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

Chair Senator Jessie Danielson and Members
Senate Business, Labor, & Technology Committee
Colorado General Assembly

February 24, 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 creating legal uncertainty for platforms, developers and consumers.

- The bill does **not create an age verification system**, but instead relies entirely on self-declared age information entered during device setup.
- Liability is shifted away from both operating system providers and developers even when age data is inaccurate, leaving children with no legal recourse if harmed online.
- Services may obtain effective legal protection by relying on an age signal that has never been independently verified.
- The framework assumes devices have a single stable user, which does not reflect real-world device usage.
- There is no mechanism to ensure that a parent, rather than a child, establishes or configures a device account.

In short, the bill reallocates responsibility for determining age without establishing a reliable method for doing so.

While we usually support any measure that might help protect children online better, we must oppose this bill because it creates a false sense of security, and provides a liability shield to platforms which will remove the only existing legal pressure to consider the risks to children from their operations.

This position should not be understood as opposition to well-designed device-level or app store participation in age assurance ecosystems (e.g. the App Store Accountability Act), which can play a valuable but complementary role when combined with independently verifiable age assurance methods.

We set out below several technical and policy considerations which we respectfully recommend the Committee address.

1. SB26-051 establishes age attestation, not age assurance

The bill requires an operating system provider to collect a birth date or age declaration at account setup and generate an "age signal" shared with applications.

No verification requirement exists at any stage.

The accuracy of the entire framework therefore depends on truthful self-declaration by whoever configures the device. The legislation does not require:

- documentary verification
- biometric or estimation checks
- parental authentication
- periodic confirmation of age
- independent auditing of accuracy

Modern child-safety regulation internationally has moved toward **highly effective age assurance**, recognising that self-declaration alone has repeatedly proven ineffective. SB26-051 instead codifies self-declaration as a compliance mechanism, and gives platforms safe harbor if they look for these unreliable signals.

This risks creating a statutory system that appears protective but delivers limited real-world safeguarding.

2. The bill functions as a parental consent model without verifying parents

The legislation assumes that an "account holder" is either an adult user or a parent configuring a child's device.

Yet there is no mechanism to confirm that the person entering age information:

- is an adult
- is a parent or guardian
- has authority over the child
- is not the child themselves

A minor may therefore configure a device and declare an adult age without any safeguard preventing or detecting this outcome.

The bill effectively recognises parental consent without establishing parental identity or even that the person claiming to be a parent is themselves an adult.

3. Liability allocation creates a potential safe harbour based on unverified data

SB26-051 provides that operating system providers are not liable for erroneous age signals where they make a good-faith effort to comply.

At the same time, developers must treat the age signal as the primary indicator of age unless they possess clear contrary evidence.

Together, these provisions risk producing an unintended (or possibly intentional) consequence:

- operating systems are protected even when age data is wrong, and
- developers may rely on that incorrect data to demonstrate compliance.

This will function in practice as a liability shield for services whose platforms are accessed by minors, despite the absence of independent age assurance – a new Section 230 to protect technology platforms from any liability for doing harm, and in this case, harm to children.

The Committee may wish to consider whether reliance on unverified self-reported data should satisfy child-protection obligations in every possible use case – even where the risk to the child is very high, such as, for example, live video calls with other unknown users.

4. Real-world device usage undermines the model

The bill assumes each device has a single identifiable “primary user”. Modern device ecosystems operate differently.

Common scenarios include:

- shared family tablets and consoles
- devices handed down from adults to children
- resale and refurbishment markets
- temporary borrowing or guest use
- children using parents’ logged-in devices

The legislation explicitly removes liability where a device is used by someone other than the designated user.

This provision acknowledges a structural limitation while leaving the resulting safety gap unresolved.

An inaccurate age signal may therefore persist indefinitely across multiple users and services; and devices are more often sharing in less affluent households putting already disadvantaged children at even greater risk.

5. Legal fiction of “knowledge” without factual certainty

The bill deems developers to have knowledge of a user’s age range once an age signal is received.

However, that signal may originate solely from self-declaration entered years earlier under unknown circumstances with no audit trail to check who completed that set-up process.

