Age Verification Providers Association
557B Wandsworth Road, London, SW8 3JD
| iain@avpassociation.com

Chair and Members
House Business Affairs & Labor Committee
Colorado General Assembly

April 23, 2026

Dear Chair and Members of the Committee,

Re: Senate Bill 26-051 – Age Attestation for Users of Computing Devices

I write in my capacity as Executive Director of the Age Verification Providers Association (AVPA), the global trade association representing providers of privacy-preserving, standards-based age assurance technologies operating across the United States, United Kingdom, European Union, Australia and other jurisdictions.

Our members collectively perform more than one billion age checks annually and supply the technologies currently used to comply with online child-protection laws worldwide. We therefore welcome the Committee's efforts to improve protections for minors online.

However, we believe SB26-051 contains several structural flaws which risk undermining that objective while simultaneously weakening the enforcement tools Colorado currently has against platforms that harm children.

We set out our concerns below and respectfully ask the Committee to pause this bill pending further work.

Our core concern: this bill is not age verification

The bill's title refers to "age attestation" — and that word choice matters. Attestation means someone declares their age. Verification means that declaration is checked. This bill does the former and not the latter.

The entire framework rests on whatever age a user enters during device setup. There is no requirement to check that information against any document, database or independent source. There is no requirement to confirm that the person entering the age is an adult, or a parent, or has any authority over the child who will use the device. A thirteen year old can set up a device, declare themselves an adult, and this bill provides no mechanism to detect or prevent that outcome.

The bill then requires every app and platform in Colorado to treat that unverified declaration as the primary legal indicator of a user's age. That is not child protection. That is a legal framework built on an assumption that will routinely be wrong.

The liability shield concern

We are particularly concerned about the combined effect of two provisions. The bill protects operating system providers from liability for erroneous age signals where they make a good faith

effort to comply. It simultaneously requires developers to treat the age signal as the primary indicator of age, over-rideable only by clear and convincing evidence to the contrary.

Together, these provisions create a complete liability chain in which no party is accountable when a child is harmed — because the operating system provider is protected by good faith compliance, and the developer is protected by statutory reliance on the signal.

This Committee will be aware of the $375 million judgment against Meta in New Mexico, which rested on the argument that Meta had information suggesting users were minors and chose to ignore it. Under this bill, that case would be significantly harder to bring in Colorado. Once a developer receives a state-mandated age signal saying a user is an adult, that signal becomes the primary legal indicator of their age. Behavioural signals — the kind that succeeded in New Mexico — may not meet the clear and convincing threshold this bill requires to override it.

We do not believe the Committee intends to hand the largest platforms in the world a statutory defence against exactly the kind of enforcement action Colorado should want to bring. But that is the practical effect of this bill as drafted.

The centralisation risk

By designating operating system providers — Apple, Google and Microsoft — as the authoritative source of age signals, the bill creates a centralised signalling infrastructure at the heart of Colorado's app ecosystem. The bill restricts what those platforms share with developers, and we acknowledge that as a genuine data minimisation provision. However, it does not address how long those platforms may retain records of age signal requests, how frequently those requests may be made, or how that centralised infrastructure may evolve over time. The platforms that will operate this system are the same ones this Committee has repeatedly scrutinised for accumulating data on users. This bill gives them a new, legally mandated role in every age-related transaction in Colorado, without equivalent obligations on their own data practices.

Real-world device usage

The bill assumes each device has a single, stable, identifiable user. That does not reflect how devices are actually used. Shared family tablets, devices handed down from adults to children, borrowed devices and resold handsets are all common. The bill explicitly removes liability where a device is used by someone other than the designated user — acknowledging this limitation while leaving the resulting safety gap entirely unresolved. Shared devices are disproportionately common in less affluent households, meaning the children already at greatest risk are the least protected by this framework.

A better approach exists

We are not asking this Committee to abandon the goal of protecting children online. We are asking it to pursue that goal through a framework that actually works.

Age verification systems exist today — operated by independent, regulated providers — that can verify a user's age accurately and privately, without routing every transaction through a Big Tech platform account. These systems use reusable tokens that allow a user to prove their age to any website or app without the operating system provider acting as intermediary or retaining any record

of the transaction. Websites and apps remain fully accountable for who they admit. The verification is real, not declared. And the infrastructure does not concentrate yet more data and power in the hands of a small number of platform gatekeepers.

As we noted in our earlier submission to the Senate Business, Labor, & Technology Committee, this position should not be understood as opposition to well-designed app store or device-level participation in age assurance ecosystems, which can play a complementary role when combined with independently verified age assurance methods, and not reliant on operating systems to co-sign age signals to prove authenticity.

A more durable framework for Colorado would distinguish clearly between self-declaration and verified age assurance, ensure that liability aligns with actual control over risk, permit independent privacy-preserving solutions to operate alongside any device-level signals, and apply proportionate requirements based on the risk profile of the service involved.

Conclusion

SB26-051 creates an age signalling infrastructure without age verification, and reallocates liability without ensuring accuracy. It risks creating a false sense of security while removing the legal pressure on platforms that is currently the most effective tool available to protect children.

We would be pleased to work with the Committee and the bill's sponsors on amendments that address these concerns. We remain available to answer questions or provide further technical briefing at any time.

Yours sincerely,

Iain M. Corby

Executive Director

Age Verification Providers Association

House Business Affairs & Labor

04/23/2026

SB26-051 Age Attestation on Computing Devices

Typed Text of Testimony Submitted

Name, Position, Representing	**Typed Text of Testimony**
Joseph Pero Against themself	I respectfully urge you to oppose SB 26-051. While protecting minors online is an important goal, this bill creates significant constitutional, privacy, and practical concerns. By requiring operating systems to collect age information at the device level and transmit age â€œsignalsâ€ to apps, the state would mandate a new, centralized age-tracking infrastructure. Even if limited to age brackets, this expands the collection of sensitive data and increases the risk of misuse or breaches. The proposal also relies on self-reported ages, which are easily misrepresented. This creates a false sense of safety while exposing developers, especially small businesses, to substantial liability, including penalties of up to $7,500 per minor for intentional violations. In addition, restructuring how users access lawful online content raises serious First Amendment concerns and will likely result in costly litigation for the state. Protecting children online requires targeted, effective solutions. SB 26-051 instead imposes sweeping technical mandates with uncertain benefits and significant legal and economic risks. I respectfully ask you to vote AGAINST this bill. Thank you for your consideration.