a selfie image for this purposes, it should be noted that the estimation can be made locally on the user's own phone or PC, so the image need never be shared with a third party.

Given there is a margin for error, typically this would be made available as an option for users who are several years over 18 – for example, 23 – when it is statistically proven that the vast majority of minors under 18 would not be estimated to look at least 23. Users who are closer to 18 will need to use an alternative mechanism.

Note: Sometimes people are concerned this method encourages children to share selfie images online. Of course, that is entirely misplaced because it is only adults well over the age of 18 who will be using this option. Children should not be trying to access obscene material – and would of course fail the test anyway. As noted, images need never leave the user's own device.

- **Reusable digital identity** – Digital ID is becoming increasingly available. Several US states issue mobile drivers licenses, for example. Users can give consent for the age to be selectively shared with AV providers, typically using an approach called Verifiable Credentials.

Standards, audit and certification

All of these standards are delivered in compliance with international standards, such as BSI PAS 1296:2018, and IEEE 2089.1. Regulators and courts can look to see that adult websites apply age verification technology, either built internally or outsourced from specialist age verification providers, which has been audited and certified to meet the requirements of those standards. Standards not only address the accuracy of the outcome of the age checking process, but also privacy and data security.

The virtual private network fallacy

We also note that the use of a virtual private network (VPN) would not excuse an adult website from its responsibility to prevent children from being exposed to obscene content. There is no "get-out-of-jail-free card" offered in this Bill – so if an adult website decided to block access from Ohio but then promoted VPN products that enabled users to evade an age verification requirement by pretending to be located out-of-state, the website would remain liable if a minor actually in Ohio was given access via a VPN.

No personal data retained

There is no need to retain any identifying information once the age verification has been completed. So, if personal data is shared with a third party in course of an age check, it would be for a few seconds and must then be deleted.

Some vendors already offer age assurance that is processed on the user's own device, so no personal data is ever shared with third parties.

Courts need to be given confidence that websites have checked ages effectively based on their use of a certified provider, not demand the production of specific evidence that each user was checked accurately, as this would have the perverse impact of encouraging the collection and retention of sensitive personal data. We strongly recommend that age verification is not designed to retain any personally identifiable information centrally. The only non-hackable database is no database at all. Good practice principles of data minimization and privacy by design should dictate that such databases of personal data are not created by websites or their age verification providers.

Reusability and interoperability

The European Commission funded a project to create interoperability that would allow a single age check to be re-used across multiple websites without the user repeating the age checking process. The project, www.euCONSENT.eu, delivered a successful largescale pilot in 5 different EU states, and has been continued by a non-profit organization of the same name. This week it announced plans for a further pilot based on an updated architecture, which would create a tokenized system, and an on-device application, that utilizes Privacy Enhancing Technology (PET), and zero-knowledge proof. This is being designed to add further privacy protections, using concepts developed by the French and Spanish data protection authorities, CNIL and AEPD

[Note: There may be a benefit in refining the definition of "identifying information" so it is clear that age verification providers can re-use age checks, through pseudonymized records of previous checks (such that if the records were stolen by a bad actor, they would be of no use or value).]

This approach, grounded in international standards, would deliver privacy-by-design, and could easily be implemented in Ohio, using the trust framework that participating age verification providers form between them, under the auspices of this non-profit certification body.

Conclusion

The essence of online age verification is proving your age without disclosing your identity. If anonymity were not required, our industry would not exist, as its role could be played by the much larger and well-established digital identity provider industry. Commercial and legal objectives both drive the need to implement age verification in a way that protects the users identity, and prevents any possibility of tracking.

Thank you for the opportunity to contribute to the important work of the Committee, in making the Internet a safer place for children, in Ohio.

Yours faithfully,

Iain Corby
Executive Director
The Age Verification Providers Association