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

This creates a regulatory fiction in which legal knowledge is established without evidentiary reliability, potentially weakening enforcement and creating uncertainty in litigation.

6. Absence of proportional or risk-based assurance

All applications receive the same age signal regardless of risk profile.

The framework does not allow higher-risk services to require stronger assurance levels, nor does it support progressive verification where risk increases. This differs from modern regulatory models, which apply proportionate safeguards depending on harm exposure.

7. Market and competition implications

Centralising age signalling within operating systems may also unintentionally:

- discourage deployment of independent privacy-preserving age assurance solutions
- reduce consumer choice in verification methods
- concentrate even more power in a small number of platform gatekeepers who become the sole mechanism for compliance with legal age restrictions.

International standards increasingly support interoperable ecosystems where users can choose among competing privacy-protective providers rather than relying on a single device-level declaration.

8. International interoperability challenges

Many jurisdictions now require demonstrably effective age assurance for certain services. A system based solely on device self-attestation may not satisfy those obligations.

Platforms operating globally could therefore face conflicting legal requirements, complicating compliance and enforcement.

Concluding observations

The AVPA supports the Committee's objective of improving online protections for minors. However, SB26-051 currently creates an **age signalling infrastructure without age verification**, and reallocates liability without ensuring accuracy.

A more durable framework would:

- distinguish clearly between self-declaration and verified age assurance
- ensure accountability aligns with control over risk
- permit independent, privacy-preserving age assurance solutions to operate alongside device signals
- recognise the realities of shared and evolving device usage
- encourage the adoption of modern, tokenized, double-blind interoperable and reusable age verification networks.

We would be pleased to work with the Committee to explore amendments that preserve privacy while delivering demonstrably effective protection for minors.

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

Thank you for the opportunity to provide technical input. We remain available to answer any questions or provide further briefing.

Yours sincerely,

Iain M. Corby
Executive Director
Age Verification Providers Association

Testimony of John Read, Digital Childhood Alliance
Before the Senate Committee on Business, Labor & Technology
Opponent Testimony on SB26-051

My name is John Read, and I am the Senior Policy Counsel for the Digital Childhood Alliance. The alliance consists of over 170 grassroots and larger organizations committed to protecting children and holding Big Tech accountable. Before joining the Digital Childhood Alliance, I was an attorney at the Department of Justice for 30 years, with my last years concentrated on legal issues surrounding Big Tech's businesses.

I would like to provide background first on where children are primarily being harmed in the digital world and second on competing approaches to online age verification – a fundamental step to protecting kids online.

Today, 95% of all teens have access to a smartphone.[1] Teens spend an average of 7.5 hours per day on screens.[2] While on the phone, those teenagers are spending 88% of their time on apps, with the average teen receiving approximately 240 app notifications each day.[3]

Teens vastly prefer an iPhone over an Android (88% versus 12%).[4] Today you can download more than 1.9 million apps from almost 800,000 developers from the App Store.[5] Apple collects for itself and developers over $90 billion per year from those app downloads.[6]

With the growth of the iPhone and apps that run on it, there has been a spike in kids who are depressed, anxious, socially isolated, and contemplating suicide. Research shows that increased smartphone and app use is a major cause of that spike.[7]

---

[1] https://www.pewresearch.org/internet/fact-sheet/teens-and-internet-device-access-fact-sheet/
[2] https://www.aacap.org/AACAP/Families_and_Youth/Facts_for_Families/FFF-Guide/Children-And-Watching-TV-054.aspx
[3] https://www.mobiloud.com/blog/what-percentage-of-internet-traffic-is-mobile
https://www.michiganmedicine.org/health-lab/study-average-teen-received-more-200-app-notifications-day
[4] https://mashable.com/article/teens-really-love-their-iphones (April 10, 2025)
[5] https://42matters.com/ios-apple-app-store-statistics-and-trends
[6] https://www.businessofapps.com/data/apple-app-store-statistics/ (January 22, 2025)
[7] https://pmc.ncbi.nlm.nih.gov/articles/PMC7012622/ Canadian Medical Association Journal, "Smartphones, social media use and youth mental health" (2020);
https://www.adventisthealth.org/blog/2023/august/how-screen-time-affects-teens-mental-health-and-/;
https://www.psychiatrist.com/news/chronic-smartphone-use-linked-to-teen-anxiety-depression-and-insomnia/ ; Jonathan Haidt, *The Anxious Generation: How the Great Rewiring of Childhood Is Causing an Epidemic of Mental Illness* (2024).

As a result, many states are looking to protect children online. A common challenge they face, however, is how to determine online who is an adult and who is a minor. There are three general approaches to that problem. Unfortunately, SB26-051 chooses a problematic, inferior approach.

The tech companies have been fighting with each other over the merits of two age verification approaches for apps on phones. On one side are developers like Meta or Match.com with its dating apps; on the other are the app stores (run by Apple and Google) through which consumers download or purchase the apps.

Apple and Google argue that the developers should figure out who is an adult and who is a minor on each of their apps since they created content that is harming minors. The problem, of course, is this would mean more than 800,000 developers would become responsible for figuring out the ages of their users on their apps. That is unworkable.

To avoid that unworkability issue, some states have identified only certain developers who they determined harm minors and have tasked only them to age verify their users. But courts have struck down such legislation as violating the First Amendment because the state is chosing to disfavor one or two types of speech over other speech.

A second alternative to figuring out who is a minor online is to have the app store do it. This mirrors the approach in the physical world where stores that choose to sell tobacco or alcohol must verify they are selling to an adult. A useful fact is that in the online world, Apple and Google have already verified the customers' ages. They already take the ages entered into the phone and have verified them with the credit card you uploaded to make purchases, and all the other touch points their algorithms use to distinguish adults from minors.

That second approach is not burdensome to consumers as the verification has been done behind the scenes. It is the most accurate approach and has been adopted by the states of Texas, Utah, Alabama, and Louisiana.

This bill takes a third approach. It says that whatever age the kid declares will be the online age of that person that the developers and app stores must abide by. This approach is called self-attestation and was recently adopted by California. There the tech companies were fighting the merits of the first two approaches, but eventually got together, and, without giving the large community of child advocates a seat at the table, came up with this third approach.

The tech companies agreed that whatever age someone declares will be the age they all have to take as true. They did this even though the research shows that children routinely lie about their age to access more mature content. *See*

https://www.bbc.com/news/technology-63204605 (one in three children lie about their age to access adult content); https://shellypalmer.com/2013/07/survey-children-lie-about-their-age/ (finding 80% of children lie about their age online). This should not be surprising as we all know teenagers who got fake IDs to enter bars, which is much easier to do than just clicking a false age online. This California, self-attestation approach did not protect kids, just the tech companies.

Here is an example of what SB26-051 would require based on this self-attestation approach: Assume a 15-year-old declares they are 18 to access gambling apps, to have conversations with 21-year-olds on a dating app, or to access porn. The app developer would then be REQUIRED to give the 15-year-old access to everything they would an adult. This happens even if the app store knows the kid is lying and the developer suspects it. In fact, the bill immunizes the app store for sending the false age information. *See* Sec. 6-30-104 (the app store "is not liable for an erroneous age signal indicating a user's age range or for conduct by a developer that receives an age signal indicating a user's age range."). When a kid lies about their age, the developer can only use the accurate age if the developer creates "clear and convincing" evidence of the accurate age. That is a high legal threshold that developers will usually have no incentive to meet.

Today, many developers rely on self-attestation which has helped create the litany of problems for children in the first place. This bill will not solve those online problems for children. But it will immunize Big Tech.

I encourage you to oppose the bill.

contact: Andrew Brandt
policy@electmorehackers.com

Testimony supporting an "oppose" position to bill SB26-051

BOULDER, CO (February 24, 2026): Thank you, members of the senate business, labor, and technology committee for taking the time to read my testimony. My name is Andrew Brandt, and I am the executive director of an organization called Elect More Hackers, the purpose of which is to advise policymakers on topics relating to technology, information- and cybersecurity, data privacy, and machine learning/AI, and to recruit and train people with a cybersecurity background to run for public office. Just this month, I organized the first Hackers on the Hill event at the Colorado legislature.

My background includes a 19-year career in cybercrime investigations and cybersecurity research, which includes serving in the role of director of threat research for Solera Networks, Blue Coat Systems, and Symantec, and as a principal researcher at both Sophos and Netcraft, all of which provide cybersecurity products or services to government, enterprise, and household consumers. Prior to working in the cybersecurity industry, I worked as an editor and investigative journalist for the magazine PC World, covering the cybersecurity industry as a beat, and authoring the Privacy Watch column for six years.

I'm writing today to express opposition to the age attestation bill, SB26-051. While I understand and appreciate the protective intent of the main sponsors/authors of this bill, the technology envisioned by the bill's authors does not currently exist, and would require signficant reworking of virtually all technological devices and operating systems in order even to be able to be implemented.

I'm not sure what stakeholding has been done in the software development community, but from my experience, the entire concept of such a protocol to develop an age bracketing signal is deeply flawed from a technical, information security, and data privacy perspective.

For one thing, many developers would simply resist or ignore any state-level requirement for implementation of an age attestation protocol in the operating system of a device they manufacture. In the open source software community, there would be widespread resistance to accomodating the requirements of the bill. Would the use of Linux become illegal under this law?

The bill envisions technologies that require processing of legal forms of ID at the time of first installation, without regard to the fact that the technology required to enable such a task has never been created, and that existing age verification services operated by third party private businesses exist in a legal grey area, in ways that violate the privacy of the people who use such services. Would we entrust the safety of sensitive personally identifiable information of every Coloradan to companies like Palantir, whose founder's explicit goal is to destroy democracy itself for his personal benefit?

What happens when people bring devices purchased or used outside of Colorado, where such an age attestation law may not exist, into the state? Do those devices suddenly change their fundamental

operation based on their location when inside the state's borders? Are international visitors required to install custom software on their devices in order to ensure compliance with this bill the moment they step off an aircraft at Denver airport? Will visitors from Europe be required to violate their own continent-wide General Data Protection Rights upon disembarkation in the state?

Successful implementation of this bill would require all devices to set and use the attestation protocol, but the wording of the bill does not account for many common circumstances in which technology is used by a variety of people. Whose age will the attestation service on a multiuser device, such as a desktop or laptop shared by family members, a television with internet capabilities, or the myriad other types of internet connected devices such as Raspberry Pi or Arduino computing boards, streaming TV or audio devices, smart speakers, or videogame consoles, just to name a small subset of the internet-of-things that would fall under the purview of this bill.

Colorado happens to be the home of the Media Archaeology Lab, which houses the largest collection of functional retrocomputing and retrotechnology devices in north America, at the University of Colorado at Boulder. I am a docent and volunteer at the MAL. If this law passes, would any technological device in the lab from the dawn of the internet era suddenly become contraband and would its operation become illicit?

Have the bill's authors considered that the very act of digital media preservation would become legally impossible in the future, in devices that require the continuous operation of an internet-connected service to perform this attestation? From my experience in the work I do in the lab, the greatest threat to software preservation comes from now-defunct digital rights management, which preservationists and hobbyists must bypass using legally questionable software cracks, just to maintain access to systems that require license keys or other technology from long-dead companies.

If, in the future, the service shuts down, do the authors envision a built-in killswitch for the attestation functionality, or do they just expect to create mountains of unusable e-waste for our landfills, as devices render themselves unusable?

And what would be the outcome? That only a small subset of the technology devices currently on the market could ever even hope to implement such a protocol, and everything else would become contraband.

From a cybersecurity perspective, the entire prospect of this bill creates a gigantic attack surface. Any attestation feature will end up being yet another battleground between device users and adversaries intent on capturing their personally identifiable information. We already have historically poor society-wide understanding of even basic cybersecurity principles. Will you now add a new layer of risk to our already fragile data environment?

As someone who works in cyberdefense, I already have enough to defend that my employability is guaranteed until any time I want to retire. Please do not make the mistake of moving forward with an ill advised and unimplementable law such as this.

Thank you.

Andrew Brandt

My name is Lexi Roth. I have developed both mobile and desktop applications, in my personal capacity, and for no commercial gain. While I believe the intention of the sponsors of this bill is important, I worry that the bill, as written, is overly broad and may lead to harm.

Firstly, I have concerns about several broad definitions within the bill. At page 3, line 24, the bill defines “Application” as “A SOFTWARE APPLICATION THAT MAY BE RUN OR DIRECTED BY A USER ON A DEVICE.” This, clearly, refers to all apps – mobile apps, desktop apps, desktop video games, and more.

Meanwhile, "OPERATING SYSTEM PROVIDER" MEANS A PERSON THAT DEVELOPS, LICENSES, OR CONTROLS THE OPERATING SYSTEM SOFTWARE ON A DEVICE. While it is likely the intention of the sponsors to include iOS (iPhone devices), Android, Windows computers, and Mac OS computers under this definition, the definition is much more expansive. It includes operating systems based on Linux, which are often developed by many, diverse contributors. Is it the intention of this bill to define every person who contributes to an operating system as an “operating system provider”? If not, which Linux developers *are* the “operating system provider” who is required to provide an interface at account startup?

I am also worried about the definition of a “COVERED APPLICATION STORE” (page 3, line 26), which would include websites like GitHub, where developers can upload their applications, and users can download those third-party applications. This definition may also include independent, free and open source software stores like F-Droid. It is unclear what obligations a Covered Application Store would have under this bill. The bill places clear obligations on an operating system provider, but only allows, and requires under certain circumstances, *developers* to request age signal information from a Covered Application Store.

To be clear, Covered Application Stores may not be able to specifically identify which user downloaded an application, and they have no clear obligation to ask for, or disclose, a user’s age. I believe the bill could serve the same purpose by removing all references to a Covered Application Store.

As discussed earlier, the bill has an expansive definition of “Application”. I will use an application that I developed as an example. When I was around 15 or 16 years old, I had my Colorado learner’s permit, and needed to collect supervised driving hours. There is a publicly available app that is recommended by the State, RoadReady, but that application had significant usability issues. I decided to develop my own app to log my supervised driving hours, and created an application which runs on Android devices. Under the bill, this driving log app is unambiguously an “Application”. If I updated my app on or after January 1, 2027, I would therefore be *required* to request the age of every user of my application. This is despite the fact that my driving log app currently does not connect to the internet, does not share any information with any third-party, and certainly does not have any content that is potentially harmful to minors. There is absolutely no reason my application should be *required* to request, from the operating system, a user’s age.

Instead, I would suggest that the bill be amended to narrow the definition of “Application” to exclude apps like mine. The term could limited to *only* include applications which a developer knows, or reasonably should know, may contain content harmful to minors or be regulated by specific laws which require the application to behave differently for users of different ages. If a developer reasonably should know that their application meets this definition, but fails to request an age signal, the same penalties could apply.

I believe this narrower definition of “Application” would fulfill the purpose of the bill without needlessly burdening developers of applications like a driving log, a clock, or a text editor.

The bill requires an operating system provider to have an interface for “age signals”, including “age-bracket data.” This term requires *at a minimum* the age brackets of: under 13 years of age; 13-15 years of age; 16-17 years of age; and 18+ years of age. Specifying “at a minimum” in the bill implies that an operating system provider *could* provide more age brackets. However, the bill later requires (at page 5, line 7) that the interface “[s]end only the minimum amount of information necessary to comply with this article 30.” This is contradictory. If an operating system provider is required to provide the minimum amount of information, then specifying a user’s age beyond the 4 brackets that are explicitly required would be a violation of the bill.

Finally, the bill requires that “An operating system provider shall not share an age signal with a third party for a purpose not required by this article 30.” I believe this provision is important, but perhaps impossible to implement. By implementing an interface that is accessible to all applications, any application could request age signal information and use it for any purpose – including, for example, targeted advertising towards the user. While this would potentially be a breach on the part of the *developer*, it is effectively impossible for the operating system provider to prevent this abuse. The bill puts a flag on every user with their age range, requires that applications request this information, and expects those applications to use the information only for age verification, and no other reason. I worry that many applications will take advantage of this information for their own gain, and may harm minors in the process.

For these reasons, I urge you to AMEND Senate Bill 26-051. I ask that you remove references to “Covered Application Store[s],” narrow the definition of “Application,” and perhaps put in place greater restrictions to prevent the misuse of age bracket data.

Thank you,
Lexi Roth